IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 22 June 2023, accepted 9 July 2023, date of publication 12 July 2023, date of current version 21 July 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3294844

RESEARCH ARTICLE

Star-Specific Key-Homomorphic PRFs From Learning With Linear Regression

VIPIN SINGH SEHRAWAT[1,*], FOO YEE YEO[2], AND DMITRIY VASSILYEV[3]

[1]Circle Internet Financial, Boston, MA 02129, USA
[2]Seagate Technology, Singapore 139944
[3]Seagate Technology, Longmont, CO 80503, USA

Corresponding author: Vipin Singh Sehrawat (vipin.sehrawat.cs@gmail.com)

*Vipin Singh Sehrawat was with Seagate Technology, Fremont, CA 94538, USA at the time of this work.

ABSTRACT We introduce a novel method to derandomize the learning with errors (LWE) problem by generating deterministic yet sufficiently independent LWE instances that are constructed by using linear regression models, which are generated via (wireless) communication errors. We also introduce star-specific key-homomorphic (SSKH) pseudorandom functions (PRFs), which are defined by the respective sets of parties that construct them. We use our derandomized variant of LWE to construct a SSKH PRF family. The sets of parties constructing SSKH PRFs are arranged as star graphs with possibly shared vertices, i.e., the pairs of sets may have non-empty intersections. We reduce the security of our SSKH PRF family to the hardness of LWE. To establish the maximum number of SSKH PRFs that can be constructed — by a set of parties — in the presence of passive/active and external/internal adversaries, we prove several bounds on the size of maximally cover-free at most t-intersecting k-uniform family of sets $\mathcal{H}$, where the three properties are defined as: (i) k-uniform: $\forall A \in \mathcal{H} : |A| = k$, (ii) at most t-intersecting: $\forall A, B \in \mathcal{H}, B \neq A : |A \cap B| \leq t$, (iii) maximally cover-free: $\forall A \in \mathcal{H} : A \not\subseteq \bigcup_{\substack{B \in \mathcal{H} \\ B \neq A}} B$. For the same purpose, we define and compute the mutual information between different linear regression hypotheses that are generated from overlapping training datasets.

INDEX TERMS Extremal set theory, key-homomorphic PRFs, learning with errors, learning with linear regression, mutual information, physical layer communications.

I. INTRODUCTION

Derandomized LWE: The learning with errors (LWE) problem [1] is at the basis of multiple cryptographic constructions [2], [3]. Informally, LWE requires solving a system of 'approximate' linear modular equations. Given positive integers w and $q \geq 2$, an LWE sample is defined as: $(a, b = \langle a, s \rangle + e \bmod q)$, where $s \in \mathbb{Z}_q^w$ and $a \xleftarrow{\$} \mathbb{Z}_q^w$. The error term e is sampled randomly, typically from a normal distribution with standard deviation αq where $\alpha = 1/\mathsf{poly}(w)$, followed by which it is rounded to the nearest integer and reduced modulo q. Banerjee et al. [4] introduced a derandomized variant of LWE, called learning with rounding (LWR), wherein instead of adding a random small error, a *deterministically* rounded version of the sample is announced. Specifically, for some positive integer $p < q$, the elements of $\mathbb{Z}_q$ are divided into p contiguous intervals containing (roughly) q/p elements each. The rounding function, defined as: $\lfloor \cdot \rceil_p : \mathbb{Z}_q \to \mathbb{Z}_p$, maps the given input $x \in \mathbb{Z}_q$ into the index of the interval that x belongs to. An LWR instance is generated as: $(a, \lfloor \langle a, s \rangle \rceil_p)$ for vectors $s \in \mathbb{Z}_q^w$ and $a \xleftarrow{\$} \mathbb{Z}_q^w$. For certain range of parameters, Banerjee et al. proved the hardness of LWR under the LWE assumption. In this work, we propose a new derandomized variant of LWE, called learning with linear regression (LWLR). We reduce the hardness of LWLR to that of LWE for certain choices of parameters.

Physical Layer Communications and Shared Secret Extraction: In the OSI (Open Systems Interconnection)

The associate editor coordinating the review of this manuscript and approving it for publication was Yassine Maleh.

model,[1] physical layer consists of the fundamental hardware transmission technologies. It provides electrical, mechanical, and procedural interface to the transmission medium for transmitting raw bits over a communication channel. Physical layer communication between parties has certain inherent characteristics that make it an attractive source of renewable, shared secrecy. Multiple methods to extract secret bits from channel measurements have been explored (e.g., [6], [7], [8], [9], [10], [11], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21], [22], [23], [24], [25], [26], [27]). See [28] and [29] for an overview of some of the notable results in the area. *Channel reciprocity* simply means that the signal distortion (attenuation, delay, phase shift, and fading) is identical in both directions of a link. Hence, it follows from channel reciprocity that the two receive-nodes of a channel observe identical channel characteristic and state information. Secrecy of this information follows directly from the *spatial decorrelation* property, which states that in rich scattering environments, the receivers located at least half a wavelength away experience uncorrelated channels. Therefore, an eavesdropper separated by at least half a wavelength from the two communicating nodes experiences an entirely different channel, and hence cannot make accurate measurements. In typical cellular or wireles LAN frequencies, this distance — of half a wavelength — is less than half a foot, which is an acceptable assumption for separation from an eavesdropping adversary [13]. Both channel reciprocity and spatial decorrelation have been examined extensively and demonstrated to hold in practice [30], [31], [32], [33], [34], [35], [36]. For further details on these two properties of communication channels, we refer the interested reader to [37]. In this work, we use these two properties to securely generate sufficiently independent yet deterministic errors to derandomize LWE.

Cryptography From Physical/Hardware Properties: Apart from complexity/information-theoretic assumptions, security guarantees of cryptographic protocols can also be based on physical/hardware principles/properties. For instance, the physical principles of non-cloneability of quantum states [38], [39] and monogamy of entanglement [40] are at the heart of quantum cryptography [41], [42] — providing an ensemble of (quantum) cryptographic protocols, including quantum key distribution [43], [44], [45], quantum random number generator [46], closed group quantum digital signatures [47], long-term secure data storage [48] and quantum multiparty computation [49]. In classical, i.e., non-quantum, settings, physical/hardware principles/properties have been used to circumvent impossibility results, and efficiency and security bounds (e.g., [50], [51], [52], [53], [54], [55], [56], [57], [58], [59]). Furthermore, protocols based on physical properties or assumptions may offer qualitatively stronger security guarantees than the ones based on purely complexity-theoretic arguments/assumptions [60]. The subclass of such protocols that is related to a portion of our work concerns the so-called physically uncloneable functions (PUFs) which are cryptographic functions, defined over stateless hardware modules that implement/realize a function family with some threshold min-entropy output [61] (see [62] for the quantum analogue, called quantumPUF). Contrary to the standard digital systems, the output of a PUF depends on the unavoidably and sometimes purposefully included nanoscale structural disorders in the hardware which lead to a response behavior that cannot be cloned or reproduced exactly, not even by the hardware manufacturer. To capture their complex and disordered structure, formal definitions for PUFs often include requirements for one-wayness and unforgeability of output (typically against a probabilistic polynomial-time (PPT) adversary) [61], [63], [64], [65], [66], [67], [68], [69], [70] — which, in addition to deterministic behavior, are also the requirements for pseudorandom functions (PRFs).

In this work, our protocol relies on the inherent (random) channel errors occurring in physical layer communications over Gaussian channels with nonzero standard deviation. Known information theoretic arguments establish that channel communications always have an inherent random error component. Using mathematical proofs/arguments and statistical randomness tests such as the ones provided by the NIST [71] and Dieharder [72] test suites, channel randomness has been established with repsect to various channel characteristics, including received signal strength information [15], [16], [17], channel state information [11], [18] and phase shifts [19], [20].

Determinism From Probabilistic Events: Algorithmic information theory [73], [74] provides a fundamental measure of randomness of (finite) strings and (infinite) sequences in terms of their Kolmogorov complexity [75], [76], leading to the notions of algorithmic [73], [74] and c-Kolmogorov randomness [73]. Such formal notions of randomness have been used to establish that some (partially) deterministic procedures and events can lead to (pseudo/perfectly)random outcomes (e.g., see [77], [78], [79], [80], [81]). On the other hand, particle physics establishes that even-even nuclei demonstrate high degree of order in result of completely random interactions [82], [83], [84]. Outside of particle physics, approximating integer programs is an example problem for which probabilistic constructions lead to deterministic outcomes [85]. Our goal is similar in this work: we use probabilistic errors occurring in channel communications to generate a static and deterministic model $\mathcal{M}$, which can be used as a black box to generate deterministic errors (from target distributions) that are sufficiently independent — to a PPT adversary — due to the probabilistic nature of the channel errors.

Rounded Gaussians: Using discrete Gaussian elements to hide secrets is a common approach in lattice-based cryptography. The majority of digital methods for generating Gaussian random variables are based on transformations of uniform random variables [86]. Popular methods include Ziggurat [87], inversion [88], Wallace [89], and

[1] See Section 1.4.1 from [5] for an introduction to the OSI model.

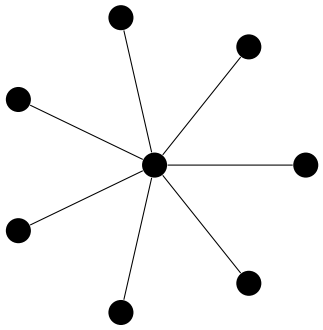

FIGURE 1. An example star graph, S_7.

Box-Muller [90]. Sampling discrete Gaussians can also be done by sampling from some continuous Gaussian distribution, followed by rounding the coordinates to nearby integers [90], [91], [92]. Using such rounded Gaussians can lead to better efficiency and, in some cases, better security guarantees for lattice-based cryptographic protocols [92]. In our work, we use rounded Gaussian errors that are derived from deterministic yet sufficiently independent samples from continuous Gaussians, which are themselves generated via our model $\mathcal{M}$.

Key-Homomorphic PRFs: In a PRF family [93], each function is specified by a key such that it can be evaluated deterministically given the key but appears to be a random function without the key. For a PRF F_k, the index k is called its key or seed. A PRF family F is called key-homomorphic if the set of keys has a group structure and there is an efficient algorithm that, given $F_{k_1}(x)$ and $F_{k_2}(x)$, outputs $F_{k_1 \oplus k_2}(x)$, where $\oplus$ is the group operation [94]. Multiple key-homomorphic PRF families have been constructed via varying approaches [94], [95], [96], [97], [98], [99]. In this work, we introduce and construct an extended variant of key-homomorphic PRFs, called star-specific key-homomorphic (SSKH) PRFs, which are defined for settings wherein parties constructing the PRFs are part of an interconnection network that can be (re)arranged as a graph comprised of only (undirected) star graphs with restricted vertex intersections. An undirected star graph S_k can be defined as a tree with one internal node and k leaves. Figure 1 depicts an example star graph, S_7, with seven leaves.

Henceforth, we use the terms star and star graph interchangeably.

Cover-Free Families With Restricted Intersections: Cover-free families were first defined by Kautz and Singleton in 1964 as superimposed binary codes [100]. They were motivated by investigating binary codes wherein disjunction of at most r ($\geq$ 2) codewords is distinct. In early 1980s, cover-free families were studied in the context of group testing [101] and information theory [102]. Erdös et al. called the corresponding set systems r-cover-free and studied their cardinality for $r = 2$ [103] and $r < n$ [104].

Definition 1 (r-cover-free Families [103], [104]): We say that a family of sets $\mathcal{H} = \{H_i\}_{i=1}^{\alpha}$ is r-cover-free for some integer $r < \alpha$ if there exists no $H_i \in \mathcal{H}$ such that:

$$H_i \subseteq \bigcup_{H_j \in \mathcal{H}^{(r)}} H_j,$$

where $\mathcal{H}^{(r)} \subset \mathcal{H}$ is some subset of $\mathcal{H}$ with cardinality r.

In addition to earlier applications to group testing [101] and information theory [102], cover-free families have found many applications in cryptography and communications, including blacklisting [105], broadcast encryption [106], [107], [108], [109], anti-jamming [110], source authentication in networks [111], group key predistribution [109], [112], [113], [114], compression schemes [115], fault-tolerant signatures [116], [117], [118], frameproof/traceability codes [119], [120], traitor tracing [121], modification localization on signed documents and redactable signatures [122], broadcast authentication [123], batch signature verification [124], and one-time and multiple-times digital signature schemes [125], [126].

In this work, we initiate the study of new variants of r-cover-free families. The motivation behind exploring this direction is to compute the maximum number of SSKH PRFs that can be constructed by overlapping sets of parties. We prove various bounds on the novel variants of r-cover-free families and later use them to establish the maximum number of SSKH PRFs that can be constructed by overlapping sets of parties in the presence of active/passive and internal/external adversaries.

A. OUR CONTRIBUTIONS

1) CRYPTOGRAPHIC CONTRIBUTIONS

We know that physical layer communications over Gaussian channels introduce independent Gaussian errors. Therefore, it is logical to wonder whether we can use some processed form of those Gaussian errors to generate deterministic yet sufficiently independent errors to derandomize LWE without losing its hardness. Such an ability would have direct applications to use cases wherein LWR is used to realize derandomized/deterministic LWE. Our algorithm to derandomize LWE uses channel communications over Gaussian channels as the training data for linear regression analysis, whose (optimal) hypothesis is used to generate a model $\mathcal{M}$ that can be used as a black box to compute deterministic yet sufficiently independent errors belonging to the desired Gaussian distributions. We round the resulting error to the nearest integer and reduce it modulo the LWE modulus to generate the final error. It is worth mentioning that many hardness proofs for LWE, including Regev's initial proof [1], used an analogous approach — without the linear regression component — to sample random "LWE errors" [1], [92], [127], [128]. We call our derandomized variant of LWE: learning with linear regression (LWLR). We prove that, for certain parameter choices, LWLR is as hard as LWE.

We introduce a new class of PRFs, called star-specific key-homomorphic (SSKH) PRFs, which are key-homomorphic

PRFs that are defined by the respective sets of parties that construct them. In our construction, the sets of parties are arranged as star graphs wherein the leaves represent the parties and edges denote communication channels between them. Each SSKH PRF is unique to the set/star of parties that constructs it. As an example application of LWLR, we replace LWR with LWLR in the LWR-based key-homomorphic PRF construction from [96] to construct the first SSKH PRF family. Due to their conflicting goals, statistical inference and cryptography are almost dual of each other. Given some data, statistical inference aims to identify the distribution that they belong to whereas in cryptography, the central aim is to design a distribution that is hard to predict. Interestingly, our work uses statistical inference to construct novel a cryptographic tool. In addition to the known applications of key-homomorphic PRFs — as given in [95] and [129] — our SSKH PRF family also allows collaborating parties to securely generate pseudorandom nonce/seed without relying on any pre-provisioned secrets; hence supporting applications such as interactive key generation over unauthenticated channels.

2) MUTUAL INFORMATION BETWEEN LINEAR REGRESSION MODELS

To quantify the relation between different SSKH PRFs, we examine the mutual information between different linear regression hypotheses that are generated via (training) datasets with overlapping data points. A higher mutual information translates into a stronger relation between the corresponding SSKH PRFs, that are generated via those linear regression hypotheses. The following text summarizes the main result that we prove in this context.

Suppose, for $i = 1, 2, \ldots, \ell$, we have:

$$y_i \sim \mathcal{N}(\alpha + \beta x_i, \sigma^2) \quad \text{and} \quad z_i \sim \mathcal{N}(\alpha + \beta w_i, \sigma^2),$$

with $x_i = w_i$ for $i = 1, \ldots, a$. Let $h_1(x) = \hat{\alpha}_1 x + \hat{\beta}_1$ and $h_2(w) = \hat{\alpha}_2 w + \hat{\beta}_2$ be the linear regression hypotheses obtained from the samples (x_i, y_i) and (w_i, z_i), respectively. We introduce the following notations:

- $X_1 = \sum_{i=1}^{\ell} x_i$, $X_2 = \sum_{i=1}^{\ell} x_i^2$,
- $W_1 = \sum_{i=1}^{\ell} w_i$, $W_2 = \sum_{i=1}^{\ell} w_i^2$,
- $C_1 = \sum_{i=1}^{a} x_i = \sum_{i=1}^{a} w_i$,
- $C_2 = \sum_{i=1}^{a} x_i^2 = \sum_{i=1}^{a} w_i^2$,
- $C_3 = \sum_{i=1}^{\ell} \sum_{j=1, j\neq i}^{\ell} x_i x_j$,
- $\Delta = \ell C_2 - 2C_1 X_1 + a X_2$,
- $\mho = \ell C_2 - 2C_1 W_1 + a W_2$,
- $\aleph = (a-1)C_2 - C_3$.

Theorem 1: The mutual information between $(\hat{\alpha_1}, \hat{\beta_1})$ *and* $(\hat{\alpha_2}, \hat{\beta_2})$ *is:*

$$I((\hat{\alpha_1}, \hat{\beta_1}); (\hat{\alpha_2}, \hat{\beta_2})) = -\frac{1}{2}\log\left(1 - \frac{\Delta\mho}{(\ell X_2 - X_1^2)(\ell W_2 - W_1^2)} + \frac{\aleph(\aleph + \ell(X_2 + W_2) - 2X_1 W_1)}{(\ell X_2 - X_1^2)(\ell W_2 - W_1^2)}\right).$$

3) BOUNDS ON t-INTERSECTING MAXIMALLY COVER FREE FAMILIES

Since we use physical layer communications to generate derandomized LWE instances, a large enough overlap among different sets of parties/devices can lead to reduced collective and conditional entropy for the SSKH PRFs constructed by those sets.

We say that a set system $\mathcal{H}$ is (i) k-uniform if: $\forall A \in \mathcal{H} : |A| = k$, (ii) at most t-intersecting if: $\forall A, B \in \mathcal{H}, B \neq A : |A \cap B| \leq t$.

Definition 2 (Maximally Cover-free Families): A family of sets $\mathcal{H}$ is *maximally* cover-free if it holds that:

$$\forall A \in \mathcal{H} : A \not\subseteq \bigcup_{\substack{B \in \mathcal{H} \\ B \neq A}} B.$$

It follows trivially that if the sets of parties — each of which is arranged as a star — belong to a maximally cover-free family, then no SSKH PRF can have zero conditional entropy since each set/star of parties must have at least one member that is exclusive to it. We know from Theorem 1 that based on the overlap in training data, we can compute the mutual information between different linear regression hypotheses. Since the training data for a set/star of parties performing linear regression analysis is simply their mutual communications, it follows that the mutual information between any two SSKH PRFs increases with the overlap between the sets of parties that construct them. Hence, given a maximum mutual information threshold, Theorem 1 can be used to compute the maximum acceptable overlap between different sets of parties. To establish the maximum number of SSKH PRFs that can be constructed by such overlapping sets, we revisit and extend the notion of cover-free families. Based on our requirements, we focus on the following two cases:

- $\mathcal{H}$ is at most t-intersecting and k-uniform,
- $\mathcal{H}$ is maximally cover-free, at most t-intersecting and k-uniform.

We derive multiple bounds on the size of $\mathcal{H}$ for both these cases and later use them to establish the maximum number of SSKH PRFs that can be constructed securely against active/passive and internal/external adversaries. The following theorem captures our central results on cover-free families.

Theorem 2: Let $k, t \in \mathbb{Z}^+$, *and* $C < 1$ *be any positive real number.*

1) *Suppose* $t < k - 1$. *Then, for all sufficiently large* N, *the maximum size* $\nu(N, k, t)$ *of a maximally cover-free, at most* t*-intersecting and* k*-uniform family* $\mathcal{H} \subseteq 2^{[N]}$ *satisfies*

$$CN \leq \nu(N, k, t) < N.$$

2) *Suppose $t < k$. Then, for all sufficiently large n, the maximum size $\varpi(n,k,t)$ of an at most t-intersecting and k-uniform family $\mathcal{H} \subseteq 2^{[n]}$ satisfies*

$$\frac{Cn^{t+1}}{k(k-1)\cdots(k-t)} \leq \varpi(n,k,t) < \frac{n^{t+1}}{k(k-1)\cdots(k-t)}.$$

In particular:

$$\nu(N,k,t) \sim N \text{ and } \varpi(n,k,t) \sim \frac{n^{t+1}}{k(k-1)\cdots(k-t)}.$$

We also provide an explicit construction for at most t-intersecting and k-uniform set systems.

4) MAXIMUM NUMBER OF SSKH PRFs

We use the results from Theorems 1 and 2 to derive the maximum number, ζ, of SSKH PRFs that can be constructed securely against various adversaries (modeled as PPT Turing machines). Specifically, we prove the following:

- For an external/eavesdropping adversary with oracle access to the SSKH PRF family, we get:

$$\zeta \sim \frac{n^k}{k!}.$$

- For non-colluding semi-honest parties, we get:

$$\zeta \geq Cn,$$

where $C < 1$ is a positive real number.

We also establish the ineffectiveness of the man-in-the-middle attack against our SSKH PRF construction.

B. ORGANIZATION

The rest of the paper is organized as follows: Section II recalls the concepts and constructs that are relevant to our solutions and constructions. Section III reviews the related work. Section IV gives a formal definition of SSKH PRFs. We prove various bounds on maximally cover-free, at most t-intersecting and k-uniform families in Section V. In Section VI, we present our protocol for generating the desired Gaussian errors from physical layer communications. The section also discusses the implementation, simulation, test results, error analysis, and complexity for our protocol. In Section VII, we analyze the mutual information between different linear regression hypotheses that are generated from overlapping training datasets. In Section VIII, we define LWLR and construct LWLR instances. In the same section, we reduce the hardness of LWLR to that of LWE. In Section IX, we use LWLR to adapt the key-homomorphic PRF construction from [96] to construct the first SSKH PRF family, and prove its security under the hardness of LWLR (and therefore that of LWE). In the same section, we use our results from Section V, and Section VII to establish the maximum number of SSKH PRFs that can be constructed by a given set of parties in the presence of active/passive and external/internal adversaries. Section X gives the conclusion.

II. PRELIMINARIES

For a positive integer n, let: $[n] = \{1, \ldots, n\}$. As mentioned earlier, we use the terms star and star graph interchangeably. For a vector $\mathbf{v} = (v_1, v_2, \ldots, v_w) \in \mathbb{R}^w$, the Euclidean and infinity norms are defined as: $||\mathbf{v}|| = \sqrt{(\sum_{i=1}^{w} v_i^2)}$ and $||\mathbf{v}||_\infty = \max(|v_1|, |v_2|, \ldots, |v_w|)$, respectively. In this text, vectors and matrices are denoted by bold lower case letters and bold upper case letters, respectively. We say that an algorithm is efficient if its running time is polynomial in its input size.

Definition 3: The probability density function (p.d.f.) of a continuous random variable X with support S is an integrable function f_X such that following conditions hold:

- $\forall x \in S : f_X(x) > 0$,
- $\int_S f_X(x)dx = 1$,
- $\Pr[X \in \Im] = \int_{\Im} f_X(x)dx$.

Definition 4: The probability mass function (p.m.f.) p_X of a discrete random variable X with support S is a function for which the following hold:

- $\forall x \in S : \Pr[X = x] = p_X(x) > 0$,
- $\sum_{x \in S} p_X(x) = 1$,
- $\Pr[X \in \Im] = \sum_{x \in \Im} p_X(x)$.

A. ENTROPY

The concept of entropy was originally introduced as a thermodynamic construct by Rankine in 1850 [130]. It was later adapted to information theory by Shannon [131] as a measure of the uncertainty associated with a random variable. Hence, (information) entropy is defined as a measure of the average information content that is missing when value of a random variable is not known.

Definition 5: For a finite set $\mathcal{S} = \{s_1, s_2, \ldots, s_n\}$ with probabilities $p_1, p_2, \ldots, p_n$, respectively, the entropy of the probability distribution over $\mathcal{S}$ is defined as:

$$H(\mathcal{S}) = \sum_{i=1}^{n} p_i \log \frac{1}{p_i}.$$

B. LATTICES

A lattice Λ of $\mathbb{R}^w$ is defined as a discrete subgroup of $\mathbb{R}^w$. In cryptography, we are interested in integer lattices, i.e., $\Lambda \subseteq \mathbb{Z}^w$. Given w-linearly independent vectors $b_1, \ldots, b_w \in \mathbb{R}^w$, a basis of the lattice generated by them can be represented as the matrix $\mathbf{B} = (b_1, \ldots, b_w) \in \mathbb{R}^{w \times w}$. The lattice generated by $\mathbf{B}$ is the following set of vectors:

$$\Lambda(B) = \left\{ \sum_{i=1}^{w} c_i b_i : c_i \in \mathbb{Z} \right\}.$$

Historically, lattices received attention from several mathematicians, including Lagrange, Gauss, Dirichlet, Hermite, Korkine-Zolotareff, and Minkowski (see [132], [133], [134], [135], [136], [137]). Problems in lattices have been of interest to cryptographers since 1997, when Ajtai and Dwork [138]

proposed a lattice-based public key cryptosystem following Ajtai's [139] seminal worst-case to average-case reductions for lattice problems. In lattice-based cryptography, *q-ary* lattices are of particular interest; they satisfy the following condition:

$$q\mathbb{Z}^w \subseteq \Lambda \subseteq \mathbb{Z}^w,$$

for some (possibly prime) integer q. In other words, the membership of a vector x in Λ is determined by x mod q. Given a matrix $A \in \mathbb{Z}_q^{w\times n}$ for some integers q, w, n, we can define the following two n-dimensional *q-ary* lattices,

$$\Lambda_q(A) = \{y \in \mathbb{Z}^n : y = A^T s \bmod q \text{ for some } s \in \mathbb{Z}^w\},$$
$$\Lambda_q^{\perp}(A) = \{y \in \mathbb{Z}^n : Ay = 0 \bmod q\}.$$

The first *q-ary* lattice is generated by the rows of A while the second contains all vectors that are orthogonal (modulo q) to the rows of A. Hence, the first *q-ary* lattice, $\Lambda_q(A)$, corresponds to the code generated by the rows of A whereas the second, $\Lambda_q^{\perp}(A)$, corresponds to the code whose parity check matrix is A. For a complete introduction to lattices, we refer the interested reader to the monographs by Grätzer [140], [141].

C. GAUSSIAN DISTRIBUTIONS

Gaussian sampling is an extremely useful tool in lattice-based cryptography. Introduced by Gentry et al. [142], Gaussian sampling takes a short basis B of a lattice Λ and an arbitrary point v as inputs and outputs a point from a Gaussian distribution discretized on the lattice points and centered at v. Gaussian sampling does not leak any information about the lattice Λ. It has been used directly to construct multiple cryptographic schemes, including hierarchical identity-based encryption [143], [144], standard model signatures [143], [145], and attribute-based encryption [146]. In addition, Gaussian sampling/distribution also plays an important role in other hard lattice problems, such as, learning single periodic neurons [147], and has direct connections to standard lattice problems [148], [149], [150].

Definition 6: A continuous Gaussian distribution, $\mathcal{N}^w(v, \sigma^2)$, over $\mathbb{R}^w$, centered at some $\mathbf{v} \in \mathbb{R}^w$ with standard deviation σ is defined for $x \in \mathbb{R}^w$ as the following density function:

$$\mathcal{N}_x^w(v, \sigma^2) = \left(\frac{1}{\sqrt{2\pi\sigma^2}}\right)^w \exp\left(\frac{-||x-v||^2}{2\sigma^2}\right).$$

A rounded Gaussian distribution can be obtained by simply rounding the samples from a continuous Gaussian distribution to their nearest integers. Rounded Gaussians have been used to establish hardness of LWE [1], [127], [128] — albeit not as frequently as discrete Gaussians.

Definition 7 (Adapted from [92]): A rounded Gaussian distribution, $\Psi^w(v, \hat{\sigma}^2)$, over $\mathbb{Z}^w$, centered at some $v \in \mathbb{Z}^w$ with parameter σ is defined for $x \in \mathbb{Z}^w$ as:

$$\Psi_x^w(v, \hat{\sigma}^2) = \int_{A_x} \mathcal{N}_s^w(v, \sigma^2)\, ds$$
$$= \int_{A_x} \left(\frac{1}{\sqrt{2\pi\sigma^2}}\right)^w \exp\left(\frac{-||s-v||^2}{2\sigma^2}\right) ds,$$

where A_x denotes the region $\prod_{i=1}^w [x_i - \frac{1}{2}, x_i + \frac{1}{2})$; $\hat{\sigma}$ and σ are the standard deviations of the rounded Gaussian and its underlying continuous Gaussian, respectively, such that $\hat{\sigma} = \sqrt{\sigma^2 + 1/12}$.

Definition 8 (Gaussian channel): A Gaussian channel is a discrete-time channel with input x_i and output $y_i = x_i + \varepsilon_i$, where ε_i is drawn i.i.d. from a Gaussian distribution $\mathcal{N}(0, \sigma^2)$, with mean 0 and standard deviation σ, which is assumed to be independent of the signal x_i.

Definition 9 (Gram-Schmidt norm): Let $B = (b_i)_{i\in[w]}$ be a finite basis, and $\widetilde{B} = (\tilde{b}_i)_{i\in[w]}$ be its Gram-Schmidt orthogonalization. Then, Gram-Schmidt norm of B is defined as:

$$||B||_{GS} = \max_{i\in[w]} ||\tilde{b}_i||.$$

For an introduction to Gram-Schmidt orthogonalization, see [151].

Definition 10 (Discrete Gaussian over Lattices): Given a lattice $\Lambda \in \mathbb{Z}^w$, the discrete Gaussian distribution over Λ with standard deviation $\sigma \in \mathbb{R}$ and center $v \in \mathbb{R}^w$ is defined as:

$$D(\Lambda, v, \sigma^2)_x = \frac{\rho_x(v, \sigma^2)}{\rho_\Lambda(v, \sigma^2)};\ \forall x \in \Lambda,$$

where $\rho_\Lambda(v, \sigma^2) = \sum_{x_i\in\Lambda} \rho_{x_i}(v, \sigma^2)$ and

$$\rho_x(v, \sigma^2) = \exp\left(-\frac{||x-v||^2}{2\sigma^2}\right).$$

The smoothing parameter is defined as a measure of the "difference" between discrete and standard Gaussians, that are defined over identical parameters. Informally, it is the smallest σ required by a discrete Gaussian distribution, over a lattice Λ, to behave like a continuous Gaussian — up to some acceptable statistical error. For more details, see [152] and [153]. Various methods such as computing the cumulative density function, taking convolutions of smaller deviation discrete Gaussians, and rejection/Bernoulli/Binomial/Ziggurat/Knuth-Yao/CDT (cumulative distribution table) sampling have been employed to efficiently sample from discrete Gaussians for lattice-based cryptography [154], [155], [156], [157], [158], [159], [160], [161], [162], [163], [164], [165], [166], [167], [168], [169], [170], [171], [172].

Theorem 3 (Drowning/Smudging [173]): Let $\sigma > 0$ and $y \in \mathbb{Z}$. The statistical distance between $\Psi(v, \sigma^2)$ and $\Psi(v, \sigma^2) + y$ is at most $|y|/\sigma$.

Typically, in lattice-based cryptography, drowning/smudging is used to hide some information by introducing a sufficiently large random noise — with large standard deviation — such that the resulting distribution is, to the desired degree, independent of the information that needs to be hidden [4], [127], [173], [174], [175], [176], [177], [178],

[179], [180], [181]. However, in our work, we do not use it for that purpose; instead, we use it argue about the insignificance of a small component of the total error.

D. LEARNING WITH ERRORS

The learning with errors (LWE) problem [1] is at the center of the majority of lattice-based cryptographic constructions [2]. LWE is known to be hard based on the worst-case hardness of standard lattice problems such as GapSVP (decision version of the Shortest Vector Problem) and SIVP (Shortest Independent Vectors Problem) [1], [182]. Multiple variants of LWE such as ring LWE [183], module LWE [184], cyclic LWE [185], continuous LWE [186], **PRIM LWE** [187], middle-product LWE [188], group LWE [189], entropic LWE [190], universal LWE [191], and polynomial-ring LWE [192] have been developed since 2010. Many versatile cryptosystems rely on the hardness of LWE [2], [193], [194].

Definition 11 (Decision-LWE [1]): For positive integers w and $q \geq 2$, and an error (probability) distribution χ over $\mathbb{Z}$, the decision-LWE$_{w,q,\chi}$ problem is to distinguish between the following pairs of distributions:

$$((a_i, \langle a_i, s\rangle + e_i \bmod q))_i \quad \text{and} \quad ((a_i, u_i))_i,$$

where $i \in [\mathsf{poly}(w)]$, $a_i \xleftarrow{\$} \mathbb{Z}_q^w$, $s \in \mathbb{Z}_q^w$, $e_i \leftarrow \chi$, and $u_i \xleftarrow{\$} \mathbb{Z}_q$.

Regev [1] showed that for certain noise distributions and a sufficiently large q, the LWE problem is as hard as the worst-case SIVP and GapSVP problems under a quantum reduction (see [156], [182], [195] for other reductions). Standard instantiations of LWE assume χ to be a rounded or discrete Gaussian distribution. Regev's proof requires $\alpha q \geq 2\sqrt{w}$ for "noise rate" $\alpha \in (0, 1)$. These results were extended by Applebaum et al. [196] to show that the fixed secret s can be sampled from a low norm distribution. Specifically, they showed that sampling s from the noise distribution χ does not weaken the hardness of LWE. Later, Micciancio and Peikert discovered that a simple low-norm distribution also works as χ [197].

E. PSEUDORANDOM FUNCTIONS

In a pseudorandom function (PRF) family [93], each function is specified by a key such that it can be evaluated deterministically with the key but behaves like a random function without it. Here, we recall the formal definition of a PRF family. Recall that an ensemble of probability distributions is a sequence $\{X_n\}_{n\in\mathbb{N}}$ of probability distributions.

Definition 12 (Negligible Function): For security parameter L, a function $\eta(\mathsf{L})$ is called *negligible* if for all $c > 0$, there exists a L_0 such that $\eta(\mathsf{L}) < 1/\mathsf{L}^c$ for all $\mathsf{L} > \mathsf{L}_0$.

Definition 13 (Computational Indistinguishability [198]): Let $X = \{X_\lambda\}_{\lambda\in\mathbb{N}}$ and $Y = \{Y_\lambda\}_{\lambda\in\mathbb{N}}$ be ensembles, where X_λ's and Y_λ's are probability distributions over $\{0,1\}^{\kappa(\lambda)}$ for $\lambda \in \mathbb{N}$ and some polynomial $\kappa(\lambda)$. We say that $\{X_\lambda\}_{\lambda\in\mathbb{N}}$ and $\{Y_\lambda\}_{\lambda\in\mathbb{N}}$ are polynomially/computationally indistinguishable if the following holds for every (probabilistic) polynomial-time algorithm $\mathcal{D}$ and all $\lambda \in \mathbb{N}$:

$$\Big|\Pr[t \leftarrow X_\lambda : \mathcal{D}(t) = 1] - \Pr[t \leftarrow Y_\lambda : \mathcal{D}(t) = 1]\Big| \leq \eta(\lambda),$$

where η is a negligible function.

Remark 1 (Perfect Indistinguishability): We say that $\{X_\lambda\}_{\lambda\in\mathbb{N}}$ and $\{Y_\lambda\}_{\lambda\in\mathbb{N}}$ are perfectly indistinguishable if the following holds for all t:

$$\Pr[t \leftarrow X_\lambda] = \Pr[t \leftarrow Y_\lambda].$$

We consider adversaries interacting as part of probabilistic experiments called games. For an adversary $\mathcal{A}$ and two games $\mathfrak{G}_1, \mathfrak{G}_2$ with which it can interact, $\mathcal{A}'s$ distinguishing advantage is:

$$Adv_{\mathcal{A}}(\mathfrak{G}_1, \mathfrak{G}_2) := \Big|\Pr[\mathcal{A} \vdash\!\dashv \mathfrak{G}_1] - \Pr[\mathcal{A} \vdash\!\dashv \mathfrak{G}_2]\Big|,$$

where $\mathcal{A} \vdash\!\dashv \mathfrak{G}$ denotes that $\mathcal{A}$ accepts in $\mathfrak{G}$. For the security parameter L, the two games are said to be computationally indistinguishable if it holds that:

$$Adv_{\mathcal{A}}(\mathfrak{G}_1, \mathfrak{G}_2) \leq \eta(\mathsf{L}),$$

where η is a negligible function.

Definition 14 (PRF): Let A and B be finite sets, and let $\mathcal{F} = \{F_k : A \to B\}$ be a function family, endowed with an efficiently sampleable distribution (more precisely, $\mathcal{F}, A$, and B are all indexed by the security parameter L). We say that $\mathcal{F}$ is a PRF family if the following two games are computationally indistinguishable:

(i) Choose a function $F_k \in \mathcal{F}$ and give the adversary adaptive oracle access to F_k.
(ii) Choose a uniformly random function $U : A \to B$ and give the adversary adaptive oracle access to U.

Hence, PRF families are efficient distributions of functions that cannot be efficiently distinguished from the uniform distribution. For a PRF $F_k \in \mathcal{F}$, the index k is called its key/seed. PRFs have a wide range of applications, most notably in cryptography, but also in computational complexity and computational learning theory. For a detailed introduction to PRFs and review of the noteworthy results, we refer the interested reader to the survey by Bogdanov and Rosen [199].

F. LINEAR REGRESSION

Linear regression is a linear approach to model relationship between a dependent variable and explanatory/independent variable(s). As is the case with most statistical analysis, the goal of regression is to make sense of the observed data in a useful manner. It analyzes the training data and attempts to model the relationship between the dependent and explanatory/independent variable(s) by fitting a linear equation to the observed data. These predictions (often) have errors, which cannot be predicted accurately [200], [201]. For linear regression, the mean and variance functions are defined as:

$$\mathsf{E}(Y|X = x) = \beta_0 + \beta_1 x \quad \text{and} \quad \mathrm{var}(Y|X = x) = \sigma^2,$$

respectively, where $\mathsf{E}(\cdot)$ and σ denote the expected value and standard deviation, respectively; β_0 represents the intercept, which is the value of $\mathsf{E}(Y|X = x)$ when x equals zero; β_1 denotes the slope, i.e., the rate of change in $\mathsf{E}(Y|X = x)$ for a unit change in X. The parameters β_0 and β_1 are also known as *regression coefficients*.

For any regression model, the observed value y_i might not always equal its expected value $\mathsf{E}(Y|X = x_i)$. This difference between the observed data and the expected value is called statistical error, and is defined as:

$$\epsilon_i = y_i - \mathsf{E}(Y|X = x_i).$$

For linear regression, errors are random variables that correspond to the vertical distance between the point y_i and the mean function $\mathsf{E}(Y|X = x_i)$. Depending on the type and size of the training data, different algorithms such as gradient descent and least squares may be used to compute the values of β_0 and β_1. In this paper, we employ least squares linear regression to estimate the values of β_0 and β_1, and generate the optimal hypothesis for the target function. Due to the inherent error in all regression models, it holds that:

$$h(x) = f(x) + \varepsilon_x,$$

where $h(x)$ is the (optimal) hypothesis of the linear regression model, $f(x)$ is the target function and ε_x is the total (reducible + irreducible) error at point x.

G. INTERCONNECTION NETWORK

In an interconnection network, each device is independent and connects with other devices via point-to-point links, which are two-way communication lines. Therefore, an interconnection network can be modeled as an undirected graph $G = (V, E)$, where each device is a vertex in V and edges in E represent communication lines/channels between the devices. Next, we recall some basic definitions/notations for undirected graphs.

Definition 15: The degree $\deg(v)$ of a vertex $v \in V$ is the number of adjacent vertices it has in a graph G. The degree of a graph G is defined as: $\deg(G) = \max_{v \in V}(\deg(v))$.

If $\deg(v_i) = \deg(v_j)$ for all $v_i, v_j \in V$, then G is called a regular graph. Since it is easy to construct star graphs that are hierarchical, vertex edge symmetric, maximally fault tolerant, and strongly resilient along with having other desirable properties such as small(er) degree, diameter, genus and fault diameter [202], [203], networks of star graphs are well-suited to model interconnection networks. For a detailed introduction to interconnection networks, we refer the interested reader to the comprehensive book by Duato et al. [204].

H. SOME USEFUL RESULTS

Here, we recall two useful, elementary results from probability theory.

Definition 16 (Chebyshev inequality [205], [206]): Let X be a random variable with mean μ and variance $\mathrm{var}(X) = \sigma^2$. Then, the following holds for all $\varsigma > 0$:

$$\Pr[|X - \mu| \geq \varsigma] \leq \frac{\sigma^2}{\varsigma^2}.$$

Definition 17 (The Union Bound [207]): For any random events $A_1, A_2, \ldots, A_n$, it holds that:

$$\Pr\left(\bigcup_{i=1}^{n} A_i\right) \leq \sum_{i=1}^{n} \Pr(A_i).$$

Let $X_1, X_2, \ldots, X_n$ be i.i.d. random variables from the same distribution, i.e., all X_i's have the same mean μ and standard deviation σ. Let random variable $\overline{X}_n$ be the average of $X_1, \ldots, X_n$. Then, $\overline{X}_n$ converges almost surely to μ as $n \to \infty$.

III. RELATED WORK

A. LEARNING WITH ROUNDING

Naor and Reingold [208] introduced synthesizers to construct PRFs via a hard-to-learn deterministic function. The obstacle in using LWE as the hard learning problem in their synthesizers is that the hardness of LWE relies directly on random errors. In fact, without the error, LWE becomes a trivial problem, that can be solved via Gaussian elimination. Therefore, in order to use these synthesizers for constructing LWE-based PRFs, there was a need to replace the random errors with deterministic yet sufficiently independent errors such that the hardness of LWE is not (significantly) weakened. Banerjee et al. [4] addressed this problem by introducing the learning with rounding (LWR) problem, wherein instead of adding a small random error, as done in LWE, a deterministically rounded version of the sample is generated. For $q \geq p \geq 2$, the rounding function, $\lfloor \cdot \rceil_p : \mathbb{Z}_q \to \mathbb{Z}_p$, is defined as:

$$\lfloor x \rceil_p = \left\lfloor \frac{p}{q} \cdot x \right\rceil,$$

i.e., if $\lfloor x \rceil_p = y$, then $y \cdot \lfloor q/p \rceil$ is the integer multiple of $\lfloor q/p \rceil$ that is nearest to x. Hence, the error in LWR originates from deterministically rounding x to a (relatively) nearby value in $\mathbb{Z}_p$.

Definition 18 (LWR Distribution [4]): Let $q \geq p \geq 2$ be positive integers, then: for a vector $s \in \mathbb{Z}_q^w$, LWR distribution L_s is defined to be a distribution over $\mathbb{Z}_q^w \times \mathbb{Z}_p$ that is obtained by choosing a vector $a \xleftarrow{\$} \mathbb{Z}_q^w$ and outputting $(a, b = \lfloor \langle a, s \rangle \rceil_p)$.

For a given distribution over $s \in \mathbb{Z}_q^w$ (e.g., the uniform distribution), the decision-LWR$_{w,q,p}$ problem is to distinguish (with advantage non-negligible in w) between some fixed number of independent samples $(a_i, b_i) \leftarrow L_s$, and the same number of samples drawn uniformly from $\mathbb{Z}_q^w \times \mathbb{Z}_p$. Banerjee et al. proved decision-LWR to be as hard as decision-LWE for a setting of parameters where the modulus and modulus-to-error ratio are superpolynomial in the security parameter [4]. Alwen et al. [209], Bogdanov et al. [210], and Bai et al. [211] made further improvements on the range

of parameters and hardness proofs for LWR. LWR has been used to construct pseudorandom generators/functions [4], [95], [96], [212], [213], [214], and probabilistic [215], [216] and deterministic [217] encryption schemes.

As mentioned earlier, hardness reductions of LWR hold for superpolynomial approximation factors over worst-case lattices. Montgomery [218] partially addressed this issue by introducing a new variant of LWR, called Nearby Learning with Lattice Rounding problem, which supports unbounded number of samples and polynomial (in the security parameter) modulus.

B. LWR/LWE-BASED KEY-HOMOMORPHIC PRFs

Since LWR allows generating derandomized/deterministic LWE instances, it can be used as the hard-to-learn deterministic function in Naor and Reingold's synthesizers, and hence, construct LWE-based PRF families for specific parameters. Due to the indispensable small error, LWE-based key-homomorphic PRFs only achieve what is called 'almost homomorphism' [95].

Definition 19 (Key-homomorphic PRF [95]): Let $F : \mathcal{K} \times \mathcal{X} \to \mathbb{Z}_q^w$ be an efficiently computable function such that $(\mathcal{K}, \oplus)$ is a group. We say that the tuple $(F, \oplus)$ is a γ-almost key-homomorphic PRF if the following two properties hold:

(i) F is a secure PRF,
(ii) for all $k_1, k_2 \in \mathcal{K}$ and $x \in \mathcal{X}$, there exists $e \in [0, \gamma]^w$ such that:

$$F_{k_1}(x) + F_{k_2}(x) = F_{k_1 \oplus k_2}(x) + e \bmod q.$$

Multiple key-homomorphic PRF families have been constructed via varying approaches [94], [95], [96], [97], [98], [99], [212].

IV. SSKH PRF: DEFINITION

For any two sets X and Y, let $\texttt{PartFunc}(X, Y)$ denote the space of partial functions from X to Y.

Definition 20: An efficient randomized algorithm $\mathfrak{A} : \Re \to \texttt{PartFunc}(\mathbb{Z}, \mathbb{Z})$ is probabilistic to static-independent (P2SI) if it takes some random $r \in \Re$ (chosen according to some fixed probability distribution on $\Re$) as input, and outputs a deterministic function $\mathfrak{M}_r : \mathcal{X}_r \to \mathbb{Z}$, where $\mathcal{X}_r \subseteq \mathbb{Z}$, such that, for all $x_i, x_j \in \mathbb{Z}$ with $x_i \neq x_j$:

1) the probability distributions of $\mathfrak{M}_r(x_i)$ (taken with respect to the randomness $r \in \Re$ such that $x_i \in \mathcal{X}_r$) and $\mathfrak{M}_r(x_j)$ are both computationally indistinguishable from rounded Gaussians with the same parameters,
2) the following quantities are equal up to a negligible function:
   - $H[\mathfrak{M}_r(x_i) \mid \mathfrak{M}_r(x_j)]$,
   - $H[\mathfrak{M}_r(x_j) \mid \mathfrak{M}_r(x_i)]$,
   - $H[\mathfrak{M}_r(x_i)]$,
   - $H[\mathfrak{M}_r(x_j)]$.

Next, we define a star-specific key-homomorphic (SSKH) PRF family. Let $G = (V, E)$ be a graph, representing an interconnection network, containing multiple star graphs

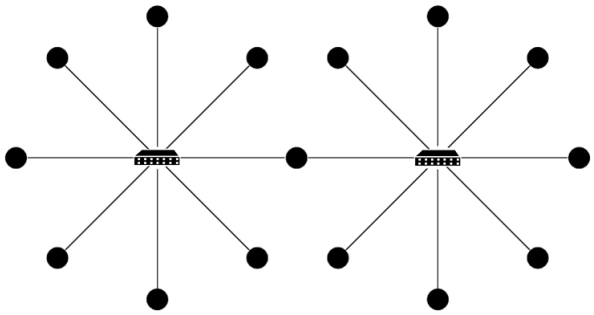

FIGURE 2. An example interconnection graph.

wherein the leaves of each star graph, ∂, represent unique parties and the root represents a central hub that broadcasts messages to all leaves/parties in ∂. Different star graphs may have arbitrary numbers of shared leaves. Henceforth, we call such a graph an *interconnection graph*. Figure 2 depicts a simple interconnection graph with two star graphs, each containing one central hub, respectively, along with eight parties/leaves out of which one leaf is shared by both star graphs. Note that an interconnection graph can also be viewed as a bipartite graph with its vertices partitioned into two disjoint subsets, $V_1, V_2 \subset V$, wherein the vertices in V_1 and V_2 represent the central hubs and parties, respectively.

Definition 21: Let graph $G = (V, E)$ be an interconnection graph with a set of vertices V and a set of edges E. Let there be ρ star graphs $\partial_1, \ldots, \partial_\rho$ in G. Let $\mathcal{F} = \left(F^{(\partial_i)}\right)_{i=1,\ldots,\rho}$ be a family of PRFs, where, for each i, $F^{(\partial_i)} : \mathcal{K} \times \mathcal{X} \to \mathbb{Z}_q^w$ with $(\mathcal{K}, \oplus)$ a group. Then, we say that the tuple $(\mathcal{F}, \oplus)$ is a star-specific (δ, γ, p)-almost key-homomorphic PRF family if the following two conditions hold:

1) for all $\partial_i \neq \partial_j$ $(i, j \in [\rho])$, $k \in \mathcal{K}$ and $x \in \mathcal{X}$, it holds that:

$$\Pr[F_k^{(\partial_i)}(x) = F_k^{(\partial_j)}(x)] \leq \delta^w + \eta(\mathsf{L}),$$

   where $F_k^{(\partial)}(x)$ denotes the PRF computed by parties in star graph $\partial \subseteq V(G)$ on input $x \in \mathcal{X}$ and key $k \in \mathcal{K}$, and $\eta(\mathsf{L})$ is a negligible function in the security parameter L,
2) for all $k_1, k_2 \in \mathcal{K}$ and $x \in \mathcal{X}$, there exists a vector $e = (e_1, \ldots, e_w)$ satisfying:

$$F_{k_1}^{(\partial)}(x) + F_{k_2}^{(\partial)}(x) = F_{k_1 \oplus k_2}^{(\partial)}(x) + e \bmod q,$$

   such that for all $a \in [w]$, it holds that:

$$\Pr[-\gamma \leq e_a \leq \gamma] \geq p.$$

V. MAXIMALLY COVER-FREE AT MOST t-INTERSECTING k-UNIFORM FAMILIES

Extremal combinatorics deals with the problem of determining or estimating the maximum or minimum cardinality of a collection of finite objects that satisfies some specific set of requirements. It is also concerned with the investigation of inequalities between combinatorial invariants, and questions

dealing with relations among them. For an introduction to the topic, we refer the interested reader to the books by Jukna [219] and Bollobás [220], and the surveys by Alon [221], [222], [223], [224]. In this work, we focus on extremal (finite) set theory, which concerns with determining the size of set-systems that satisfy certain restrictions. It was first investigated by Sperner [225] in 1928 by establishing the maximum size of an antichain, i.e., a set-system where no member is a superset of another. However, it was Erdős et al. [226] who started systematic research in extremal set theory. It is one of the most rapidly developing areas in combinatorics, with applications in various other branches of mathematics and theoretical computer science, including functional analysis, probability theory, circuit complexity, cryptography, coding theory, probabilistic methods, discrete geometry, linear algebra, spectral graph theory, ergodic theory, and harmonic analysis [187], [227], [228], [229], [230], [231], [232], [233], [234], [235], [236], [237], [238], [239], [240], [241]. For more details on extremal set theory, we refer the reader to the book by Gerbner and Patkos [242]; for probabilistic arguments/proofs, see the books by Bollobás [243] and Spencer [244].

Our work in this paper concerns a subfield of extremal set theory, called *intersection theorems*, wherein set-systems under specific intersection restrictions are constructed, and bounds on their sizes are derived. A wide range of methods have been employed to establish a large number of intersection theorems over various mathematical structures, including vector subspaces, graphs, subsets of finite groups with given group actions, and uniform hypergraphs with stronger or weaker intersection conditions. The methods used to derive these theorems have included purely combinatorial methods such as shifting/compressions, algebraic methods (including linear-algebraic, Fourier analytic and representation-theoretic), analytic, probabilistic and regularity-type methods. We shall not give a full account of the known intersection theorems, but only touch upon the results that are particularly relevant to our set-system and its construction. For a broader account, we refer the interested reader to the comprehensive surveys by Ellis [245], and Frankl and Tokushige [246]. For an introduction to intersecting and cross-intersecting families related to hypergraphs, see [247] and [248].

Note 1: Set-system and hypergraph are very closely related terms, and commonly used interchangeably. Philosophically, in a hypergraph, the focus is more on vertices, vertex subsets being in "relation", and subset(s) of vertices satisfying a specific configuration of relations; whereas in a set-system, the focus is more on set-theoretic properties of the sets.

In this section, we derive multiple intersection theorems for:

1) at most t-intersecting k-uniform families of sets,
2) maximally cover-free at most t-intersecting k-uniform families of sets.

We also provide an explicit construction for at most t-intersecting k-uniform families of sets. Later in the text, we use the results from this section to establish the maximum number of SSKH PRFs that can be constructed securely by a set of parties against various active/passive and internal/external adversaries.

For $a, b \in \mathbb{Z}$ with $a \leq b$, let $[a, b] := \{a, a+1, \ldots, b-1, b\}$.

Definition 22: $\mathcal{H} \subseteq 2^{[n]}$ is k-uniform if $|A| = k$ for all $A \in \mathcal{H}$.

Definition 23: $\mathcal{H} \subseteq 2^{[n]}$ is maximally cover-free if

$$A \nsubseteq \bigcup_{B \in \mathcal{H}, B \neq A} B$$

for all $A \in \mathcal{H}$.

It is clear that $\mathcal{H} \subseteq 2^{[n]}$ is maximally cover-free if and only if every $A \in \mathcal{H}$ has some element x_A such that $x_A \notin B$ for all $B \in \mathcal{H}$ where $B \neq A$. Furthermore, the maximum size of a k-uniform family $\mathcal{H} \subseteq 2^{[n]}$ that is maximally cover-free is $n - k + 1$, and it is realized by the following set system:

$$\mathcal{H} = \{[k-1] \cup \{x\} : x \in [k, n]\}$$

(and this is unique up to permutations of $[n]$).

Definition 24: Let t be a non-negative integer. We say the set system $\mathcal{H}$ is

1) at most t-intersecting if $|A \cap B| \leq t$,
2) exactly t-intersecting if $|A \cap B| = t$,
3) at least t-intersecting if $|A \cap B| \geq t$,

for all $A, B \in \mathcal{H}$ with $A \neq B$.

Property (iii) in Definition 24 is often simply called "t-intersecting" [249], but we shall use the term "at least t-intersecting" for clarity.

Definition 25: Let $\mathcal{F}, \mathcal{G} \subseteq 2^{[n]}$. We say that $\mathcal{F}$ and $\mathcal{G}$ are equivalent (denoted as $\mathcal{F} \sim \mathcal{G}$) if there exists a permutation π of $[n]$ such that $\pi^*(\mathcal{F}) = \mathcal{G}$, where

$$\pi^*(\mathcal{F}) = \{\{\pi(a) : a \in A\} : A \in \mathcal{F}\}.$$

For $n, k, t, m \in \mathbb{Z}^+$ with $t \leq k \leq n$, let $N(n, k, t, m)$ denote the collection of all set systems $\mathcal{H} \subseteq 2^{[n]}$ of size m that are at most t-intersecting and k-uniform, and $M(n, k, t, m)$ denote the collection of set systems $\mathcal{H} \in N(n, k, t, m)$ that are also maximally cover-free.

The following proposition establishes a bijection between equivalence classes of these two collections of set systems (for different parameters):

Proposition 1: Suppose $n, k, t, m \in \mathbb{Z}^+$ satisfy $t \leq k \leq n$ and $m < n$. Then there exists a bijection

$$M(n, k, t, m) / \sim \leftrightarrow N(n - m, k - 1, t, m) / \sim .$$

Proof: We will define functions

$$\bar{f} : M(n, k, t, m) / \sim \to N(n - m, k - 1, t, m) / \sim$$
$$\bar{g} : N(n - m, k - 1, t, m) / \sim \to M(n, k, t, m) / \sim$$

that are inverses of each other.

Let $\mathcal{H} \in M(n, k, t, m)$. Since $\mathcal{H}$ is maximally cover-free, for every $A \in \mathcal{H}$, there exists $x_A \in A$ such that $x_A \notin B$ for all $B \in \mathcal{H}$ where $B \neq A$. Consider the set system $\{A \setminus \{x_A\} :$

$A \in \mathcal{H}\}$. First, note that although this set system depends on the choice of $x_A \in A$ for each $A \in \mathcal{H}$, the equivalence class of $\{A \setminus \{x_A\} : A \in \mathcal{H}\}$ is independent of this choice. Hence, we get the following map:

$$f : M(n,k,t,m) \to N(n-m,k-1,t,m)\,/\sim \\ \mathcal{H} \mapsto [\{A \setminus \{x_A\} : A \in \mathcal{H}\}].$$

Furthermore, it is clear that that if $\mathcal{H} \sim \mathcal{H}'$, then $f(\mathcal{H}) \sim f(\mathcal{H}')$. So, f induces a well-defined map as:

$$\bar{f} : M(n,k,t,m)\,/\sim \to N(n-m,k-1,t,m)\,/\sim .$$

Next, for a set system $\mathcal{G} = \{G_1,\ldots,G_m\} \in N(n-m,k-1,t,m)$, define

$$g : N(n-m,k-1,t,m) \to M(n,k,t,m)\,/\sim \\ \mathcal{G} \mapsto [\{G_i \cup \{n-m+i\} : i \in [m]\}].$$

Again, this induces a well-defined map

$$\bar{g} : N(n-m,k-1,t,m)\,/\sim \to M(n,k,t,m)\,/\sim$$

since $g(\mathcal{G}) \sim g(\mathcal{G}')$ for any $\mathcal{G}, \mathcal{G}'$ such that $\mathcal{G} \sim \mathcal{G}'$.

We can check that $\bar{f} \circ \bar{g} = id_{N(n-m,k-1,t,m)}$ and that $\bar{g} \circ \bar{f} = id_{M(n,k,t,m)}$. Hence, $\bar{f}$ and $\bar{g}$ are bijections. ∎

Corollary 1: Let $n,k,t,m \in \mathbb{Z}^+$ be such that $t \le k \le n$ and $m < n$. Then there exists a maximally cover-free, at most t-intersecting, k-uniform set system $\mathcal{H} \subseteq 2^{[n]}$ of size m if and only if there exists an at most t-intersecting, $(k-1)$-uniform set system $\mathcal{G} \subseteq 2^{[n-m]}$.

Remark 2: Both Proposition 1 and Corollary 1 remain true if, instead of at most t-intersecting families, we consider exactly t-intersecting or at least t-intersecting families.

At least t-intersecting families have been completely characterized by Ahlswede and Khachatrian [250], but the characterization of exactly t-intersecting and at most t-intersecting families remain open.

Let $\mathcal{H} \subseteq 2^{[n]}$ be a at most t-intersecting and k-uniform family, and $\varpi(n,k,t) = \max\{|\mathcal{H}|\}$.

Proposition 2: Suppose $n,k,t \in \mathbb{Z}^+$ are such that $t \le k \le n$. Then

$$\varpi(n,k,t) \le \frac{\binom{n}{t+1}}{\binom{k}{t+1}}.$$

Proof: Let $\mathcal{H} \subseteq 2^{[n]}$ be an at most t-intersecting and k-uniform family. The number of pairs (X,A), where $A \in \mathcal{H}$ and $X \subseteq A$ is of size $t+1$, is equal to $|\mathcal{H}| \cdot \binom{k}{t+1}$. Since $\mathcal{H}$ is at most t-intersecting, any $(t+1)$-element subset of $[n]$ lies in at most one set in $\mathcal{H}$. Thus,

$$|\mathcal{H}| \cdot \binom{k}{t+1} \le \binom{n}{t+1} \implies |\mathcal{H}| \le \frac{\binom{n}{t+1}}{\binom{k}{t+1}}.$$

∎

Using Proposition 1, we immediately obtain the following as a corollary:

Corollary 2: Suppose $\mathcal{H} \subseteq 2^{[n]}$ is maximally cover-free, at most t-intersecting and k-uniform. Then

$$|\mathcal{H}| \le \frac{\binom{n-|\mathcal{H}|}{t+1}}{\binom{k-1}{t+1}}.$$

Similarly, by applying Proposition 1, other results on at most t-intersecting and k-uniform set systems can also be translated into results on set systems that, in addition to having these two properties, are maximally cover-free. Thus, henceforth, we do not explicitly state such results when their derivation is trivial.

A. BOUNDS FOR SMALL n

In this section, we give several bounds on $\varpi(n,k,t)$ for small values of n.

Lemma 1: Let $n,k,t \in \mathbb{Z}^+$ be such that $t \le k \le n < \frac{1}{2}k\left(\frac{k}{t}+1\right)$. Let m' be the least positive integer such that $n < m'k - \frac{1}{2}m'(m'-1)t$. Then

$$\varpi(n,k,t) = m' - 1.$$

Proof: First, we show that there exists $m^\star \in \mathbb{Z}^+$ such that $n < m^\star k - \frac{1}{2}m^\star(m^\star-1)t$. Consider the quadratic polynomial $p(x) = xk - \frac{1}{2}x(x-1)t$. Note that $p(x)$ achieves its maximum value at $x = \frac{k}{t} + \frac{1}{2}$. If we let $m^\star$ be the unique positive integer such that $\frac{k}{t} \le m^\star < \frac{k}{t} + 1$, then

$$p(m^\star) \ge p\left(\frac{k}{t}\right) = \frac{1}{2}k\left(\frac{k}{t}+1\right) > n,$$

as required.

Next, suppose $\mathcal{H}$ is an at most t-intersecting, k-uniform set family with $|\mathcal{H}| \ge m'$. Let $A_1,\ldots,A_{m'} \in \mathcal{H}$ be distinct. Then

$$n \ge \left|\bigcup_{i=1}^{m'} A_i\right| = \sum_{i=1}^{m'} \left|A_i \setminus \bigcup_{j=1}^{i-1} A_j\right| \ge \sum_{i=0}^{m'-1}(k-it) \\ = m'k - \frac{1}{2}m'(m'-1)t,$$

which is a contradiction. This proves that $|\mathcal{H}| \le m' - 1$.

It remains to construct an at most t-intersecting, k-uniform set family $\mathcal{H} \subseteq 2^{[n]}$ with $|\mathcal{H}| = m' - 1$. Let $m = m' - 1$. The statement is trivial if $m = 0$, so we may assume that $m \in \mathbb{Z}^+$. By the minimality of m', we must have $n \ge mk - \frac{1}{2}m(m-1)t$. Let $k = \alpha t + \beta$ with $\alpha, \beta \in \mathbb{Z}$ and $0 \le \beta \le t-1$. Define a set system $\mathcal{H} = \{A_1,\ldots,A_m\}$ as follows:

$$A_i = \{(l,\{i,j\}) : l \in [t], j \in [\alpha+1] \setminus \{i\}\} \cup \{(i,j) : j \in [\beta]\}.$$

It is clear, by construction, that $\mathcal{H}$ is at most t-intersecting and k-uniform. Furthermore, since $\alpha = \lfloor k/t \rfloor \ge m$, the number of elements in the universe of $\mathcal{H}$ is

$$t \cdot |\{i,j\} : 1 \le i < j \le \alpha+1,\ i \le m| + m\beta \\ = t\left(\binom{\alpha+1}{2} - \binom{\alpha+1-m}{2}\right) + m\beta \\ = t\left(m\alpha - \frac{1}{2}m(m-1)\right) + m\beta$$

$$= mk - \frac{1}{2}m(m-1)t.$$

■

Proposition 3: *Let $n, k, t \in \mathbb{Z}^+$ be such that $t \leq k \leq n$.*

(a) If $n < \frac{1}{2}k\left(\frac{k}{t}+1\right)$, then

$$\varpi(n,k,t) = \left\lfloor \frac{1}{2} + \frac{k}{t} - \sqrt{\left(\frac{1}{2}+\frac{k}{t}\right)^2 - \frac{2n}{t}} \right\rfloor.$$

(b) If $t \mid k$ and $n = \frac{1}{2}k\left(\frac{k}{t}+1\right)$, then

$$\varpi(n,k,t) = \frac{k}{t} + 1.$$

Proof:

(a) Note that $m = \left\lfloor \frac{1}{2} + \frac{k}{t} - \sqrt{\left(\frac{1}{2}+\frac{k}{t}\right)^2 - \frac{2n}{t}} \right\rfloor$ satisfies $n \geq mk - \frac{1}{2}m(m-1)t$ and $m' = m+1$ satisfies $n < m'k - \frac{1}{2}m'(m'-1)t$; hence, the result follows immediately from Lemma 1.

(b) Let $\mathcal{H} \subseteq 2^{[n]}$ be an at most t-intersecting, k-uniform set family. We may assume that $|\mathcal{H}| \geq \frac{k}{t}$. We will first show that any three distinct sets in $\mathcal{H}$ have empty intersection. Let A_1, A_2 and A_3 be any three distinct sets in $\mathcal{H}$, and let $A_4, \ldots, A_{\frac{k}{t}} \in \mathcal{H}$ be such that the A_i's are all distinct. Then

$$\left|\bigcup_{i=1}^{\frac{k}{t}} A_i\right| = \sum_{i=1}^{\frac{k}{t}} \left|A_i \setminus \bigcup_{j=1}^{i-1} A_j\right| \geq \sum_{i=0}^{\frac{k}{t}-1}(k-it) = \frac{1}{2}k\left(\frac{k}{t}+1\right) = n,$$

and thus we have must equality everywhere. In particular, we obtain $|A_3 \setminus (A_1 \cup A_2)| = k - 2t$, which together which the fact that $\mathcal{H}$ is at most t-intersecting, implies that $A_1 \cap A_2 \cap A_3 = \varnothing$, as claimed. Therefore, every $x \in [n]$ lies in at most 2 sets in $\mathcal{H}$. We get:

$$|\mathcal{H}| \cdot k = |(A,x) : A \in \mathcal{H},\ x \in A| \leq 2n$$
$$\implies |\mathcal{H}| \leq \frac{2n}{k} = \frac{k}{t} + 1,$$

proving the first statement.

Next, we shall exhibit an at most t-intersecting, k-uniform set family $\mathcal{H} \subseteq 2^{[n]}$, where $n = \frac{1}{2}k\left(\frac{k}{t}+1\right)$, with $|\mathcal{H}| = \frac{k}{t}+1$. Let $\mathcal{H} = \{A_1, \ldots, A_{\frac{k}{t}+1}\}$ with

$$A_i = \left\{(l, \{i,j\}) : l \in [t], j \in \left[\frac{k}{t}+1\right] \setminus \{i\}\right\}.$$

It is clear that $\mathcal{H}$ is exactly t-intersecting and k-uniform, and that it is defined over a universe of $t \cdot \binom{k/t+1}{2} = n$ elements

■

Remark 3: The condition $n < \frac{1}{2}k\left(\frac{k}{t}+1\right)$ in Proposition 3(a) is necessary. Indeed, if $n = \frac{1}{2}k\left(\frac{k}{t}+1\right)$, then

$$\left\lfloor \frac{1}{2} + \frac{k}{t} - \sqrt{\left(\frac{1}{2}+\frac{k}{t}\right)^2 - \frac{2n}{t}} \right\rfloor = \frac{k}{t} < \frac{k}{t} + 1.$$

Next, we examine the case where $n = \frac{1}{2}k\left(\frac{k}{t}+1\right) + 1$. Unlike earlier cases, we do not have exact bounds for this case. But what is perhaps surprising is that, for certain k and t, the addition of a single element to the universe set can increase the maximum size of the set family by 3 or more.

Proposition 4: *Let $n, k, t \in \mathbb{Z}^+$ be such that $t \leq k \leq n$ and $t \mid k$. If $n = \frac{1}{2}k\left(\frac{k}{t}+1\right)+1$, then*

$$\varpi(n,k,t) \leq \frac{\frac{k}{t}+1}{1-\frac{k}{n}} = \left(\frac{k^2+kt+2t}{k^2-kt+2t}\right)\left(\frac{k}{t}+1\right).$$

Proof: Let $\mathcal{H} \subseteq 2^{[n]}$ be an at most t-intersecting and k-uniform family. There exists some element $x \in [n]$ such that x is contained in at most $\lfloor \frac{k|\mathcal{H}|}{n} \rfloor$ sets in $\mathcal{H}$. We construct a set family $\mathcal{H}' \subseteq 2^{[n]\setminus\{x\}}$ by taking those sets in $\mathcal{H}$ that do not contain x. Since $\mathcal{H}'$ is defined over a universe of $\frac{1}{2}k\left(\frac{k}{t}+1\right)$ elements, we obtain the following by applying Proposition 3:

$$|\mathcal{H}| - \left\lfloor \frac{k|\mathcal{H}|}{n} \right\rfloor \leq |\mathcal{H}'| \leq \frac{k}{t} + 1$$
$$\implies \left\lceil |\mathcal{H}| - \frac{k|\mathcal{H}|}{n} \right\rceil \leq \frac{k}{t} + 1$$
$$\implies |\mathcal{H}| - \frac{k|\mathcal{H}|}{n} \leq \frac{k}{t} + 1$$
$$\implies |\mathcal{H}| \leq \frac{\frac{k}{t}+1}{1-\frac{k}{n}}.$$

■

Remark 4: (a) If $k = 3$, $t = 1$, and $n = \frac{1}{2}k\left(\frac{k}{t}+1\right) + 1 = 7$, then the bound in the Proposition 4 states that $\varpi(n,k,t) \leq \left(\frac{k^2+kt+2t}{k^2-kt+2t}\right)\left(\frac{k}{t}+1\right) = 7$. The Fano plane, depicted in Figure 3, is an example of a 3-uniform family of size 7, defined over a universe of 7 elements, that is exactly 1-intersecting. Thus, the bound in Proposition 4 can be achieved, at least for certain choices of k and t. An interesting side note: Fano plane has applications/relations to integer factorization [251], [252], [253] and octonians [254], [255], [256], [257], both of which have direct applications to cryptography [258], [259], [260], [261], [262], [263].

(b) Note that

$$\left(\frac{k^2+kt+2t}{k^2-kt+2t}\right)\left(\frac{k}{t}+1\right) - \left(\frac{k}{t}+1\right) = \frac{2k^2+2kt}{k^2-kt+2t}.$$

We can show that the above expression is (strictly) bounded above by 6 (for $k \neq t$), with slightly better

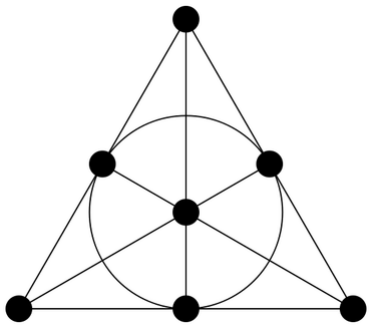

FIGURE 3. The Fano plane.

bounds for $t = 1,\ 2,\ 3,\ 4$. It follows that

$$\varpi(n,k,t) \leq \begin{cases} \frac{k}{t}+4 & \text{if } t=1, \\ \frac{k}{t}+5 & \text{if } t=2,\ 3,\ 4, \\ \frac{k}{t}+6 & \text{if } t \geq 5. \end{cases}$$

Furthermore, $\lim_{k\to\infty} \frac{2k^2+2kt}{k^2-kt+2t} = 2$; thus, for fixed t, we have $\varpi(n,k,t) \leq \frac{k}{t}+3$ for large enough k.

Next, we give a necessary condition for the existence of at most t-intersecting and k-uniform families $\mathcal{H} \subseteq 2^{[n]}$, which implicitly gives a bound on $\varpi(n,k,t)$.

Proposition 5: Let $n,k,t \in \mathbb{Z}^+$ satisfy $t \leq k \leq n$, and $\mathcal{H} \subseteq 2^{[n]}$ be an at most t-intersecting and k-uniform family with $|\mathcal{H}| = m$. Then

$$(n-r)\left\lfloor \frac{km}{n} \right\rfloor^2 + r\left\lceil \frac{km}{n} \right\rceil^2 \leq (k-t)m + tm^2$$

where $r = km - n\left\lfloor \frac{km}{n} \right\rfloor$.

Proof: Let α_j be the number of elements that is contained in exactly j sets in $\mathcal{H}$. We claim that the following holds:

$$\sum_{j=0}^{m} \alpha_j = n, \tag{1}$$

$$\sum_{j=0}^{m} j\alpha_j = km, \tag{2}$$

$$\sum_{j=0}^{m} j(j-1)\alpha_j \leq tm(m-1). \tag{3}$$

(1) is immediate, (2) follows from double counting the set $\{(A,x) : A \in \mathcal{H},\ x \in A\}$, and (3) follows from considering $\{(A,B,x) : A,B \in \mathcal{H},\ A \neq B,\ x \in A \cap B\}$ and using the fact that $\mathcal{H}$ is at most t-intersecting. This proves the claim.

Next, let us find non-negative integer values of $\alpha_0,\ldots,\alpha_m$ satisfying both (1) and (2) that minimize the expression $\sum_{j=0}^{m} j(j-1)\alpha_j$. Note that

$$\sum_{j=0}^{m} j(j-1)\alpha_j = \sum_{j=0}^{m} (j^2\alpha_j - j\alpha_j) = \sum_{j=0}^{m} j^2\alpha_j - km.$$

So, we want to minimize $\sum_{j=0}^{m} j^2\alpha_j$, subject to the restrictions (1) and (2). If $n \nmid km$, this is achieved by letting $\alpha_{\lfloor \frac{km}{n} \rfloor} = n-r$ and $\alpha_{\lceil \frac{km}{n} \rceil} = r$, with all other α_j's equal to 0. If $n \mid km$, we let $\alpha_{\frac{km}{n}} = n$ with all other α_j's equal to 0.

Indeed, it is easy to see that the above choice of $\alpha_0,\ldots,\alpha_m$ satisfy both (1) and (2). Now, let $\alpha_0,\ldots,\alpha_m$ be some other choice of the α_j's that also satisfy both (1) and (2). We will show that the function $f(\alpha_0,\ldots,\alpha_m) = \sum_{j=0}^{m} j^2\alpha_j$ can be decreased with a different choice of $\alpha_0,\ldots,\alpha_m$.

Suppose $\alpha_i \neq 0$ for some $i \neq \lfloor \frac{km}{n} \rfloor, \lceil \frac{km}{n} \rceil$, and assume that $i < \lfloor \frac{km}{n} \rfloor$ (the other case where $i > \lceil \frac{km}{n} \rceil$ is similar). Since the α_j's satisfy both (1) and (2), there must be some i_1 with $i_1 \geq \lceil \frac{km}{n} \rceil$ (the inequality is strict if $n \mid km$) such that $\alpha_{i_1} \neq 0$. It follows that if we decrease α_i and α_{i_1} each by one, and increase α_{i+1} and α_{i_1-1} each by one, constraints (1) and (2) continue to be satisfied. Furthermore, considering that $i_1 \geq \lfloor \frac{km}{n} \rfloor + 1 > i+1$, we get:

$$\begin{aligned} &f(\alpha_1,\ldots,\alpha_i,\alpha_{i+1},\ldots,\alpha_{i_1-1},\alpha_{i_1},\ldots,\alpha_m) \\ &-f(\alpha_1,\ldots,\alpha_i-1,\alpha_{i+1}+1,\ldots,\alpha_{i_1-1}+1,\alpha_{i_1}-1,\ldots, \\ &\alpha_m) = i^2-(i+1)^2-(i_1-1)^2+i_1^2 = 2i_1-2i-2 > 0. \end{aligned}$$

This proves the claim that the choice of $\alpha_{\lfloor \frac{km}{n} \rfloor} = n-r$ and $\alpha_{\lceil \frac{km}{n} \rceil} = r$ minimizes f.

Therefore, we can only find non-negative integers $\alpha_0,\ldots,\alpha_m$ satisfying all three conditions above if and only if

$$(n-r)\left\lfloor \frac{km}{n} \right\rfloor^2 + r\left\lceil \frac{km}{n} \right\rceil^2 - km \leq tm(m-1),$$

as desired. ∎

Remark 5: For fixed k and t, if n is sufficiently large, then the inequality in Proposition 5 will be true for all m. Thus, the above proposition is only interesting for values of n that are not too large.

B. ASYMPTOTIC BOUNDS

A Steiner system is defined as an arrangement of a set of elements in triples such that each pair of elements is contained in exactly one triple. The study of Steiner systems has a long history, dating back to the 19th century work on triple block designs by Plücker [264], Kirkman [265], Steiner [266], Reiss [267], Noether [268], Netto [269], Moore [270], Sylvester [271], Power [272], and Clebsch and Lindemann [273]. The term Steiner (triple) systems was coined in 1938 by Witt [274]. The Fano plane — discussed in Remark 4 and depicted in Figure 3 — represents a unique Steiner system of order 7; it can be seen as having 7 elements in 7 blocks of size 3 such that each pair of elements is contained in exactly 1 block. In cryptography, Steiner systems primarily have applications to (anonymous) secret sharing [275], [276] and low-redundancy private information retrieval [277]. For a broader introduction to the topic, we refer the interested reader to [278] (also see [279], [280]). In this section, we will see how at most t-intersecting families are related to Steiner systems. Using a result from

Keevash [281] about the existence of Steiner systems with certain parameters, we obtain an asymptotic bound on the maximum size of at most t-intersecting families.

Definition 26: A Steiner system $S(t, k, n)$, where $t \leq k \leq n$, is a family $\mathcal{S}$ of subsets of $[n]$ such that

1) $|A| = k$ for all $A \in \mathcal{S}$,
2) any t-element subset of $[n]$ is contained in exactly one set in $\mathcal{S}$.

The elements of $\mathcal{S}$ are known as blocks.

From the above definition, it is clear that there exists a family $\mathcal{H}$ that achieves equality in Proposition 2 if and only if $S(t+1, k, n)$ exists. It is easy to derive the following well known necessary condition for the existence of a Steiner system with given parameters:

Proposition 6: If $S(t, k, n)$ exists, then $\binom{n-i}{t-i}$ is divisible by $\binom{k-i}{t-i}$ for all $0 \leq i \leq t$, and the number of blocks in $S(t, k, n)$ is equal to $\binom{n}{t}/\binom{k}{t}$.

In 2019, Keevash [281] proved the following result, providing a partial converse to the above, and answering in the affirmative a longstanding open problem in the theory of designs.

Theorem 4 ([281]): For any $k, t \in \mathbb{Z}^+$ with $t \leq k$, there exists $n_0(k, t)$ such that for all $n \geq n_0(k, t)$, a Steiner system $S(t, k, n)$ exists if and only if

$$\binom{k-i}{t-i} \text{ divides } \binom{n-i}{t-i} \quad \text{for all } i = 0, 1 \ldots, t-1.$$

Using this result, we will derive asymptotic bounds for the maximum size of an at most t-intersecting and k-uniform family.

Proposition 7: Let $k, t \in \mathbb{Z}^+$ with $t < k$, and $C < 1$ be any positive real number.

1) *There exists $n_1(k, t, C)$ such that for all integers $n \geq n_1(k, t, C)$, there is an at most t-intersecting and k-uniform family $\mathcal{H} \subseteq 2^{[n]}$ with*

$$|\mathcal{H}| \geq \frac{Cn^{t+1}}{k(k-1)\cdots(k-t)}.$$

2) *For all sufficiently large n,*

$$\frac{Cn^{t+1}}{k(k-1)\cdots(k-t)} \leq \varpi(n, k, t) < \frac{n^{t+1}}{k(k-1)\cdots(k-t)}.$$

In particular,

$$\varpi(n, k, t) \sim \frac{n^{t+1}}{k(k-1)\cdots(k-t)}.$$

Proof:

1) Let $t' = t+1$. By Theorem 4, there exists $n_0(k, t')$ such that for all $N \geq n_0(k, t')$, a Steiner system $S(t', k, N)$ exists if

$$\binom{k-i}{t'-i} \text{ divides } \binom{N-i}{t'-i} \quad \text{for all } i = 0, 1 \ldots, t'-1. \tag{$*$}$$

Suppose n is sufficiently large. Let $n' \leq n$ be the largest integer such that ($*$) is satisfied with $N = n'$. Since

$$\binom{k-i}{t'-i} \text{ divides } \binom{N-i}{t'-i}$$
$$\iff (k-i)\cdots(k-t'+1) \mid (N-i)\cdots(N-t'+1),$$

all N of the form $\lambda k(k-1)\cdots(k-t'+1)+t'-1$ with $\lambda \in \mathbb{Z}$ will satisfy ($*$). Hence,

$$n - n' \leq k(k-1)\cdots(k-t'+1).$$

By our choice of n', there exists a Steiner system $S(t', k, n')$, which is an at most t-intersecting and k-uniform set family, defined over the universe $[n'] \subseteq [n]$, such that

$$|S(t', k, n')| = \frac{\binom{n'}{t'}}{\binom{k}{t'}} = \frac{n'(n'-1)\cdots(n'-t'+1)}{k(k-1)\cdots(k-t'+1)}$$
$$\geq \frac{(n-\alpha)(n-\alpha-1)\cdots(n-\alpha-t'+1)}{k(k-1)\cdots(k-t'+1)},$$

where $\alpha = \alpha(k, t') = k(k-1)\cdots(k-t'+1)$ is independent of n. Since $C < 1$, there exists $n_2(k, t', C)$ such that for all $n \geq n_2(k, t', C)$,

$$\frac{(n-\alpha)(n-\alpha-1)\cdots(n-\alpha-t'+1)}{n^{t'}} \geq C,$$

from which it follows that

$$|S(t', k, n')| \geq \frac{Cn^{t'}}{k(k-1)\cdots(k-t'+1)}$$
$$= \frac{Cn^{t+1}}{k(k-1)\cdots(k-t)}$$

for all sufficiently large n. From the above argument, we see that we can pick

$$n_1(k, t, C) = \max\left(n_0(k, t') + \alpha(k, t'), n_2(k, t', C)\right).$$

2) By Proposition 2,

$$\varpi(n, k, t) \leq \frac{\binom{n}{t+1}}{\binom{k}{t+1}} = \frac{n(n-1)\cdots(n-t)}{k(k-1)\cdots(k-t)}$$
$$< \frac{n^{t+1}}{k(k-1)\cdots(k-t)}.$$

The other half of the inequality follows immediately from 1.

■

Proposition 8: Let $k, t \in \mathbb{Z}^+$ with $t < k-1$, and $C < 1$ be any positive real number. Then for all sufficiently large N,

1) *there exists a maximally cover-free, at most t-intersecting and k-uniform family $\mathcal{H} \subseteq 2^{[N]}$ with $|\mathcal{H}| \geq CN$,*
2) *the maximum size $\nu(N, k, t)$ of a maximally cover-free, at most t-intersecting and k-uniform family $\mathcal{H} \subseteq 2^{[N]}$ satisfies*

$$CN \leq \nu(N, k, t) < N.$$

Proof: We note that (ii) follows almost immediately from (i). So, we prove (i).

Fix C_0 such that $C < C_0 < 1$. It follows from Propositions 1 and 7 that for all integers $n \geq n_1(k-1, t, C_0)$, there exists a maximally cover-free, at most t-intersecting and k-uniform family $\mathcal{H} \subseteq 2^{\left[n+\frac{n^{t+1}}{(k-1)(k-2)\cdots(k-t-1)}\right]}$ with

$$|\mathcal{H}| \geq \frac{C_0 n^{t+1}}{(k-1)(k-2)\cdots(k-t-1)}.$$

Since $C < C_0$, there exist $\delta > 1$ and $\varepsilon > 0$ such that $C_0 > \delta(1+\varepsilon)C$. Given N, let $n \in \mathbb{Z}^+$ be maximum such that

$$n + \frac{n^{t+1}}{(k-1)(k-2)\cdots(k-t-1)} \leq N.$$

Assume that N is sufficiently large so that $n \geq n_1(k-1, t, C_0)$. Then, by the above, there is a maximally cover-free, at most t-intersecting and k-uniform family $\mathcal{H} \subseteq 2^{[N]}$ so that

$$|\mathcal{H}| \geq \frac{C_0 n^{t+1}}{(k-1)(k-2)\cdots(k-t-1)}.$$

Since n is maximal, we have

$$N < (n+1) + \frac{(n+1)^{t+1}}{(k-1)(k-2)\cdots(k-t-1)}.$$

If N (and thus n) is sufficiently large such that

- $(n+1) < \frac{\varepsilon(n+1)^{t+1}}{(k-1)(k-2)\cdots(k-t-1)}$,
- $\left(1+\frac{1}{n}\right)^{t+1} < \delta$,

then

$$\begin{aligned} N &< \frac{(1+\varepsilon)(n+1)^{t+1}}{(k-1)(k-2)\cdots(k-t-1)} \\ &< \frac{\delta(1+\varepsilon)n^{t+1}}{(k-1)(k-2)\cdots(k-t-1)} \end{aligned}$$

and it follows that

$$|\mathcal{H}| \geq \frac{C_0 n^{t+1}}{(k-1)(k-2)\cdots(k-t-1)} > \frac{C_0 N}{\delta(1+\varepsilon)} > CN.$$

■

C. AN EXPLICIT CONSTRUCTION

While Proposition 7 provides an answer for the maximum size of an at most t-intersecting and k-uniform family for large enough n, we cannot explicitly construct such set families since Theorem 4 (and hence Proposition 7) is nonconstructive. In this section, we establish a method that explicitly constructs set families with larger parameters from set families with smaller parameters.

Fix a positive integer t. For an at most t-intersecting and k-uniform family $\mathcal{H} \subseteq 2^{[n]}$, define

$$s(\mathcal{H}) = \frac{k|\mathcal{H}|}{n}$$

as the "relative size" of $\mathcal{H}$ with respect to the parameters k and n. Note that the maximum possible value of $|\mathcal{H}|$ should increase with larger n and decrease with larger k, hence $s(\mathcal{H})$ is a reasonable measure of the "relative size" of $\mathcal{H}$.

The following result shows that it is possible to construct a sequence of at most t-intersecting and k_j-uniform families $\mathcal{H} \subseteq 2^{[n_j]}$, where $k_j \to \infty$, such that all set families in the sequence have the same relative size.

Proposition 9: Let $\mathcal{H} \subseteq 2^{[n]}$ be an at most t-intersecting and k-uniform family. Then there exists a sequence of set families $\mathcal{H}_j$ such that

(a) $\mathcal{H}_j$ is an at most t-intersecting and k_j-uniform set family,
(b) $s(\mathcal{H}_j) = s(\mathcal{H})$ for all j,
(c) $\lim_{j\to\infty} k_j = \infty$.

Proof: We will define the set families $\mathcal{H}_j$ inductively. Let $\mathcal{H}_1 = \mathcal{H}$, and $\mathcal{H}_j \subseteq 2^{[n_j]}$ be an at most t-intersecting k_j-uniform family for some $j \in \mathbb{Z}^+$ such that $m = |\mathcal{H}_j|$. Consider set families $\mathcal{G}^{(1)}, \ldots, \mathcal{G}^{(m)}, \mathcal{H}^{(1)}, \ldots, \mathcal{H}^{(m)}$, defined over disjoint universes such that each $\mathcal{G}^{(\ell)}$ (and similarly, each $\mathcal{H}^{(\ell)}$) is isomorphic to $\mathcal{H}_j$. Let

$$\mathcal{G}^{(\ell)} = \{B_1^{(\ell)}, \ldots, B_m^{(\ell)}\}, \quad \mathcal{H}^{(\ell)} = \{C_1^{(\ell)}, \ldots, C_m^{(\ell)}\}.$$

For $1 \leq h, i \leq m$, define the sets $A_{h,i} = B_h^{(i)} \sqcup C_i^{(h)}$, and let

$$\mathcal{H}_{j+1} = \{A_{h,i} : 1 \leq h, i \leq m\}.$$

It is clear that $\mathcal{H}_{j+1}$ is a $2k_j$-uniform family defined over a universe of $2mn_j$ elements, and that $|\mathcal{H}_{j+1}| = m^2$. We claim that $\mathcal{H}_{j+1}$ is at most t-intersecting. Indeed, if $(h_1, i_1) \neq (h_2, i_2)$, then

$$\begin{aligned} |A_{h_1,i_1} \cap A_{h_2,i_2}| &= |(B_{h_1}^{(i_1)} \sqcup C_{i_1}^{(h_1)}) \cap (B_{h_2}^{(i_2)} \sqcup C_{i_2}^{(h_2)})| \\ &= |B_{h_1}^{(i_1)} \cap B_{h_2}^{(i_2)}| + |C_{i_1}^{(h_1)} \cap C_{i_2}^{(h_2)}| \\ &= \begin{cases} |C_{i_1}^{(h_1)} \cap C_{i_2}^{(h_2)}| \leq t & \text{if } h_1 = h_2 \text{ and } i_1 \neq i_2, \\ |B_{h_1}^{(i_1)} \cap B_{h_2}^{(i_2)}| \leq t & \text{if } h_1 \neq h_2 \text{ and } i_1 = i_2, \\ 0 & \text{if } h_1 \neq h_2 \text{ and } i_1 \neq i_2. \end{cases} \end{aligned}$$

Finally,

$$s(\mathcal{H}_{j+1}) = \frac{k_{j+1}|\mathcal{H}_{j+1}|}{n_{j+1}} = \frac{2k_j m^2}{2mn_j} = \frac{k_j|\mathcal{H}_j|}{n_j} = s(\mathcal{H}_j).$$

■

Remark 6: In the above proposition, n_j, k_j, and $|\mathcal{H}_j|$ grow with j. Clearly, given a family $\mathcal{H}$, it is also possible to construct a sequence of set families $\mathcal{H}_j$ such that $s(\mathcal{H}_j) = s(\mathcal{H})$ for all j, where n_j and $|\mathcal{H}_j|$ grow with j, while k_j stays constant.

It is natural to ask, therefore, if it is possible to construct a sequence of set families satisfying $s(\mathcal{H}_j) = s(\mathcal{H})$, where n_j and k_j grow with j, but $|\mathcal{H}_j|$ stays constant. In fact, this is not always possible. Indeed, let $\mathcal{H}$ be the Fano plane, then $t = 1$, $n = 7$, $k = 3$, and $|\mathcal{H}| = 7$. Note that $\mathcal{H}$ satisfies Proposition 5 with equality, i.e.,

$$\frac{(k|\mathcal{H}|)^2}{n} = k|\mathcal{H}| + t(|\mathcal{H}|^2 - |\mathcal{H}|).$$

If we let $n' = \lambda n$ and $k' = \lambda k$ for some $\lambda > 1$, then

$$\frac{(k'|\mathcal{H}|)^2}{n'} = \lambda \frac{(k|\mathcal{H}|)^2}{n} = \lambda \left(k|\mathcal{H}| + t(|\mathcal{H}|^2 - |\mathcal{H}|)\right) > k'|\mathcal{H}| + t(|\mathcal{H}|^2 - |\mathcal{H}|).$$

Hence, by Proposition 5, there is no k'-uniform and at most t-intersecting family $\mathcal{H}' \subseteq 2^{[n']}$ such that $|\mathcal{H}'| = |\mathcal{H}| = 7$.

VI. GENERATING ROUNDED GAUSSIANS FROM PHYSICAL COMMUNICATIONS

In this section, we describe our procedure, called *Rounded Gaussians from Physical Communications (RGPC)*, that generates deterministic errors from a rounded Gaussian distribution — which we later prove to be sufficiently independent in specific settings. RGPC is comprised of the following two subprocedures:

- Hypothesis generation: a protocol to generate a linear regression hypothesis from the training data, which, in our case, is comprised of the physical layer communications between participating parties.
- Rounded Gaussian error generation: this procedure allows us to use the linear regression hypothesis — generated by using physical layer communications as training data — to derive deterministic rounded Gaussian errors. The outcome of this procedure is that it samples from a rounded Gaussian distribution in a manner that is (pseudo)random to a PPT external/internal adversary but is deterministic to the authorized parties.

A. SETTING AND CENTRAL IDEA

For the sake of intelligibility, we begin by giving a brief overview of our central idea. Let there be a set of $n \geq 2$ parties, $\mathcal{P} = \{P_i\}_{i=1}^n$. All parties agree upon a function $f(x) = \beta_0 + \beta_1 x$, with intercept $\beta_0 \leftarrow \mathbb{Z}$ and slope $\beta_1 \leftarrow \mathbb{Z}$. Let $\mathcal{H} \subseteq 2^{\mathcal{P}}$ be a family of sets such that each set $H_i \in \mathcal{H}$ forms a star graph ∂_i wherein each party is connected to a central hub $C_i \notin H_i$ (for all $i \in [|\mathcal{H}|]$) via two channels: one Gaussian and another error corrected. If $\mathcal{H}$ is k-uniform and at most t-intersecting, then each star in the interconnection graph formed by the sets $H_i \in \mathcal{H}$ contains exactly k members and $2k$ channels such that $|\partial_i \cap \partial_j| \leq t$. During the protocol, each party P_j sends out message pairs of the form $x_j, f(x_j)$, where $x_j \leftarrow \mathbb{Z}$ and f is a randomly selected function of specific type (more on this later), to the central hubs of all stars that it is a member of, such that:

- $f(x)$ is sent over the Gaussian channel,
- x is sent over the error corrected channel.

For the sake of simplicity, we only consider a single star for analyses in this section. All arguments and analyses from this section naturally extend to the setting with multiple stars. Due to the guaranteed errors occurring in the Gaussian channel, the messages recorded at each central hub C_i are of the form: $y = f(x) + \varepsilon_x$, where ε_x belongs to some Gaussian distribution $\mathcal{N}(0, \sigma^2)$ with mean zero and standard deviation σ. Recall that for most schemes, the value of σ primarily relies on the smoothing parameter. In our experiments, which are discussed in Section VI-C, we choose the range of σ as $\sigma \in [10, 300]$ — which contains the ranges mandated by New Hope [282], BCNS [283], and BLISS [168]. Note that even though techniques such as Gaussian 'convolutions' [91] can be used to shrink the range of σ that is required for the security guarantees of the given cryptosystem [284], such techniques are not necessary for our solution as any range for σ can be trivially realized by generating training data from a distribution with the suitable σ value/range. The central hub, C_i, forwards $\{x, y\}$ to all parties over the respective error corrected channels in ∂_i.

In our algorithm, we use least squares linear regression which aims to minimize the sum of the squared residuals. We know that the hypothesis generated by linear regression is of the form: $h(x) = \hat{\beta}_0 + \hat{\beta}_1 x$. Thus, the statistical error, with respect to our target function, comes out as:

$$\bar{e}_x = |y - h(x)|. \tag{4}$$

Due to the nature of the physical layer errors and independent channels, we know that the errors ε_x are random and independent. Thus, it follows that for restricted settings, the error terms $\bar{e}_{x_i}$ and $\bar{e}_{x_j}$ are independent (with respect to a PPT adversary) for all $x_i \neq x_j$, and — are expected to — belong to a Gaussian distribution. Next, we round $\bar{e}_x$ to the nearest integer as: $e_x = \lfloor \bar{e}_x \rceil$ to get the final error, e_x, which:

- is determined by x,
- belongs to a rounded Gaussian distribution.

We know from [1], [92], [127], and [128] that — with appropriate parameters — rounded Gaussians satisfy the hardness requirements for multiple LWE-based constructions. We are now ready to discuss RGPC protocol in detail.

Note 2: With a sufficiently large number of messages, $f(x)$ can be very closely approximated by the linear regression hypothesis $h(x)$. Therefore, with a suitable choice of parameters, it is quite reasonable to expect that the error distribution is Gaussian (which is indeed the case — see Lemma 2, where we use drowning/smudging to argue about the insignificance of negligible uniform error introduced by linear regression analysis). Considering this, we also examine the more interesting case wherein the computations are performed in $\mathbb{Z}_m$ (for some $m \in \mathbb{Z}^+ \setminus \{1\}$) instead of over $\mathbb{Z}$. However, our proofs and arguments are presented according to the former case, i.e., where the computations are performed over $\mathbb{Z}$. We leave adapting the proofs and arguments for the latter case, i.e., computations over $\mathbb{Z}_m$, as an open problem.

B. HYPOTHESIS GENERATION FROM PHYSICAL LAYER COMMUNICATIONS

In this section, we describe hypothesis generation from physical layer communications which allows us to generate an optimal linear regression hypothesis, $h(x)$, for the target function $f(x)$. As mentioned in Note 2, we consider the case wherein the error computations are performed in $\mathbb{Z}_m$.

As described in Section VI-A, the linear regression data for each subset of parties $H_i \in \mathcal{H}$ is comprised of the messages exchanged within star graph ∂_i — that is formed by the parties in $H_i \cup C_i$.

1) ASSUMPTIONS

We assume that the following conditions hold:

1) Value of the integer modulus m:
   - is either known beforehand, or
   - can be derived from the target function.
2) Size of the dataset, i.e., the total number of recorded physical layer messages, is reasonably large such that there are enough data points to accurately fit linear regression on any function period. In our experiments, we set it to 2^{16} messages.
3) For a dataset $\mathcal{D} = \{(x_i, y_i)\}$ $(i \in [\ell])$ of unique function input, message received pairs, it holds for the slope, β_1, of $f(x)$, that ℓ/β_1 is superpolynomial. For our experiments, we set β_1 such that $\ell/\beta_1 \geq 100$.

2) SETUP

Recall that the goal of linear regression is to find subset(s) of data points that can be used to generate a hypothesis $h(x)$ to approximate the target function, which in our case is $f(x)+\varepsilon_x$. Then, we extrapolate it to the entire dataset. However, since modulo is a periodic function, there is no explicit linear relationship between $x \leftarrow \mathbb{Z}$ and $y = f(x) + \varepsilon_x \bmod m$, even without the error term ε_x. Thus, we cannot directly apply linear regression to the entire dataset $\mathcal{D} = \{(x_i, y_i)\}$ $(i \in [\ell])$ and expect meaningful results unless $\beta_0 = 0$ and $\beta_1 = 1$.

We arrange the dataset, $\mathcal{D}$, in ascending order with respect to the x_i values, i.e., for $1 \leq i < j \leq m$ and all $x_i, x_j \in \mathcal{D}$, it holds that: $x_i < x_j$. Let $\mathcal{S} = \{x_i\}_{i=1}^{\ell}$ denote the ordered set with x_i $(\forall i \in [\ell])$ arranged in ascending order. Observe that the slope of $y = f(x) + \varepsilon_x \bmod m$ is directly proportional to the number of periods on any given range, $[x_i, x_j]$. For example, observe the slope in Figure 4, which depicts the scatter plot for $y = 3x + \varepsilon_x \bmod 12288$ with three periods. Therefore, in order to find a good linear fit for our target function on a subset of dataset that lies inside the given range, $[x_i, x_j]$, we want to correctly estimate the length of a single period. Consequently, our aim is to find a range $[x_i, x_j]$ for which the following is minimized:

$$\left|\hat{\beta}_1 - \frac{m}{x_j - x_i}\right|, \tag{5}$$

where $\hat{\beta}_1$ denotes the slope for our linear regression hypothesis $h(x) = \hat{\beta}_0 + \hat{\beta}_1 x$ computed on the subset with x values in $[x_i, x_j]$.

3) GENERATING OPTIMAL HYPOTHESIS

The following procedure describes our algorithm for finding the optimal hypothesis $h(x)$ and the target range $[x_i, x_j]$ that satisfies Equation 5 for $\beta_0 = 0$. When β_0 is not necessarily 0, a small modification to the procedure (namely, searching over all intervals $[x_i, x_j]$, instead of searching over only certain intervals as described below) is needed.

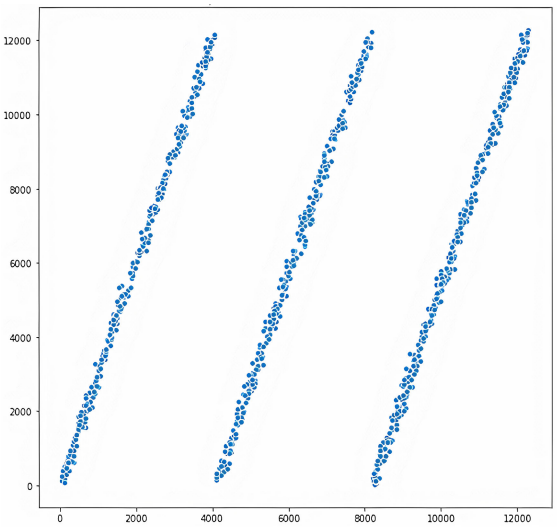

FIGURE 4. Scatter plot for $y = 3\,x + \varepsilon_x \bmod 12288$ (three periods).

Let κ denote the total number of periods, then it follows from Assumption 3 (from Section VI-B1) that $\kappa \leq \lceil \ell/100 \rceil$. Let $\delta_{\kappa,i} = |\hat{\beta}_1(\kappa, i) - \kappa|$, where $\hat{\beta}_1(\kappa, i)$ denotes that $\hat{\beta}_1$ is computed over the range $\left[x_{\lfloor (i-1)\ell/\kappa \rfloor + 1}, x_{\lfloor i\ell/\kappa \rfloor}\right]$.

1) Initialize the number of periods with $\kappa = 1$ and calculate $\delta_{1,1} = |\hat{\beta}_1(1, 1) - 1|$.
2) Compute the $\delta_{\kappa,i}$ values for all $1 < \kappa \leq \lceil \ell/100 \rceil$ and $i \in [\kappa]$. For instance, $\kappa = 2$ denotes that we consider two ranges: $\hat{\beta}_1(2, 1)$ is calculated on $\left[x_1, x_{\lfloor \ell/\kappa \rfloor}\right]$ and $\hat{\beta}_1(2, 2)$ on $\left[x_{\lfloor \ell/\kappa \rfloor + 1}, x_\ell\right]$. Hence, we compute $\delta_{2,i}$ for these two ranges. Similarly, $\kappa = 3$ denotes that we consider three ranges $\left[x_1, x_{\lfloor \ell/\kappa \rfloor}\right]$, $\left[x_{\lfloor \ell/\kappa \rfloor + 1}, x_{\lfloor 2\ell/\kappa \rfloor}\right]$ and $\left[x_{\lfloor 2\ell/\kappa \rfloor + 1}, x_\ell\right]$, and we compute $\hat{\beta}(3, i)$ and $\delta_{3,i}$ over these three ranges. Hence, $\delta_{\kappa,i}$ values are computed for all (κ, i) that satisfy $1 \leq i \leq \kappa \leq \lceil \ell/100 \rceil$.
3) Identify the optimal value $\delta = \min_{\kappa,i}(\delta_{\kappa,i})$, which is the minimum over all $\kappa \in [\lceil \ell/100 \rceil]$ and $i \in [\kappa]$.
4) After finding the minimal δ, output the corresponding (optimal) hypothesis $h(x)$.

What the above algorithm does is basically a grid search over κ and i with the performance metric being minimizing the $\delta_{\kappa,i}$ value.

Grid search: more details

Grid search is an approach used for hyperparameter tuning. It methodically builds and evaluates a model for each combination of parameters. Due to its ease of implementation and parallelization, grid search has prevailed as the de-facto standard for hyperparameter optimization in machine learning, especially in lower dimensions. For our purpose, we tune two parameters κ and i. Specifically, we perform grid search to find hypotheses $h(x)$ for all κ and i such that $\kappa \in [\lceil \ell/100 \rceil]$ and $i \in [\kappa]$. Optimal hypothesis is the one with the smallest value of the performance metric $\delta_{\kappa,i}$.

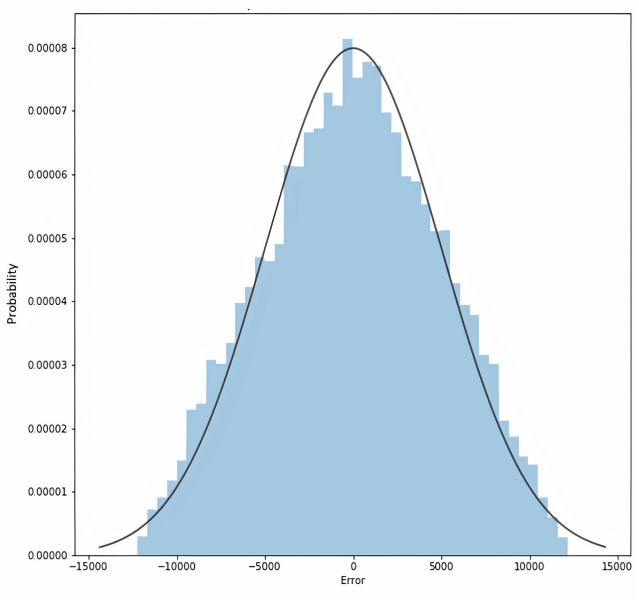

FIGURE 5. Distribution plot of $\bar{e}_x$ for $y = 546\,x + \varepsilon_x \bmod 12288$. Slope estimate: $\beta_1 = 551.7782$.

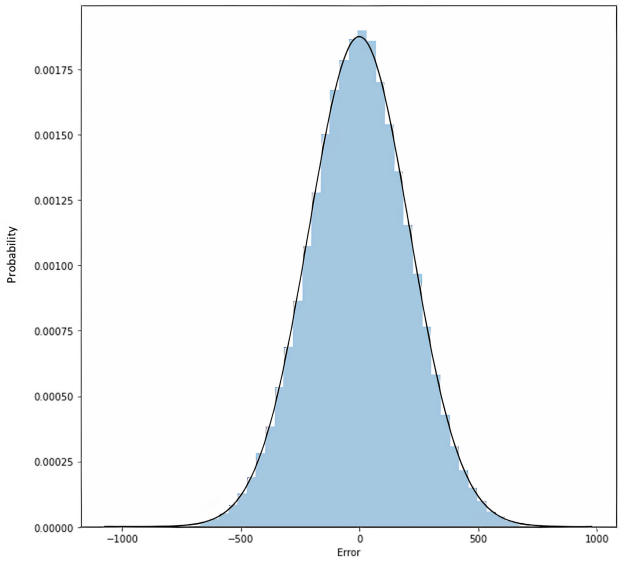

FIGURE 6. Distribution plot of $\bar{e}_x$ for $y = 240\sqrt{x} + \varepsilon_x \bmod 12288$. Slope estimate: $\beta_1 = 239.84$.

C. SIMULATION AND TESTING

We tested our RGPC algorithm with varying values of m and β_1 for the following functions:

- $f(x) = \beta_0 + \beta_1\, x$,
- $f(x) = \beta_0 + \beta_1 \sqrt{x}$,
- $f(x) = \beta_0 + \beta_1 x^2$,
- $f(x) = \beta_0 + \beta_1 \sqrt[3]{x}$,
- $f(x) = \beta_0 + \beta_1 \ln(x+1)$.

To generate the training data, we simulated the channel noise, ε_x, as a random Gaussian noise (introduced by the Gaussian channel), which we sampled from various distributions with zero mean, standard deviation $\sigma \in [10, 300]$, and $m \in [20000]$. Final channel noise was computed by rounding ε_x to the nearest integer and reducing the result modulo m.

For each function, we generated 2^{16} unique input-output pairs, exchanged over Gaussian channels, i.e., the dataset for each function is of the form $\mathcal{D} = \{(x_i, y_i)\}$, where $i \in [2^{16}]$. As expected, given the dataset $\mathcal{D}$ with data points $x_i, y_i = f(x_i) + \varepsilon_i \bmod m$, our algorithm always converged to the optimal range, yielding close approximations for the target function with deterministic errors, $\bar{e}_x = |y - h(x)| \bmod m$. Figure 5 shows a histogram of the errors $\bar{e}_x$ generated by our RGPC protocol — with our training data — for the target (linear) function $y = 546\,x + \varepsilon_x \bmod 12288$. The errors indeed belong to a truncated Gaussian distribution, bounded by the modulus 12288 from both tails.

Moving on to the cases wherein the independent variable x and the dependent variable y have a nonlinear relation: the most representative example of such a relation is the power function $f(x) = \beta_1 x^{\vartheta}$, where $\vartheta \in \mathbb{R}$. We know that nonlinearities between variables can sometimes be linearized by transforming the independent variable. Hence, we applied the following transformation: if we let $x_\upsilon = x^{\vartheta}$, then $f_\upsilon(x_\upsilon) = \beta_1 x_\upsilon = f(x)$ is linear in x_υ. This can now be solved by applying our hypothesis generation algorithm for linear functions. Figures 6 to 9 show the histograms of the errors $\bar{e}_x$ generated by our training datasets for the various nonlinear functions from the list given at the beginning of Section VI-C. It is clear that the errors for these nonlinear functions also belong to truncated Gaussian distributions, bounded by their respective moduli from both tails.

D. COMPLEXITY

Let the size of the dataset collected by recording the physical layer communications be ℓ. Then, the complexity for least squares linear regression is $\Theta(\ell)$ additions and multiplications. It follows from Assumption 3 (from Section VI-B1) that ℓ^2 is an upper bound on the maximum number of evaluations required for grid search. Therefore, the overall asymptotic complexity of our algorithm to find optimal hypothesis, and thereafter generate deterministic rounded Gaussian errors is $O(\ell^3)$. In comparison, the complexity of performing least squares linear regression on a dataset $\{(x_i, y_i)\}$ that has not been reduced modulo m is simply $\Theta(\ell)$ additions and multiplications.

E. ERROR ANALYSIS

Before moving ahead, we recommend the reader revisit Note 2.

Our RGPC protocol generates errors, $e_x = \lceil |y - h(x)| \rfloor$, in a deterministic manner by generating a mapping defined by the hypothesis h. Recall that h depends on two factors, namely the randomly generated function $f(x)$ and the ℓ random channel errors ε_x — both of which are derived via ℓ random inputs $x \leftarrow \mathbb{Z}$. Revisiting Definition 20, we observe that:

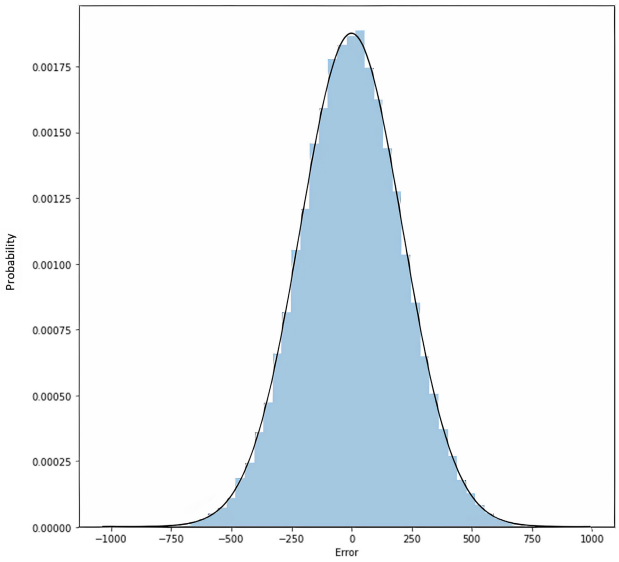

FIGURE 7. Distribution plot of $\bar{e}_x$ for $y = 125\,x^2 + \varepsilon_x \bmod 10218$. Slope estimate: $\beta_1 = 124.51$.

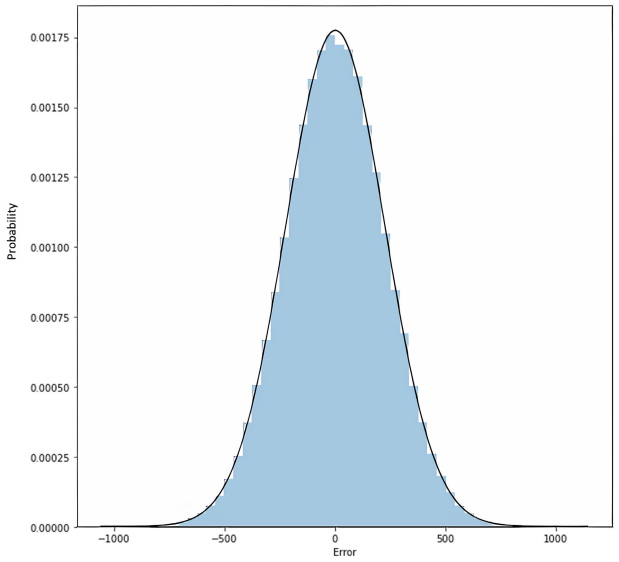

FIGURE 8. Distribution plot of $\bar{e}_x$ for $y = 221\,\sqrt[3]{x} + \varepsilon_x \bmod 11278$. Slope estimate: $\beta_1 = 221.01$.

- RGPC takes ℓ random elements $x \leftarrow \mathbb{Z}$ and ℓ evaluations of $f(x)$, each with an added random channel error ε_x. Collectively, these form the random input, r, described in Definition 20,
- RGPC returns a deterministic mapping which depends on r. Following the notation from Definition 20, we can write this mapping as $\mathfrak{M}_r$. However, taking into account the hypothesis, h, we choose the notation $\mathfrak{M}_h$ instead, but note that both are equivalent henceforth,
- Proving that $\mathfrak{M}_h$ satisfies the requirements outlined for the deterministic function/mapping in Definition 20 would directly establish RGPC as a P2SI algorithm — as described in Definition 20.

Let difference of two values modulo m is always represented by an element in $(-m/2, (m+1)/2]$. We make the further assumption that there exists a constant $b \geq 1$ such that the x_i values satisfy:

$$\frac{(x_i - \bar{x})^2}{\sum_{j=1}^{\ell}(x_j - \bar{x})^2} \leq \frac{b}{\ell} \qquad (\dagger)$$

for all $i = 1, \ldots, \ell$, where $\bar{x} = \sum_{j=1}^{\ell} \frac{x_j}{\ell}$.

Observe that if $\ell - 1$ divides $m - 1$ and the x_i values are $0, \frac{m-1}{\ell-1}, \ldots, \frac{(\ell-1)(m-1)}{\ell-1}$, then

$$\sum_{j=1}^{\ell}(x_j - \bar{x})^2 = \frac{\ell(\ell^2-1)(m-1)^2}{12(\ell-1)^2},$$

and the numerator is bounded above by $\frac{(m-1)^2}{4}$. Thus, Equation † is satisfied for $b = 3$. In general, by the strong law of large numbers, choosing a large enough number of x_i's uniformly at random from $[0, m-1]$ will, with very high probability, yield $\bar{x}$ close to $\frac{m-1}{2}$ and $\frac{1}{\ell}\sum_{j=1}^{\ell}(x_j - \bar{x})^2$ close to $\frac{(m^2-1)}{12}$ (since $X \sim U(0, m-1) \implies \mathsf{E}(X) = \frac{m-1}{2}$ and $\mathrm{var}(X) = \frac{m^2-1}{12}$). Hence, Equation † is satisfied with a small constant b, e.g., $b = 4$.

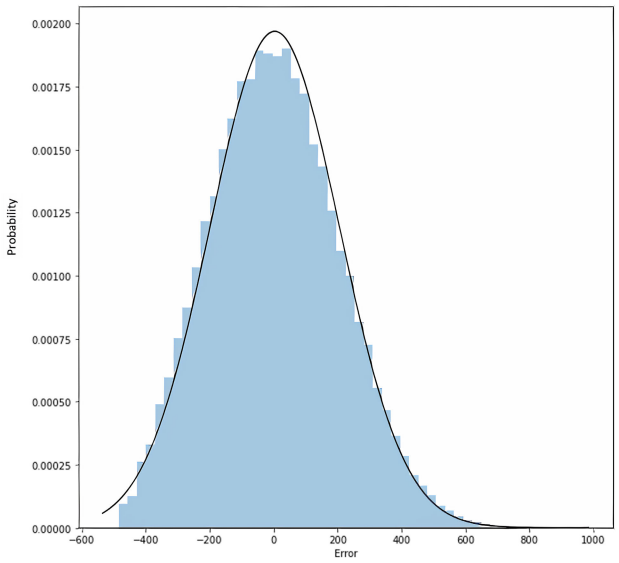

FIGURE 9. Distribution plot of $\bar{e}_x$ for $y = 53\ln(x+1) + \varepsilon_x \bmod 8857$. Slope estimate: $\beta_1 = 54.48$.

Recall that the dataset is $\mathcal{D} = \{(x_i, y_i)\}_{i=1}^{\ell}$, where $y_i = f(x_i) + \varepsilon_i = \beta_0 + \beta_1 x_i + \varepsilon_i$, with $\varepsilon_i \sim \mathcal{N}(0, \sigma^2)$. Further recall that the regression line is given by $h(x) = \hat{\beta}_0 + \hat{\beta}_1 x$. Then the error $\bar{e}_i$ is given by

$$\begin{aligned}\bar{e}_i &= (\hat{\beta}_0 + \hat{\beta}_1 x_i) - y_i = (\hat{\beta}_0 + \hat{\beta}_1 x_i) - (\beta_0 + \beta_1 x_i + \varepsilon_i) \\ &= (\hat{\beta}_0 - \beta_0) + (\hat{\beta}_1 - \beta_1)x_i - \varepsilon_i.\end{aligned}$$

The joint distribution of the regression coefficients $\hat{\beta}_0$ and $\hat{\beta}_1$ is given by the following well known result:

Proposition 10: Let $y_1, y_2, \ldots, y_\ell$ be independently distributed random variables such that $y_i \sim \mathcal{N}(\alpha + \beta x_i, \sigma^2)$ for all $i = 1, \ldots, \ell$. If $\hat{\alpha}$ and $\hat{\beta}$ are the least square estimates of α and β respectively, then:

$$\begin{pmatrix}\hat{\alpha}\\ \hat{\beta}\end{pmatrix} \sim \mathcal{N}\left(\begin{pmatrix}\alpha\\ \beta\end{pmatrix}, \sigma^2 \begin{pmatrix}\ell & \sum_{i=1}^{\ell} x_i\\ \sum_{i=1}^{\ell} x_i & \sum_{i=1}^{\ell} x_i^2\end{pmatrix}^{-1}\right).$$

Applying Proposition 10, and using the fact that $\mathbf{X} \sim \mathcal{N}(\boldsymbol{\mu}, \Sigma) \implies \mathbf{AX} \sim \mathcal{N}(\mathbf{A}\boldsymbol{\mu}, \mathbf{A}\Sigma\mathbf{A}^T)$, we get:

$$\begin{aligned}&(\hat{\beta}_0 - \beta_0) + (\hat{\beta}_1 - \beta_1)x_i\\ &\sim \mathcal{N}\left(0, \sigma^2 \frac{\sum_{j=1}^{\ell} x_j^2 - 2x_i \sum_{j=1}^{\ell} x_j + \ell x_i^2}{\ell \sum_{j=1}^{\ell} x_j^2 - (\sum_{j=1}^{\ell} x_j)^2}\right)\\ &= \mathcal{N}\left(0, \frac{\sigma^2}{\ell}\left(1 + \frac{\ell(x_i - \bar{x})^2}{\sum_{j=1}^{\ell}(x_j - \bar{x})^2}\right)\right).\end{aligned}$$

Thus, by Equation †, the variance of $(\hat{\beta}_0 - \beta_0) + (\hat{\beta}_1 - \beta_1)x_i$ is bounded above by $(1 + b)\sigma^2/\ell$.

Since $Z \sim \mathcal{N}(0, 1)$ satisfies $|Z| \leq 2.807034$ with probability 0.995, by the union bound, $\bar{e}_i$ is bounded by

$$|\bar{e}_i| \leq 2.807034\left(1 + \sqrt{\frac{1+b}{\ell}}\right)\sigma$$

with probability at least 0.99.

Note 3: Our protocol allows fine-tuning the Gaussian errors by tweaking the standard deviation σ and mean μ for the Gaussian channel. Hence, in our proofs and arguments, we only use the term "target rounded Gaussian".

Lemma 2: Suppose that the number of samples ℓ is superpolynomial, and that Equation (†) is satisfied with some constant b. Then, the errors e_i belong to the target rounded Gaussian distribution.

Proof: Recall that the error $\bar{e}_i$ has two components: one is the noise introduced by the Gaussian channel and second is the error due to regression fitting. The first component is naturally Gaussian. The standard deviation for the second component is of order $\sigma/\sqrt{\ell}$. Hence, it follows from drowning/smudging that for a superpolynomial ℓ, the error distribution for $\bar{e}_i$ is statistically indistinguishable from the Gaussian distribution to which the first component belongs. Therefore, it follows that the final output, $e_i = \lceil \bar{e}_i \rfloor$, of the RGPC protocol belongs to the target rounded Gaussian distribution (see Note 3). ∎

To prove that all conditions in Definition 20 are satisfied for $\mathfrak{M}_h$, it remains to show that no external PPT adversary $\mathcal{A}$ has non-negligible advantage in guessing e_x beforehand. We assume that for an attack query x, $\mathcal{A}$ makes poly(L) queries to $\mathfrak{M}_h$ for $x' \neq x$.

Lemma 3: For an external PPT adversary $\mathcal{A}$, it holds that $\mathfrak{M}_h : x \mapsto e_x$ maps a random element $x \leftarrow \mathbb{Z}$ to a random element e_x in the target rounded Gaussian distribution $\Psi(0, \hat{\sigma}^2)$.

Proof: It follows from Lemma 2 that $\mathfrak{M}_h$ outputs from the target rounded Gaussian distribution. Note the following straightforward observations:

- Since each coefficient of $f(x)$ is randomly sampled from $\mathbb{Z}_m$, $f(x)$ is a random function.
- The inputs to $f(x)$, $x \leftarrow \mathbb{Z}$, are sampled randomly.
- The Gaussian channel introduces a noise ε_x to $f(x)$, that is drawn i.i.d. from a Gaussian distribution $\mathcal{N}(0, \sigma^2)$ [9], [11], [12], [15], [16], [17], [18], [19], [20]. Hence, the receiving parties get a random element $f(x) + \varepsilon_x$.
- It follows from the observations stated above that $\lceil |f(x) - h(x)| \rfloor$ outputs a random element from the target rounded Gaussian $\Psi(0, \hat{\sigma}^2)$.

Hence, $\mathfrak{M}_h : x \mapsto e_x$ is a deterministic mapping that maps each of the ℓ inputs $\{x_i\}_{i=1}^{\ell}$ to an element e_x in the desired rounded Gaussian $\Psi(0, \hat{\sigma}^2)$ such that all conditions from Definition 20 are satisfied. It follows that given an input x not seen before, no external PPT adversary $\mathcal{A}$ has non-negligible advantage in guessing e_x. ∎

VII. MUTUAL INFORMATION ANALYSIS

Definition 27: Let f_X be the p.d.f. of a continuous random variable X. Then, the *differential entropy* of X is

$$H(X) = -\int f_X(x) \log f_X(x)\, dx.$$

Definition 28: The *mutual information*, $I(X; Y)$, of two continuous random variables X and Y with joint p.d.f. $f_{X,Y}$ and marginal p.d.f.'s f_X and f_Y respectively, is

$$I(X; Y) = \int\int f_{X,Y}(x, y) \log\left(\frac{f_{X,Y}(x, y)}{f_X(x) f_Y(y)}\right) dy\, dx.$$

From the above definitions, it is easy to prove that $I(X; Y)$ satisfies the equality:

$$I(X; Y) = H(X) + H(Y) - H(X, Y).$$

Let us now describe our aim. Suppose, for $i = 1, 2, \ldots, \ell$, we have

$$y_i \sim \mathcal{N}(\alpha + \beta x_i, \sigma^2) \quad \text{and} \quad z_i \sim \mathcal{N}(\alpha + \beta w_i, \sigma^2),$$

with $x_i = w_i$ for $i \in [a]$. Let $h_1(x) = \hat{\alpha}_1 x + \hat{\beta}_1$ and $h_2(w) = \hat{\alpha}_2 w + \hat{\beta}_2$ be the linear regression hypotheses obtained from the samples (x_i, y_i) and (w_i, z_i), respectively. Our goal is to compute an expression for the mutual information

$$I((\hat{\alpha}_1, \hat{\beta}_1); (\hat{\alpha}_2, \hat{\beta}_2)).$$

We begin by recalling the following standard fact:

Proposition 11: Let $\mathbf{X} \sim \mathcal{N}(\mathbf{v}, \Sigma)$, where $\mathbf{v} \in \mathbb{R}^d$ and $\Sigma \in \mathbb{R}^{d \times d}$. Then:

$$H(\mathbf{X}) = \frac{1}{2}\log(\det \Sigma) + \frac{d}{2}(1 + \log(2\pi)).$$

We introduce the following notations:

- $X_1 = \sum_{i=1}^{\ell} x_i$, $X_2 = \sum_{i=1}^{\ell} x_i^2$,
- $W_1 = \sum_{i=1}^{\ell} w_i$, $W_2 = \sum_{i=1}^{\ell} w_i^2$,
- $C_1 = \sum_{i=1}^{a} x_i = \sum_{i=1}^{a} w_i$,
- $C_2 = \sum_{i=1}^{a} x_i^2 = \sum_{i=1}^{a} w_i^2$,
- $C_3 = \sum_{i=1}^{\ell} \sum_{j=1, j\neq i}^{\ell} x_i x_j$,
- $\Delta = \ell C_2 - 2C_1 X_1 + a X_2$,

- $\mho = \ell C_2 - 2C_1 W_1 + aW_2$,
- $\aleph = (a-1)C_2 - C_3$,
- $\pounds = 1 + \log(2\pi)$.

Our main result is the following:

Proposition 12: Let $\hat{\alpha}_1$, $\hat{\beta}_1$, $\hat{\alpha}_2$, $\hat{\beta}_2$ be as above. Then

$$H(\hat{\alpha}_1, \hat{\beta}_1) = 2\log\sigma - \frac{1}{2}\log(\ell X_2 - X_1^2) + \pounds,$$
$$H(\hat{\alpha}_2, \hat{\beta}_2) = 2\log\sigma - \frac{1}{2}\log(\ell W_2 - W_1^2) + \pounds,$$

and

$$\begin{aligned} &H(\hat{\alpha}_1, \hat{\beta}_1, \hat{\alpha}_2, \hat{\beta}_2) \\ &= 4\log\sigma - \frac{1}{2}\log\Big((\ell X_2 - X_1^2)(\ell W_2 - W_1^2)\Big) + 2\pounds \\ &\quad + \frac{1}{2}\log\Bigg(1 - \frac{\Delta\mho}{(\ell X_2 - X_1^2)(\ell W_2 - W_1^2)} \\ &\qquad + \frac{\aleph\,(\aleph + \ell(X_2 + W_2) - 2X_1 W_1)}{(\ell X_2 - X_1^2)(\ell W_2 - W_1^2)}\Bigg). \end{aligned}$$

The mutual information between $(\hat{\alpha}_1, \hat{\beta}_1)$ and $(\hat{\alpha}_2, \hat{\beta}_2)$ is:

$$\begin{aligned} &I((\hat{\alpha}_1, \hat{\beta}_1); (\hat{\alpha}_2, \hat{\beta}_2)) \\ &= -\frac{1}{2}\log\Bigg(1 - \frac{\Delta\mho}{(\ell X_2 - X_1^2)(\ell W_2 - W_1^2)} \\ &\quad + \frac{\aleph\,(\aleph + \ell(X_2 + W_2) - 2X_1 W_1)}{(\ell X_2 - X_1^2)(\ell W_2 - W_1^2)}\Bigg). \end{aligned}$$

Proof: The expressions for $H(\hat{\alpha}_1, \hat{\beta}_1)$ and $H(\hat{\alpha}_2, \hat{\beta}_2)$ follow from Propositions 10 and 11, and the expression for $I((\hat{\alpha}_1, \hat{\beta}_1); (\hat{\alpha}_2, \hat{\beta}_2))$ is given by:

$$\begin{aligned} &I((\hat{\alpha}_1, \hat{\beta}_1); (\hat{\alpha}_2, \hat{\beta}_2)) \\ &\quad = H(\hat{\alpha}_1, \hat{\beta}_1) + H(\hat{\alpha}_2, \hat{\beta}_2) - H(\hat{\alpha}_1, \hat{\beta}_1, \hat{\alpha}_2, \hat{\beta}_2). \end{aligned}$$

It remains to derive the expression for $H(\hat{\alpha}_1, \hat{\beta}_1, \hat{\alpha}_2, \hat{\beta}_2)$. First, define the following matrices:

$$\mathbf{X} = \begin{pmatrix} 1 & x_1 \\ 1 & x_2 \\ \vdots & \vdots \\ 1 & x_\ell \end{pmatrix}, \qquad \mathbf{W} = \begin{pmatrix} 1 & w_1 \\ 1 & w_2 \\ \vdots & \vdots \\ 1 & w_\ell \end{pmatrix}.$$

Then

$$\begin{aligned} \hat{\boldsymbol{\theta}} := \begin{pmatrix} \hat{\alpha}_1 \\ \hat{\beta}_1 \\ \hat{\alpha}_2 \\ \hat{\beta}_2 \end{pmatrix} &= \begin{pmatrix} \alpha \\ \beta \\ \alpha \\ \beta \end{pmatrix} + \begin{pmatrix} \mathbf{X}^\nabla \mathbf{X}^T \mathbf{U} \\ \mathbf{W}^\nabla \mathbf{W}^T \mathbf{V} \end{pmatrix} \\ &= \begin{pmatrix} \alpha \\ \beta \\ \alpha \\ \beta \end{pmatrix} + \begin{pmatrix} \mathbf{X}^\nabla \mathbf{X}^T & 0 \\ 0 & \mathbf{W}^\nabla \mathbf{W}^T \end{pmatrix} \begin{pmatrix} \mathbf{U} \\ \mathbf{V} \end{pmatrix}, \end{aligned}$$

where $\mathbf{U}, \mathbf{V} \sim \mathcal{N}(0, \sigma^2 \mathbf{I}_\ell)$, $\mathbf{X}^\nabla = (\mathbf{X}^T\mathbf{X})^{-1}$ and $\mathbf{W}^\nabla = (\mathbf{W}^T\mathbf{W})^{-1}$. Hence, it follows that:

$$\begin{aligned} \mathrm{var}(\hat{\boldsymbol{\theta}}) = &\begin{pmatrix} \mathbf{X}^\nabla \mathbf{X}^T & 0 \\ 0 & \mathbf{W}^\nabla \mathbf{W}^T \end{pmatrix} \\ &\cdot \mathrm{var}\begin{pmatrix} \mathbf{U} \\ \mathbf{V} \end{pmatrix} \begin{pmatrix} \mathbf{X}\mathbf{X}^\nabla & 0 \\ 0 & \mathbf{W}\mathbf{W}^\nabla \end{pmatrix}. \end{aligned}$$

For any matrix $\mathbf{M} = (M_{i,j})$, let $[\mathbf{M}]_a$ denote the matrix with the same dimensions as $\mathbf{M}$, and with entries

$$([\mathbf{M}]_a)_{i,j} = \begin{cases} M_{i,j} & \text{if } i, j \le a, \\ 0 & \text{otherwise.} \end{cases}$$

Note that

$$\mathrm{var}\begin{pmatrix} \mathbf{U} \\ \mathbf{V} \end{pmatrix} = \begin{pmatrix} \sigma^2 \mathbf{I}_\ell & \sigma^2 [\mathbf{I}_\ell]_a \\ \sigma^2 [\mathbf{I}_\ell]_a & \sigma^2 \mathbf{I}_\ell \end{pmatrix},$$

which implies that

$$\mathrm{var}(\hat{\boldsymbol{\theta}}) = \sigma^2 \begin{pmatrix} \mathbf{X}^\nabla & [\mathbf{X}^\nabla \mathbf{X}^T]_a (\mathbf{W}\mathbf{W}^\nabla) \\ [\mathbf{W}^\nabla \mathbf{W}^T]_a (\mathbf{X}\mathbf{X}^\nabla) & \mathbf{W}^\nabla \end{pmatrix}.$$

$$\det(\mathrm{var}(\hat{\boldsymbol{\theta}})) = \sigma^8 \det(\mathbf{X}^\nabla - \mathbf{B}(\mathbf{W}^\nabla)^{-1}\mathbf{C}) \det(\mathbf{W}^\nabla),$$

where

$$\mathbf{X}^\nabla = (\mathbf{X}^T\mathbf{X})^{-1} = \begin{pmatrix} \frac{X_2}{\ell X_2 - X_1^2} & -\frac{X_1}{\ell X_2 - X_1^2} \\ -\frac{X_1}{\ell X_2 - X_1^2} & \frac{\ell}{\ell X_2 - X_1^2} \end{pmatrix},$$

$$\begin{aligned} \mathbf{B} &= [\mathbf{X}^\nabla \mathbf{X}^T]_a (\mathbf{W}\mathbf{W}^\nabla) \\ &= \begin{pmatrix} \frac{\sum_{i=1}^a (X_2 - x_i X_1)(W_2 - w_i W_1)}{(\ell X_2 - X_1^2)(\ell W_2 - W_1^2)} & \frac{\sum_{i=1}^a (\ell w_i - W_1)(X_2 - x_i X_1)}{(\ell X_2 - X_1^2)(\ell W_2 - W_1^2)} \\ \frac{\sum_{i=1}^a (\ell x_i - X_1)(W_2 - w_i W_1)}{(\ell X_2 - X_1^2)(\ell W_2 - W_1^2)} & \frac{\sum_{i=1}^a (\ell x_i - X_1)(\ell w_i - W_1)}{(\ell X_2 - X_1^2)(\ell W_2 - W_1^2)} \end{pmatrix}, \end{aligned}$$

$$\begin{aligned} \mathbf{C} &= [\mathbf{W}^\nabla \mathbf{W}^T]_a (\mathbf{X}\mathbf{X}^\nabla) \\ &= \begin{pmatrix} \frac{\sum_{i=1}^a (X_2 - x_i X_1)(W_2 - w_i W_1)}{(\ell X_2 - X_1^2)(\ell W_2 - W_1^2)} & \frac{\sum_{i=1}^a (\ell x_i - X_1)(W_2 - w_i W_1)}{(\ell X_2 - X_1^2)(\ell W_2 - W_1^2)} \\ \frac{\sum_{i=1}^a (\ell w_i - W_1)(X_2 - x_i X_1)}{(\ell X_2 - X_1^2)(\ell W_2 - W_1^2)} & \frac{\sum_{i=1}^a (\ell x_i - X_1)(\ell w_i - W_1)}{(\ell X_2 - X_1^2)(\ell W_2 - W_1^2)} \end{pmatrix}, \end{aligned}$$

$$\mathbf{W}^\nabla = (\mathbf{W}^T\mathbf{W})^{-1} = \begin{pmatrix} \ell & W_1 \\ W_1 & W_2 \end{pmatrix}^{-1}.$$

After a lengthy computation, we obtain the following expression for $\det(\mathrm{var}(\hat{\boldsymbol{\theta}}))$:

$$\begin{aligned} &\frac{\sigma^8}{(\ell X_2 - X_1^2)(\ell W_2 - W_1^2)}\Bigg(1 - \frac{\Delta\mho}{(\ell X_2 - X_1^2)(\ell W_2 - W_1^2)} \\ &\qquad + \frac{\aleph\,(\aleph + \ell(X_2 + W_2) - 2X_1 W_1)}{(\ell X_2 - X_1^2)(\ell W_2 - W_1^2)}\Bigg). \end{aligned}$$

The expression for $H(\hat{\alpha}_1, \hat{\beta}_1, \hat{\alpha}_2, \hat{\beta}_2)$ follows by applying Proposition 11. ∎

VIII. LEARNING WITH LINEAR REGRESSION (LWLR)

In this section, we define LWLR and reduce its hardness to LWE. It is very important to recall that, as mentioned in Note 3, our RGPC protocol allows freedom in tweaking the target (rounded) Gaussian distribution $\Psi(0, \hat{\sigma}^2)$ by simply selecting the desired standard deviation σ. Therefore, when referring to the desired (rounded) Gaussian distribution in the hardness proofs, we use $\Psi(0, \hat{\sigma}^2)$ (or $\Psi(0, \hat{\sigma}^2)$ mod m, i.e., $\Psi_m(0, \hat{\sigma}^2)$) without divulging into the specific value of σ.

Let $\mathcal{P} = \{P_i\}_{i=1}^n$ be a set of n parties.

Definition 29: For modulus m and a uniformly sampled $a \leftarrow \mathbb{Z}_m^w$, the learning with linear regression (LWLR) distribution $\text{LWLR}_{s,m,w}$ over $\mathbb{Z}_m^w \times \mathbb{Z}_m$ is defined as: $(a, x + e_x)$, where $x = \langle a, s \rangle$ and $e_x \in \Psi(0, \hat{\sigma}^2)$ is a rounded Gaussian error generated by the RGPC protocol, on input x.

Theorem 5: For modulus m, security parameter L, $\ell = g(\mathsf{L})$ samples (where g is a superpolynomial function), PPT adversary $\mathcal{A} \notin \mathcal{P}$, some distribution over secret $s \in \mathbb{Z}_m^w$, and a deterministic mapping $\mathfrak{M}_h : \mathbb{Z} \to \Psi(0, \hat{\sigma}^2)$ generated by the RGPC protocol, where $\Psi(0, \hat{\sigma}^2)$ is the target rounded Gaussian distribution, solving decision-LWLR$_{s,m,w}$ is at least as hard as solving the decision-LWE$_{s,m,w}$ problem for the same distribution over s.

Proof: Recall from Lemma 2 that, since ℓ is superpolynomial, the errors belong to the desired rounded Gaussian distribution $\Psi(0, \hat{\sigma}^2)$. As given, for a fixed secret $s \in \mathbb{Z}_m^w$, a decision-$\text{LWLR}_{s,m,w}$ instance is defined as $(a, x + e_x)$ for $a \xleftarrow{\$} \mathbb{Z}_m^w$ and $x = \langle a, s \rangle$. Recall that a decision-$\text{LWE}_{s,m,w}$ instance is defined as $(a, \langle a, s \rangle + e)$ for $a \leftarrow \mathbb{Z}_m^w$ and $e \leftarrow \chi$ for a rounded (or discrete) Gaussian distribution χ. We know from Lemma 3 that $\mathfrak{M}_h$ is a deterministic mapping from random inputs $x \leftarrow \mathbb{Z}$ to errors $e_x \in \Psi(0, \hat{\sigma}^2)$. We define the following two games:

- $\mathfrak{G}_1$: in this game, we begin by fixing a secret s. Each query from the attacker is answered with an $\text{LWLR}_{s,m,w}$ instance as: $(a, x + e_x)$ for a unique $a \xleftarrow{\$} \mathbb{Z}_m^w$, and $x = \langle a, s \rangle$. The error $e_x \in \Psi(0, \hat{\sigma}^2)$ is generated as: $e_x = \mathfrak{M}_h(x)$.
- $\mathfrak{G}_2$: in this game, we begin by fixing a secret s. Each query from the attacker is answered with an $\text{LWE}_{s,m,w}$ instance as: $(a, \langle a, s \rangle + e)$ for $a \xleftarrow{\$} \mathbb{Z}_m^w$ and $e \leftarrow \Psi(0, \tilde{\sigma}^2)$, where $\Psi(0, \tilde{\sigma}^2)$ denotes a rounded Gaussian distribution that is suitable for sampling LWE errors.

Let the adversary $\mathcal{A}$ be able to distinguish $\text{LWLR}_{s,m,w}$ from $\text{LWE}_{s,m,w}$ with some non-negligible advantage, i.e., $Adv_{\mathcal{A}}(\mathfrak{G}_1, \mathfrak{G}_2) \geq \varphi(w)$ for a non-negligible function φ. Hence, it follows that $Adv_{\mathcal{A}}(\Psi(0, \tilde{\sigma}^2), \Psi(0, \hat{\sigma}^2)) \geq \varphi(w)$. However, we have already established in Lemma 3 that $\mathfrak{M}_h$ is random to $\mathcal{A} \notin \mathcal{P}$. Furthermore, we know that $\hat{\sigma}$ can be brought arbitrarily close to $\tilde{\sigma}$ (see Note 3). Therefore, for appropriate Gaussian parameters, it holds that $Adv_{\mathcal{A}}(\Psi(0, \tilde{\sigma}^2), \Psi(0, \hat{\sigma}^2)) \leq \eta(w)$ for a negligible function η, which directly leads to $Adv_{\mathcal{A}}(\mathfrak{G}_1, \mathfrak{G}_2) \leq \eta(w)$. Hence, for any distribution over a secret $s \in \mathbb{Z}_m^w$, solving decision-$\text{LWLR}_{s,m,w}$ is at least as hard as solving the decision-$\text{LWE}_{s,m,w}$ problem for the same distribution over s. ■

IX. STAR-SPECIFIC KEY-HOMOMORPHIC PRFs

In this section, we use LWLR to construct the first star-specific key-homomorphic (SSKH) PRF family. We adapt the key-homomorphic PRF construction from [96] by replacing the deterministic errors generated from the rounding function in LWR with the errors produced via the deterministic mapping, generated by our RGPC protocol.

A. BACKGROUND

For the sake of completeness, we begin by recalling the key-homomorphic PRF construction from [96]. Let T be a full binary tree with at least one node, i.e., every non-leaf node in T has two children. Let $T.r$ and $T.l$ denote its right and left subtree, respectively, and $\lfloor \cdot \rceil_p$ denote the rounding function from LWR (see Section III-A for an introduction to LWR).

Let $q \geq 2$, $d = \lceil \log q \rceil$, and $x[i]$ denote the i^{th} bit of a bit-string x. Define a gadget vector as:

$$g = (1, 2, 4, \ldots, 2^{d-1}) \in \mathbb{Z}_q^d.$$

Define a decomposition function $g^{-1} : \mathbb{Z}_q \to \{0,1\}^d$ such that $g^{-1}(a)$ is a "short" vector and $\forall a \in \mathbb{Z}_q$, it holds that: $\langle g, g^{-1}(a) \rangle = a$, where $\langle \cdot \rangle$ denotes the inner product. Function g^{-1} is defined as:

$$g^{-1}(a) = (x[0], x[1], \ldots, x[d-1]) \in \{0,1\}^d,$$

where $a = \sum_{i=0}^{d-1} x[i] \cdot 2^i$ is the binary representation of a. The gadget vector is used to define the gadget matrix G as:

$$G = I_w \otimes g = \text{diag}(g, \ldots, g) \in \mathbb{Z}_q^{w \times wd},$$

where I_w is the $w \times w$ identity matrix and $\otimes$ denotes the Kronecker product [285]. The binary decomposition function, g^{-1}, is applied entry-wise to vectors and matrices over $\mathbb{Z}_q$. Thus, g^{-1} can be extended to get another deterministic decomposition function

$$G^{-1} : \mathbb{Z}_q^{w \times u} \to \{0,1\}^{wd \times u}$$

such that $G \cdot G^{-1}(A) = A$.

Given uniformly sampled matrices, $A_0, A_1 \in \mathbb{Z}_q^{w \times wd}$, define function $A_T(x) : \{0,1\}^{|T|} \to \mathbb{Z}_q^{w \times wd}$ as:

$$A_T(x) = \begin{cases} A_x & \text{if } |T| = 1, \\ A_{T.l}(x_l) \cdot G^{-1}(A_{T.r}(x_r)) & \text{otherwise,} \end{cases} \tag{6}$$

where $|T|$ denotes the total number of leaves in T and $x \in \{0,1\}^{|T|}$ such that $x = x_l || x_r$ for $x_l \in \{0,1\}^{|T.l|}$ and $x_r \in \{0,1\}^{|T.r|}$. The key-homomorphic PRF family is defined as:

$$\mathcal{F}_{A_0, A_1, T, p} = \left\{ F_s : \{0,1\}^{|T|} \to \mathbb{Z}_p^{wd} \right\},$$

where $p \leq q$ is the modulus. A member of the function family $\mathcal{F}$ is indexed by the seed $s \in \mathbb{Z}_q^w$ as:

$$F_s(x) = \lfloor s \cdot A_T(x) \rceil_p.$$

B. OUR CONSTRUCTION

We are now ready to present the construction for the first SSKH PRF family.

1) SETTINGS

Let $\mathcal{P} = \{P_i\}_{i=1}^n$ be a set of n honest parties, that are arranged as the vertices of an interconnection graph $G = (V, E)$, which is comprised of S_k stars $\partial_1, \ldots, \partial_\rho$, i.e., each subgraph ∂_i is a star with k leaves. As mentioned in Section VI-A, we assume that each party in ∂_i is connected to ∂_i's central hub C_i via two channels: one Gaussian channel with the desired parameters and another error corrected channel. Each party in $\mathcal{P}$ receives parameters A_0, A_1, i.e., all parties are provisioned with identical parameters. Hence, physical layer communications and measurements are the exclusive source of variety and secrecy in this protocol. Since we are dealing with vectors, the data points for linear regression analysis, i.e., the messages exchanged among the parties in the stars, are of the form $\{(\mathbf{x}_i, \mathbf{y}_i)\}_{i=1}^\ell$, where $x_i, y_i \in \mathbb{Z}^{wd}$. Consequently, the target rounded Gaussian distribution becomes $\Psi^{wd}(0, \hat{\sigma}^2)$. Let the parties in each star exchange messages in accordance to the RGPC protocol such that messages from different central hubs C_i, C_j ($\forall i, j \in [\rho]$; $i \neq j$) are distinguishable to the parties belonging to multiple stars.

2) CONSTRUCTION

Without loss of generality, consider a star $\partial_i \subseteq V(G)$. Each party in ∂_i follows the RGPC protocol to generate its linear regression hypothesis $h^{(\partial_i)}$. Parties in star ∂_i construct a ∂_i-specific key-homomorphic PRF family, whose member $F_{s_i}^{(\partial_i)}(x)$, indexed by the key/seed $s_i \in \mathbb{Z}_m^w$, is defined as:

$$F_{s_i}^{(\partial_i)}(x) = s_i \cdot A_T(x) + e_b^{(\partial_i)} \bmod m, \tag{7}$$

where $A_T(x)$ is as defined by Equation (6), $b = s_i \cdot A_T(x)$, and $e_b^{(\partial_i)} = \mathfrak{M}_{h^{(\partial_i)}}(b)$ denotes a rounded Gaussian error computed by the deterministic mapping $\mathfrak{M}_{h^{(\partial_i)}}$ on input b. Recall that $\mathfrak{M}_{h^{(\partial_i)}}$ is generated by our RGPC protocol from hypothesis $h^{(\partial_i)}$. The star-specific secret s_i can be generated by using a reconfigurable antenna (RA) [286], [287] at the central hub, C_i, and thereafter reconfiguring it to randomize the error-corrected channel between itself and the parties in ∂_i. Specifically, s_i can be generated via the following procedure:

1) After performing the RGPC protocol, each party $P_j \in \partial_i$ sends a random $r_j \in [\ell]$ to C_i via the error corrected channel. C_i broadcasts r_j to all parties in ∂_i and randomizes all error-corrected channels by reconfiguring its RA. If two parties' r_j values arrive simultaneously, then C_i randomly discards one of them and notifies the corresponding party to resend another random value. This ensures that the channels are re-randomized after receiving each r_j value. By the end of this cycle, each party receives k random values $\{r_j\}_{j=1}^k$. Let $\wp_i$ denote the set of all r_j values received by the parties in ∂_i.
2) Each party in ∂_i computes $\bigoplus_{r_j \in \wp_i} r_j = s \bmod m$.
3) This procedure is repeated to extract the required number of bits to generate the vector s_i.

Since C_i randomizes all its channels by simply reconfiguring its RA, no active or passive adversary can compromise all $r_j \in \wp_i$ values [286], [287], [288], [289], [290], [291], [292], [293]. In honest settings, secrecy of the star-specific secret s_i, generated by the aforementioned procedure, follows directly from the following three facts:

(i) All parties are honest.
(ii) All data points $\{x_i\}_{i=1}^\ell$ are randomly sampled integers, i.e., $x_i \xleftarrow{\$} \mathbb{Z}$.
(iii) The coefficients of $f(x)$, and hence $f(x)$ itself, are random.

In the following section, we examine the settings with active/passive and internal/external adversaries. Note that the protocol does not require the parties to share their identities. Hence, the above protocol is trivially anonymous over anonymous channels (see [294], [295] for surveys on anonymous communications). Since anonymity has multiple applications in cryptographic protocols [187], [275], [276], [296], [297], [298], [299], [300], [301], [302], [303], [304], [305], [306], it is a useful feature of our construction.

C. MAXIMUM NUMBER OF SSKH PRFs AND DEFENSES AGAINST VARIOUS ATTACKS

In this section, we employ our results from Section V to derive the maximum number of SSKH PRFs that can be constructed by a set of n parties. Recall that we use the terms star and star graph interchangeably. We know that in order to construct a SSKH PRF family, the parties are arranged in an interconnection graph G wherein the — possibly overlapping — subsets of $\mathcal{P}$ form different star graphs, $\partial_1, \ldots, \partial_\rho$, within G. We assume that for all $i \in [\rho]$, it holds that: $|\partial_i| = k$. Recall from Section V that we derived various bounds on the size of the following set families $\mathcal{H}$ defined over a set of n elements:

1) $\mathcal{H}$ is an at most t-intersecting k-uniform family,
2) $\mathcal{H}$ is a maximally cover-free at most t-intersecting k-uniform family.

We set n to be the number of vertices in G. Hence, k represents the size of each star with t being equal to (or greater than) $\max_{i \neq j}(|\partial_i \cap \partial_j|)$.

In our SSKH PRF construction, no member of a star ∂ has any secrets that are hidden from the other members of ∂. Also, irrespective of their memberships, all parties are provisioned with identical set of initial parameters. The secret keys and regression models are generated via physical layer communications and collaboration. Due to these facts, the parties in our SSKH PRF construction must be either honest or semi-honest but non-colluding. We consider these

factors while computing the maximum number of SSKH PRFs that can be constructed securely against various types of adversaries. For a star ∂, let $\mathcal{O}_\partial$ denote an oracle for the SSKH PRF $F_s^{(\partial)}$, i.e., on receiving input x, $\mathcal{O}_\partial$ outputs $F_s^{(\partial)}(x)$. Given oracle access to $\mathcal{O}_\partial$, it must holds that for a PPT adversary $\mathcal{A}$ who is allowed poly(L) queries to $\mathcal{O}_\partial$, the SSKH PRF $F_s^{(\partial)}$ remains indistinguishable from a uniformly random function U — defined over the same domain and range as $F_s^{(\partial)}$.

Let E_i denote the set of Gaussian and error-corrected channels that are represented by the edges in star ∂_i.

1) EXTERNAL ADVERSARY WITH ORACLE ACCESS

In this case, the adversary can only query the oracle for the SSKH PRF, and hence the secrecy follows directly from the hardness of LWLR. Therefore, at most t-intersecting k-uniform families are sufficient for this case, i.e., we do not need the underlying set family $\mathcal{H}$ to be maximally cover-free. Moreover, $t = k - 1$ suffices for this case because maximum overlap between different stars can be tolerated. Hence, it follows from Proposition 7 (in SectionV) that the maximum number of SSKH PRFs that can be constructed is:

$$\zeta \sim \frac{n^k}{k!}.$$

2) EAVESDROPPING ADVERSARY WITH ORACLE ACCESS

Wyner's wiretap model [307] models an eavesdropper observing a degraded version of the information exchanged on the main channel through a wiretap channel. Let $\mathcal{A}$ be an eavesdropping adversary with wiretap channels, observing a subset E' of Gaussian and/or error-corrected channels between parties and central hubs. Furthermore, assume that $\mathcal{A}$ has oracle access to the traget star's SSKH PRF. Without loss of generality, let ∂_i be the target star. Also, note that there can be more than one target stars. Let us analyze the security with respect to this adversary.

1) Secrecy of s_i: After each party $P_z \in \partial_i$ contributes to the generation of s_i by sending a random value r_z to C_i, which then broadcasts r_z to all parties in ∂_i, C_i randomizes all error-corrected channels by reconfiguring its RA. This means that $\mathcal{A}$ cannot compromise all r_z values. Hence, it follows that no information about s_i is leaked to $\mathcal{A}$. Furthermore, it follows from the wiretap channel model that $\mathcal{A}$ cannot get precise value of any r_z.
2) Messages exchanged via the channels in E': leakage of enough messages exchanged within star ∂_i would allow $\mathcal{A}$ to closely approximate the deterministic mapping $\mathfrak{M}_{h^{(\partial_i)}}$. Note that for this attack to work, $\mathcal{A}$ must successfully eavesdrop on enough channels in ∂_i. However, since $\mathcal{A}$ is an outsider with only access to wiretap channels, it follows from Proposition 12, and known information-theoretic results about physical layer communications [308], [309] and (Gaussian) wiretap eavesdropping [307], [310], [311], [312], [313], [314], [315], [316], [317] that $\mathcal{A}$ cannot gain any non-negligible information on $\mathfrak{M}_{h^{(\partial_i)}}$.

Hence, an eavesdropping adversary with wiretap channels and oracle access has no non-negligible advantage over an external adversary with oracle access. Therefore, it follows that the maximum number of SSKH PRFs that can be constructed in this case is:

$$\zeta \sim \frac{n^k}{k!}.$$

3) NON-COLLUDING SEMI-HONEST PARTIES

Let $\mathcal{P}_{\partial_i} \subseteq \mathcal{P}$ denote the set of parties that form the star ∂_i — in addition to the central hub C_i. Suppose that some or all parties in $\mathcal{P}$ are semi-honest, i.e., they follow the protocol correctly but try to gain/infer more information than what is allowed by the protocol. Further suppose that the parties do not collude with each other. However, this assumption is redundant if all malicious parties belong to same set of stars because broadcast in our protocol provides malicious parties with all the information exchanged in the stars they belong to. The restriction of non-collusion is required when at least one pair of malicious parties are members of different sets of stars. In such settings, the only way any party $P_j \notin \partial_i$ can gain additional information about the SSKH PRF $F_{s_i}^{(\partial_i)}$ is to (mis)use its membership of other stars. For instance, if $P_j \in \mathcal{P}_{\partial_d}, \mathcal{P}_{\partial_j}, \mathcal{P}_{\partial_o}$ and $\mathcal{P}_{\partial_i} \subset \mathcal{P}_{\partial_o} \cup \mathcal{P}_{\partial_j} \cup \mathcal{P}_{\partial_d}$, then because the parties send identical messages to all central hubs they are connected to, it follows that $H(F_{s_i}^{(\partial_i)} | P_j) = 0$. This follows trivially because P_j can compute s_i. Having maximally cover-free families eliminates this vulnerability against non-colluding semi-honest parties. This holds because with members of a maximally cover-free family denoting unique stars in G, the following can never hold true for any $\mathcal{P}_{\partial_i}$:

$$\mathcal{P}_{\partial_i} \subseteq \bigcup_{j \in \varrho} \mathcal{P}_{\partial_j},$$

where $\varrho \subseteq [\rho] - \{i\}$. Hence, it follows from Proposition 8 that the maximum number of SSKH PRFs that can be constructed with non-colluding semi-honest parties is at least Cn for some positive real number $C < 1$.

Thus, in order to construct SSKH PRFs that are secure against all types of adversaries and threat models discussed in this section, the underlying family of sets must be maximally cover-free, at most $(k-1)$-intersecting and k-uniform.

4) MAN-IN-THE-MIDDLE

Physical-layer-based key generation schemes exploit the channel reciprocity for secret key extraction, which can achieve information-theoretic secrecy against eavesdroppers. However, these schemes have been shown to be vulnerable against man-in-the-middle (MITM) attacks. During a typical MITM attack, the adversary creates separate connection(s) with the communicating node(s) and relays altered transmission packets to them. Eberz et al. [318] demonstrated a practical MITM attack against RSS-based key generation protocols [15], [319], wherein the MITM

adversary $\mathcal{A}$ exploits the same channel characteristics as the target/communicating parties P_1, P_2. To summarize, in the attack from [318], $\mathcal{A}$ injects packets that cause a similar channel measurement at both P_1 and P_2. This attack enables $\mathcal{A}$ to recover up to 47% of the secret bits generated by P_1 and P_2.

To defend against such attacks, we can apply techniques that allow us to detect an MITM attack over physical layer [320], and if one is detected, the antenna of ∂_i's central hub, C_i, can be reconfigured to randomize all channels in ∂_i [290]. This only requires a reconfigurable antenna (RA) at each central hub. An RA can swiftly reconfigure its radiation pattern, polarization, and frequency by rearranging its antenna currents [286], [287]. It has been shown that due to multipath resulting from having an RA, even small variation by the RA can create large variations in the channel, effectively creating fast varying channels with a random distribution [321]. One way an RA may randomize the channels is by randomly selecting antenna configurations in the transmitting array at the symbol rate, leading to a random phase and amplitude multiplied to the transmitted symbol. The resulting randomness is compensated by appropriate element weights so that the intended receiver does not experience any random variations. In this manner, an RA can be used to re-randomize the channel and hence break the temporal correlation of the channels between $\mathcal{A}$ and the attacked parties, while preserving the reciprocity of the other channels.

Therefore, even if an adversary $\mathcal{A}$ is able to perform successful injection in communication round ß, its channels with the attacked parties would be randomly modified (by the RA) when it attempts injections in round ß+1. On the other hand, the channels between the parties in star ∂_i and the central hub C_i remain reciprocal, i.e., they can still make correct/identical measurements. Hence, by reconfiguring C_i's RA, we can prevent further injections from $\mathcal{A}$ without affecting the legitimate parties' ability to make correct channel measurements. Further details on this defense technique are beyond the scope of this paper. For detailed introduction to the topic and its applications in different settings, we refer the interested reader to [286], [287], [288], [289], [290], [291], [292], and [293]. In this manner, channel state randomization can be used to effectively reduce an MITM attack to the less harmful jamming attack [322]. See [323] for a thorough introduction to jamming and anti-jamming techniques.

D. RUNTIME AND KEY SIZE

We know that the complexity of a single evaluation of the key-homomorphic PRF from [96] is $\Theta(|T|w^\omega \log^2 m)$ ring operations in $\mathbb{Z}_m$, where $\omega \in [2, 2.37286]$ is the exponent of matrix multiplication [324], [325]. Using the fast integer multiplication algorithm from [326], this gives a time complexity of $\Theta(|T|w^\omega m \log^3 m)$. The time taken by the setup of our SSKH PRF construction is equal to the time required by our RGPC algorithm to find the optimal hypothesis, which we know from Section VI-D to be $\Theta(\ell)$ additions and multiplications. If B is an upper bound on x_i and y_i, then the time complexity is $O(\ell B \log B)$. Once the optimal hypothesis is known, it takes $\Theta(wm \log^2 m)$ time to generate a deterministic LWLR error for a single input. Hence, after the initial setup, the time complexity of a single function evaluation of our SSKH PRF remains $\Theta(|T|w^\omega m \log^3 m)$.

Similarly, the key size for our SSKH PRF family is the same as that of the key-homomorphic PRF family from [96]. Specifically, for security parameter L and 2^{L} security against the well known lattice reduction algorithms [327], [328], [329], [330], [331], [332], [333], [334], [335], [336], [337], [338], [339], [340], [341], [342], [343], [344], [345], [346], [347], [348], [349], [350], the key size for our SSKH PRF family is L.

E. CORRECTNESS AND SECURITY

Recall that LWR employs rounding to hide all but some of the most significant bits of $\lfloor s \cdot A \rceil_p$; therefore, the rounded-off bits become the deterministic error. On the other hand, our solution, i.e., LWLR, uses linear regression hypothesis to generate the desired rounded Gaussian errors, which are derived from the (independent) errors occurring in the physical layer communications over Gaussian channel(s). For the sake of simplicity, the proofs assume honest parties in the absence of any adversary. For other supported cases, it is easy to adapt the statements of the results according to the bounds/conditions established in Section IX-C.

Recall that the RGPC protocol ensures that all parties in a star ∂ receive an identical dataset $\mathcal{D}$, and therefore arrive at the same linear regression hypothesis $h^{(\partial)}$ and errors $e_b^{(\partial)}$.

Theorem 6: The function family defined by Equation 7 is a SSKH PRF under the decision-LWE assumption.

Proof: We know from Theorem 5 that for $s_i \xleftarrow{\$} \mathbb{Z}_m^w$ and a superpolynomial number of samples ℓ, the LWLR instances generated in Equation 7 are as hard as LWE — to solve for s_i (and $e_b^{(\partial_i)}$). The randomness of the function family follows directly from the randomness of s_i and the public parameters, $\mathbf{A}_0, \mathbf{A}_1$. The deterministic behavior follows from the following two facts:

- $A_T(x)$ is a deterministic function,
- the mapping, $\mathfrak{M}_{h^{(\partial_i)}}$, used to generate the errors is deterministic.

Hence, it follows from [96] that the family of functions defined by Equation 7 is a PRF family.

Next, define

$$G_{\mathbf{s}}^{(\partial_i)}(x) = s \cdot \mathbf{A}_T(x) + \lfloor \boldsymbol{\varepsilon}_b^{(\partial_i)} \rceil \bmod m,$$

where $\boldsymbol{\varepsilon}_b^{(\partial_i)}$ is the (raw) Gaussian error corresponding to $\mathbf{b}$ for star ∂_i; define $G_{\mathbf{s}}^{(\partial_j)}$ similarly. Since the errors $\boldsymbol{\varepsilon}_b^{(\partial_i)}$ and $\boldsymbol{\varepsilon}_b^{(\partial_j)}$ are independent Gaussian random variables, each with variance σ^2, it holds that:

$$\begin{aligned}\Pr[G_{\mathbf{s}}^{(\partial_i)}(x) = G_{\mathbf{s}}^{(\partial_j)}(x)] &= \Pr[\lfloor \boldsymbol{\varepsilon}_b^{(\partial_i)} \rceil = \lfloor \boldsymbol{\varepsilon}_b^{(\partial_j)} \rceil] \\ &\leq \Pr[||\boldsymbol{\varepsilon}_b^{(\partial_i)} - \boldsymbol{\varepsilon}_b^{(\partial_j)}||_\infty < 1]\end{aligned}$$

$$= \Pr[|Z| < (\sqrt{2}\sigma)^{-1}]^w$$

where Z is a standard Gaussian random variable.

Furthermore, since the number of samples is superpolynomial in the security parameter L, by drowning/smudging, the statistical distance between $\boldsymbol{e}_b^{(\partial_i)}$ and $\boldsymbol{\varepsilon}_b^{(\partial_i)}$ is negligible (similarly for $\boldsymbol{\varepsilon}_b^{(\partial_j)}$ and $\boldsymbol{e}_b^{(\partial_j)}$). Hence,

$$\begin{aligned}\Pr[F_{\mathbf{s}}^{(\partial_i)}(x) = F_{\mathbf{s}}^{(\partial_j)}(x)] &= \Pr[G_{\mathbf{s}}^{(\partial_i)}(x) = G_{\mathbf{s}}^{(\partial_j)}(x)] + \eta(\mathsf{L}) \\ &\leq \Pr[|Z| < (\sqrt{2}\sigma)^{-1}]^w + \eta(\mathsf{L}),\end{aligned}$$

where $\eta(\mathsf{L})$ is a negligible function in L. By choosing $\delta = \Pr[|Z| < (\sqrt{2}\sigma)^{-1}]$, this function family satisfies Definition 21(i).

Finally, by Chebyshev's inequality and the union bound, for any $\tau > 0$,

$$F_{s_1}^{(\partial)}(x) + F_{s_2}^{(\partial)}(x) = F_{s_1+s_2}^{(\partial)}(x) + e' \bmod m,$$

where each entry of e' lies in $[-3\tau\hat{\sigma}, 3\tau\hat{\sigma}]$ with probability at least $1 - 3/\tau^2$. For example, choosing $\tau = \sqrt{300}$ gives us the bound that the absolute value of each entry is bounded by $\sqrt{2700}\hat{\sigma}$ with probability at least 0.99.

Therefore, the function family defined by Equation 7 is a SSKH PRF family — as defined by Definition 21 — under the decision-LWE assumption. ■

X. CONCLUSION

In this paper, we introduced a novel derandomized variant of the celebrated learning with errors (LWE) problem, called learning with linear regression (LWLR), which derandomizes LWE via deterministic, yet sufficiently independent, errors that are generated by using special linear regression models whose training data consists of physical layer communications over Gaussian channels. Prior to our work, learning with rounding and its variant nearby learning with lattice rounding were the only known derandomized variant of the LWE problem; both of which relied on rounding. LWLR relies on the naturally occurring errors in physical layer communications to derandomize LWE while maintaining its hardness — for specific parameters.

We also introduced star-specific key-homomorphic (SSKH) pseudorandom functions (PRFs), which are directly defined by the physical layer communications among the respective sets of parties that construct them. We used LWLR to construct the first SSKH PRF family. In order to quantify the maximum number of SSKH PRFs that can be constructed by sets of overlapping parties, we derived:

- a formula to compute the mutual information between linear regression models that are generated from overlapping training datasets,
- bounds on the size of at most t-intersecting k-uniform families of sets. We also gave an explicit construction to build such set systems,
- bounds on the size of maximally cover-free at most t-intersecting k-uniform families of sets.

Using these results, we established the maximum number of SSKH PRFs that can be constructed by a given set of parties in the presence of active/passive and internal/external adversaries.

REFERENCES

[1] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," in *Proc. 37th Annu. ACM Symp. Theory Comput.*, May 2005, pp. 84–93.
[2] C. Peikert, "A decade of lattice cryptography," *Found. Trends Theor. Comput. Sci.*, vol. 10, no. 4, pp. 283–424, 2016.
[3] H. Nejatollahi, N. Dutt, S. Ray, F. Regazzoni, I. Banerjee, and R. Cammarota, "Post-quantum lattice-based cryptography implementations: A survey," *ACM Comput. Surv.*, vol. 51, no. 6, pp. 1–41, Nov. 2019.
[4] A. Banerjee, C. Peikert, and A. Rosen, "Pseudorandom functions and lattices," in *Proc. EUROCRYPT*, 2012, pp. 719–737.
[5] A. Tanenbaum and D. Wetherall, *Computer Networks*, 5th ed. London, U.K.: Pearson, 2010.
[6] S. N. Premnath, S. Jana, J. Croft, P. L. Gowda, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "Secret key extraction from wireless signal strength in real environments," *IEEE Trans. Mobile Comput.*, vol. 12, no. 5, pp. 917–930, May 2013.
[7] L. Xiao, L. Greenstein, N. Mandayam, and W. Trappe, "Using the physical layer for wireless authentication in time-variant channels," *IEEE Trans. Wireless Commun.*, vol. 7, no. 7, pp. 2571–2579, Jul. 2008.
[8] J. Zhang, M. H. Firooz, N. Patwari, and S. K. Kasera, "Advancing wireless link signatures for location distinction," in *Proc. 14th ACM Int. Conf. Mobile Comput. Netw.*, Sep. 2008, pp. 26–37.
[9] K. Zeng, "Physical layer key generation in wireless networks: Challenges and opportunities," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 33–39, Jun. 2015.
[10] D. Kapetanovic, G. Zheng, and F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks," *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 21–27, Jun. 2015.
[11] Z. Jiang, J. Zhao, X. Li, J. Han, and W. Xi, "Rejecting the attack: Source authentication for Wi-Fi management frames using CSI information," in *Proc. IEEE INFOCOM*, Apr. 2013, pp. 2544–2552.
[12] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," *IEEE Trans. Inf. Forensics Security*, vol. 5, no. 2, pp. 240–254, Jun. 2010.
[13] C. Ye, A. Reznik, and Y. Shah, "Extracting secrecy from jointly Gaussian random variables," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2006, pp. 2593–2597.
[14] C. Ye, A. Reznik, G. Sternberg, and Y. Shah, "On the secrecy capabilities of ITU channels," in *Proc. IEEE 66th Veh. Technol. Conf.*, Sep. 2007, pp. 2030–2034.
[15] S. Jana, S. N. Premnath, M. Clark, S. K. Kasera, N. Patwari, and S. V. Krishnamurthy, "On the effectiveness of secret key extraction from wireless signal strength in real environments," in *Proc. 15th Annu. Int. Conf. Mobile Comput. Netw.*, Sep. 2009, pp. 321–332.
[16] H. Liu, J. Yang, Y. Wang, and Y. Chen, "Collaborative secret key extraction leveraging received signal strength in mobile wireless networks," in *Proc. IEEE INFOCOM*, Mar. 2012, pp. 927–935.
[17] S. N. Premnath, P. L. Gowda, S. K. Kasera, N. Patwari, and R. Ricci, "Secret key extraction using Bluetooth wireless signal strength measurements," in *Proc. 11th Annu. IEEE Int. Conf. Sens., Commun., Netw. (SECON)*, Jun. 2014, pp. 293–301.
[18] W. Xi, C. Qian, J. Han, K. Zhao, S. Zhong, X.-Y. Li, and J. Zhao, "Instant and robust authentication and key agreement among mobile devices," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2016, pp. 616–627.
[19] Q. Wang, H. Su, K. Ren, and K. Kim, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," in *Proc. IEEE INFOCOM*, Apr. 2011, pp. 1422–1430.
[20] Q. Wang, K. Xu, and K. Ren, "Cooperative secret key generation from phase estimation in narrowband fading channels," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 9, pp. 1666–1674, Oct. 2012.
[21] G. Li, A. Hu, J. Zhang, L. Peng, C. Sun, and D. Cao, "High-agreement uncorrelated secret key generation based on principal component analysis preprocessing," *IEEE Trans. Commun.*, vol. 66, no. 7, pp. 3022–3034, Jul. 2018.

[22] J. Zhang, M. Ding, G. Li, and A. Marshall, "Key generation based on large scale fading," *IEEE Trans. Veh. Technol.*, vol. 68, no. 8, pp. 8222–8226, Aug. 2019.

[23] H. Ruotsalainen, J. Zhang, and S. Grebeniuk, "Experimental investigation on wireless key generation for low-power wide-area networks," *IEEE Internet Things J.*, vol. 7, no. 3, pp. 1745–1755, Mar. 2020.

[24] W. Xu, S. Jha, and W. Hu, "LoRa-key: Secure key generation system for LoRa-based network," *IEEE Internet Things J.*, vol. 6, no. 4, pp. 6404–6416, Aug. 2019.

[25] J. Zhang, A. Marshall, and L. Hanzo, "Channel-envelope differencing eliminates secret key correlation: LoRa-based key generation in low power wide area networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 12, pp. 12462–12466, Dec. 2018.

[26] W. Xu, S. Jha, and W. Hu, "Exploring the feasibility of physical layer key generation for LoRaWAN," in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun./12th IEEE Int. Conf. Big Data Sci. Eng.*, Aug. 2018, pp. 231–236.

[27] G. Margelis, X. Fafoutis, G. Oikonomou, R. Piechocki, T. Tryfonas, and P. Thomas, "Physical layer secret-key generation with discreet cosine transform for the Internet of Things," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2017, pp. 1–6.

[28] Y. E. H. Shehadeh and D. Hogrefe, "A survey on secret key generation mechanisms on the physical layer in wireless networks," *Secur. Commun. Netw.*, vol. 8, no. 2, pp. 332–341, Jan. 2015.

[29] H. V. Poor and R. F. Schaefer, "Wireless physical layer security," *Proc. Nat. Acad. Sci. USA*, vol. 114, no. 1, pp. 19–26, Jan. 2017.

[30] F. Marino, E. Paolini, and M. Chiani, "Secret key extraction from a UWB channel: Analysis in a real environment," in *Proc. IEEE Int. Conf. Ultra-WideBand (ICUWB)*, Sep. 2014, pp. 80–85.

[31] C. Zenger, J. Zimmer, and C. Paar, "Security analysis of quantization schemes for channel-based key extraction," in *Proc. 12th EAI Int. Conf. Mobile Ubiquitous Syst., Comput., Netw. Services*, 2015, pp. 267–272.

[32] C. Zenger, H. Vogt, J. Zimmer, A. Sezgin, and C. Paar, "The passive eavesdropper affects my channel: Secret-key rates under real-world conditions," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2016, pp. 1–6.

[33] M. Edman, A. Kiayias, Q. Tang, and B. Yener, "On the security of key extraction from measuring physical quantities," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 8, pp. 1796–1806, Aug. 2016.

[34] J. Zhang, R. Woods, T. Q. Duong, A. Marshall, Y. Ding, Y. Huang, and Q. Xu, "Experimental study on key generation for physical layer security in wireless communications," *IEEE Access*, vol. 4, pp. 4464–4477, 2016.

[35] M. Ghoreishi Madiseh, S. He, M. L. Mcguire, S. W. Neville, and X. Dong, "Verification of secret key generation from UWB channel observations," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2009, pp. 1–5.

[36] S. T. Hamida, J. Pierrot, and C. Castelluccia, "Empirical analysis of UWB channel characteristics for secret key generation in indoor environments," in *Proc. 21st Annu. IEEE Int. Symp. Pers., Indoor Mobile Radio Commun.*, Sep. 2010, pp. 1984–1989.

[37] B. Zan, M. Gruteser, and F. Hu, "Improving robustness of key extraction from wireless channels with differential techniques," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Jan. 2012, pp. 980–984.

[38] J. L. Park, "The concept of transition in quantum mechanics," *Found. Phys.*, vol. 1, no. 1, pp. 23–33, 1970.

[39] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, pp. 802–803, Oct. 1982.

[40] B. M. Terhal, "Is entanglement monogamous?" *IBM J. Res. Develop.*, vol. 48, no. 1, pp. 71–78, Jan. 2004.

[41] F. Grasselli, *Quantum Cryptography—From Key Distribution to Conference Key Agreement* (Quantum Science and Technology). Cham, Switzerland: Springer, 2021.

[42] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, pp. 145–195, Mar. 2002.

[43] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theor. Comput. Sci.*, vol. 560, pp. 7–11, Dec. 2014.

[44] A. K. Ekert, "Quantum cryptography based on Bell's theorem," *Phys. Rev. Lett.*, vol. 67, no. 6, pp. 661–663, Aug. 1991.

[45] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental quantum cryptography," *J. Cryptol.*, vol. 5, no. 1, pp. 3–28, Jan. 1992.

[46] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, "Quantum random number generation," *NPJ Quantum Inf.*, vol. 2, no. 1, pp. 1–10, Jun. 2016.

[47] P. J. Clarke, R. J. Collins, V. Dunjko, E. Andersson, J. Jeffers, and G. S. Buller, "Experimental demonstration of quantum digital signatures using phase-encoded coherent states of light," *Nature Commun.*, vol. 3, no. 1, pp. 1–15, Nov. 2012.

[48] J. Braun, J. Buchmann, D. Demirel, M. Geihs, M. Fujiwara, S. Moriai, M. Sasaki, and A. Waseda, "LINCOS: A storage system providing long-term integrity, authenticity, and confidentiality," in *Proc. ACM Asia Conf. Comput. Commun. Secur.*, Apr. 2017, pp. 461–468.

[49] D. Unruh, "Universally composable quantum multi-party computation," in *Proc. EUROCRYPT*, 2010, pp. 486–505.

[50] K. Nayak, C. W. Fletcher, L. Ren, N. Chandran, S. Lokam, E. Shi, and V. Goyal, "HOP: Hardware makes obfuscation practical," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, 2017, pp. 1–22.

[51] A. Ahmad, B. Joe, Y. Xiao, Y. Zhang, I. Shin, and B. Lee, "OBFUSCURO: A commodity obfuscation engine on Intel SGX," in *Proc. Netw. Distrib. Syst. Secur. Symp.*, 2019.

[52] T. Suzuki, K. Emura, T. Ohigashi, and K. Omote, "Verifiable functional encryption using Intel SGX," *Cryptol. ePrint Arch.*, vol. 2020, pp. 1–25, Jan. 2020. [Online]. Available: https://eprint.iacr.org/2020/1221

[53] W. Zhou, Y. Cai, Y. Peng, S. Wang, K. Ma, and F. Li, "VeriDB: An SGX-based verifiable database," in *Proc. Int. Conf. Manage. Data*, Jun. 2021, pp. 2182–2194.

[54] D. Gupta, B. Mood, J. Feigenbaum, K. Butler, and P. Traynor, "Using Intel software guard extensions for efficient two-party secure function evaluation," in *Financial Cryptography and Data Security*, 2016, pp. 302–318.

[55] A. Brandão, J. S. Resende, and R. Martins, "Hardening cryptographic operations through the use of secure enclaves," *Comput. Secur.*, vol. 108, Sep. 2021, Art. no. 102327.

[56] C. Priebe, K. Vaswani, and M. Costa, "EnclaveDB: A secure database using SGX," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2018, pp. 264–278.

[57] M. H. Rachid, R. Riley, and Q. Malluhi, "Enclave-based oblivious RAM using Intel's SGX," *Comput. Secur.*, vol. 91, Apr. 2020, Art. no. 101711.

[58] Y. Ren, J. Li, Z. Yang, P. P. C. Lee, and X. Zhang, "Accelerating encrypted deduplication via SGX," in *Proc. USENIX*, 2021, pp. 303–316.

[59] T. Hoang, R. Behnia, Y. Jang, and A. A. Yavuz, "MOSE: Practical multi-user oblivious storage via secure enclaves," in *Proc. 10th ACM Conf. Data Appl. Secur. Privacy*, Mar. 2020, pp. 17–28.

[60] A. Koch, "Cryptographic protocols from physical assumptions," Ph.D. dissertation, Karlsruher Institut für Technologie (KIT), Karlsruhe, Germany, 2019.

[61] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical one-way functions," *Science*, vol. 297, no. 5589, pp. 2026–2030, Sep. 2002.

[62] M. Doosti, N. Kumar, E. Kashefi, and K. Chakraborty, "On the connection between quantum pseudorandomness and quantum hardware assumptions," *Quantum Sci. Technol.*, vol. 7, no. 3, Jul. 2022, Art. no. 035004.

[63] R. Canetti and M. Fischlin, "Universally composable commitments (extended abstract)," in *Proc. CRYPTO*, 2001, pp. 19–40.

[64] R. Canetti, E. Kushilevitz, and Y. Lindell, "On the limitations of universally composable two-party computation without set-up assumptions," in *Proc. EUROCRYPT*, 2003, pp. 68–86.

[65] F. Armknecht, D. Moriyama, A.-R. Sadeghi, and M. Yung, "Towards a unified security model for physically unclonable functions," in *Proc. CT-RSA*, 2016, pp. 271–287.

[66] C. Brzuska, M. Fischlin, H. Schröder, and S. Katzenbeisser, "Physically uncloneable functions in the universal composition framework," in *Proc. CRYPTO*, 2011, pp. 51–70.

[67] R. Ostrovsky, A. Scafuro, I. Visconti, and A. Wadia, "Universally composable secure computation with (malicious) physically uncloneable functions," in *Proc. EUROCRYPT*, 2013, pp. 702–718.

[68] D. Dachman-Soled, N. Fleischhacker, J. Katz, A. Lysyanskaya, and D. Schröder, "Feasibility and infeasibility of secure computation with malicious PUFs," *J. Cryptol.*, vol. 33, no. 2, pp. 595–617, Apr. 2020.

[69] S. Katzenbeisser, V. Rožić, A.-R. Sadeghi, I. Verbauwhede, and C. Wachsmann, "PUFs: Myth, fact or busted? A security evaluation of physically unclonable functions (PUFs) cast in silicon," in *Proc. CHES*, 2012, pp. 283–301.

[70] B. Magri, G. Malavolta, D. Schröder, and D. Unruh, "Everlasting UC commitments from fully malicious PUFs," *J. Cryptol.*, vol. 35, no. 3, p. 20, Jul. 2022.

[71] L. E. Bassham, A. L. Rukhin, J. Soto, J. R. Nechvatal, M. E. Smid, S. D. Leigh, M. Levenson, M. Vangel, N. A. Heckert, and D. L. Banks, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," NIST, Gaithersburg, MD, USA, Tech. Rep., 800-22, 2010.
[72] R. G. Brown. (2023). *Dieharder: A Random Number Test Suite*. [Online]. Available: https://webhome.phy.duke.edu/ rgb/General/dieharder.php
[73] C. Calude, *Information and Randomness: An Algorithmic Perspective*, 2nd ed. Berlin, Germany: Springer-Verlag, 2002.
[74] G. J. Chaitin, "Algorithmic information theory," *IBM J. Res. Develop.*, vol. 21, no. 4, pp. 350–359, 1977.
[75] A. N. Kolmogorov, "Three approaches to the quantitative definition of information," *Int. J. Comput. Math.*, vol. 2, nos. 1–4, pp. 157–168, 1968.
[76] M. Li and P. Vitányi, *An Introduction to Kolmogorov Complexity and Its Applications* (Texts in Computer Science). Cham, Switzerland: Springer, 2008.
[77] J. Jordan, M. A. Petrovici, O. Breitwieser, J. Schemmel, K. Meier, M. Diesmann, and T. Tetzlaff, "Deterministic networks for probabilistic computing," *Sci. Rep.*, vol. 9, no. 1, p. 18303, Dec. 2019.
[78] B. Green and T. Tao, "The primes contain arbitrarily long arithmetic progressions," *Ann. Math.*, vol. 167, no. 2, pp. 481–547, Mar. 2008.
[79] R. Gallego, L. Masanes, G. De La Torre, C. Dhara, L. Aolita, and A. Acín, "Full randomness from arbitrarily deterministic events," *Nature Commun.*, vol. 4, no. 1, p. 2654, Oct. 2013.
[80] P. Grangier and A. Auffèves, "What is quantum in quantum randomness?" *Phil. Trans. Roy. Soc. A, Math., Phys. Eng. Sci.*, vol. 376, no. 2123, Jul. 2018, Art. no. 20170322.
[81] R. Colbeck and R. Renner, "Free randomness can be amplified," *Nature Phys.*, vol. 8, no. 6, pp. 450–453, Jun. 2012.
[82] R. Bijker and A. Frank, "Band structure from random interactions," *Phys. Rev. Lett.*, vol. 84, no. 3, pp. 420–422, Jan. 2000.
[83] R. Bijker and A. Frank, "Playing dice with nuclei: Pattern out of randomness?" *Nucl. Phys. News*, vol. 11, no. 4, pp. 15–20, Jan. 2001.
[84] C. W. Johnson, G. F. Bertsch, and D. J. Dean, "Orderly spectra from random interactions," *Phys. Rev. Lett.*, vol. 80, no. 13, pp. 2749–2753, Mar. 1998.
[85] P. Raghavan, "Probabilistic construction of deterministic algorithms: Approximating packing integer programs," *J. Comput. Syst. Sci.*, vol. 37, no. 2, pp. 130–143, Oct. 1988.
[86] D. E. Knuth, *The Art of Computer Programming: Seminumerical Algorithms*. 3rd ed. Reading, MA, USA: Addison-Wesley, 1997.
[87] G. Marsaglia and W. W. Tsang, "The Ziggurat method for generating random variables," *J. Stat. Softw.*, vol. 5, no. 8, pp. 1–7, 2000.
[88] W. Hörmann and J. Leydold, "Continuous random variate generation by fast numerical inversion," *ACM Trans. Model. Comput. Simul.*, vol. 13, no. 4, pp. 347–362, Oct. 2003.
[89] C. S. Wallace, "Fast pseudorandom generators for normal and exponential variates," *ACM Trans. Math. Softw.*, vol. 22, no. 1, pp. 119–127, Mar. 1996.
[90] G. E. P. Box and M. E. Müller, "A note on the generation of random normal deviates," *Ann. Math. Statist.*, vol. 29, no. 2, pp. 610–611, Jun. 1958.
[91] C. Peikert, "An efficient and parallel Gaussian sampler for lattices," in *Proc. CRYPTO*, 2010, pp. 80–97.
[92] A. Hülsing, T. Lange, and K. Smeets. (2017). *Rounded Gaussians—Fast and Secure Constant-Time Sampling for Lattice-Based Crypto*. [Online]. Available: https://eprint.iacr.org/2017/1025
[93] O. Goldreich, S. Goldwasser, and S. Micali, "How to construct random functions," *J. ACM*, vol. 33, no. 4, pp. 792–807, Aug. 1986.
[94] M. Naor, B. Pinkas, and O. Reingold, "Distributed pseudo-random functions and KDCs," in *Proc. EUROCRYPT*, 1999, pp. 327–346.
[95] D. Boneh, K. Lewi, H. W. Montgomery, and A. Raghunathan, "Key homomorphic PRFs and their applications," in *Proc. CRYPTO*, 2013, pp. 410–428. [Online]. Available: https://eprint.iacr.org/2015/220
[96] A. Banerjee and C. Peikert, "New and improved key-homomorphic pseudorandom functions," in *Proc. CRYPTO*, 2014, pp. 353–370.
[97] J. R. Parra, T. Chan, and S.-W. Ho, "A noiseless key-homomorphic PRF: Application on distributed storage systems," in *Proc. ACISP*, 2016, pp. 505–513.
[98] S. Kim, "Key-homomorphic pseudorandom functions from LWE with small modulus," in *Proc. EUROCRYPT*, 2020, pp. 576–607.
[99] N. Alamati, H. Montgomery, and S. Patranabis, "Ring key-homomorphic weak PRFs and applications," *Cryptol. ePrint Arch.*, vol. 2020, p. 606, Jan. 2020. [Online]. Available: https://ia.cr/2020/606
[100] W. Kautz and R. Singleton, "Nonrandom binary superimposed codes," *IEEE Trans. Inf. Theory*, vol. IT-10, no. 4, pp. 363–377, Oct. 1964.
[101] K. A. Bush, W. T. Federer, H. Pesotan, and D. Raghavarao, "New combinatorial designs and their applications to group testing," *J. Stat. Planning Inference*, vol. 10, no. 3, pp. 335–343, Oct. 1984.
[102] A. G. D'yachkov and V. V. Rykov, "Bounds on the length of disjunctive codes," *Probl. Peredachi Inf.*, vol. 18, no. 3, pp. 7–13, 1982.
[103] P. Erdös, P. Frankl, and Z. Füredi, "Families of finite sets in which no set is covered by the union of two others," *J. Combinat. Theory A*, vol. 33, no. 2, pp. 158–166, Sep. 1982.
[104] P. Erdös, P. Frankl, and Z. Füredi, "Families of finite sets in which no set is covered by the union of r others," *Isr. J. Math.*, vol. 51, pp. 79–89, Jan. 1985.
[105] R. Kumar, S. Rajagopalan, and A. Sahai, "Coding constructions for blacklisting problems without computational assumptions," in *Proc. CRYPTO*, 1999, pp. 609–623.
[106] R. Canetti, J. Garay, G. Itkis, D. Micciancio, M. Naor, and B. Pinkas, "Multicast security: A taxonomy and some efficient constructions," in *Proc. Conf. Comput. Commun., 18th Annu. Joint Conf. IEEE Comput. Commun. Societies*, Feb. 1999, pp. 708–716.
[107] J. A. Garay, J. Staddon, and A. Wool, "Long-lived broadcast encryption," in *Proc. CRYPTO*, 2000, pp. 333–352.
[108] D. R. Stinson, "On some methods for unconditionally secure key distribution and broadcast encryption," *Des., Codes Cryptogr.*, vol. 12, pp. 215–243, Jan. 1997.
[109] D. R. Stinson and T. van Trung, "Some new results on key distribution patterns and broadcast encryption," *Des., Codes Cryptogr.*, vol. 14, no. 3, pp. 261–279, Sep. 1998.
[110] Y. Desmedt, R. Safavi-Naini, H. Wang, C. Charnes, and J. Pieprzyk, "Broadcast anti-jamming systems," in *Proc. IEEE Int. Conf. Netw.*, Feb. 1999, pp. 349–355.
[111] R. Safavi-Naini and H. Wang, "Multireceiver authentication codes: Models, bounds, constructions, and extensions," *Inf. Comput.*, vol. 151, nos. 1–2, pp. 148–172, May 1999.
[112] C. J. Mitchell and F. C. Piper, "Key storage in secure networks," *Discrete Appl. Math.*, vol. 21, no. 3, pp. 215–228, Oct. 1988.
[113] M. Dyer, T. Fenner, A. Frieze, and A. Thomason, "On key storage in secure networks," *J. Cryptol.*, vol. 8, no. 4, pp. 189–200, Sep. 1995.
[114] D. R. Stinson, T. van Trung, and R. Wei, "Secure frameproof codes, key distribution patterns, group testing algorithms and related structures," *J. Stat. Planning Inference*, vol. 86, no. 2, pp. 595–617, May 2000.
[115] T. Bardini Idalino and L. Moura, "Embedding cover-free families and cryptographical applications," *Adv. Math. Commun.*, vol. 13, no. 4, pp. 629–643, 2019.
[116] G. Hartung, B. Kaidel, A. Koch, J. Koch, and A. Rupp, "Fault-tolerant aggregate signatures," in *Proc. PKC*, 2016, pp. 331–356.
[117] T. B. Idalino and L. Moura, "Nested cover-free families for unbounded fault-tolerant aggregate signatures," *Theor. Comput. Sci.*, vol. 854, pp. 116–130, Jan. 2021.
[118] T. B. Idalino and L. Moura, "Efficient unbounded fault-tolerant aggregate signatures using nested cover-free families," in *Proc. Int. Workshop Combinat. Algorithms*, 2018, pp. 52–64.
[119] J. N. Staddon, D. R. Stinson, and R. Wei, "Combinatorial properties of frameproof and traceability codes," *IEEE Trans. Inf. Theory*, vol. 47, no. 3, pp. 1042–1049, Mar. 2001.
[120] D. R. Stinson and R. Wei, "Combinatorial properties and constructions of traceability schemes and frameproof codes," *SIAM J. Discrete Math.*, vol. 11, no. 1, pp. 41–53, Feb. 1998.
[121] D. Tonien and R. Safavi-Naini, "An efficient single-key pirates tracing scheme using cover-free families," in *Proc. Int. Conf. Appl. Cryptogr. Netw. Secur.*, 2006, pp. 82–97.
[122] T. Bardini Idalino, L. Moura, R. F. Custódio, and D. Panario, "Locating modifications in signed data for partial data integrity," *Inf. Process. Lett.*, vol. 115, no. 10, pp. 731–737, Oct. 2015.
[123] R. Safavi-Naini and H. Wang, "New results on multi-receiver authentication codes," in *Proc. EUROCRYPT*, 1998, pp. 527–541.
[124] G. Zaverucha and D. Stinson, "Group testing and batch verification," in *Proc. Int. Conf. Inf. Theoretic Secur.*, 2009, pp. 140–157.
[125] J. Pieprzyk, H. Wang, and C. Xing, "Multiple-time signature schemes against adaptive chosen message attacks," in *Selected Areas in Cryptography*, 2003, pp. 88–100.
[126] D. Stinson and G. Zaverucha, "Short one-time signatures," *Adv. Math. Commun.*, vol. 5, no. 3, pp. 473–488, Aug. 2011.

[127] S. Goldwasser, Y. Kalai, C. Peikert, and V. Vaikuntanathan, "Robustness of the learning with errors assumption," in *Innovations in Computer Science*, 2010, pp. 230–240.

[128] A. Duc, F. Tramér, and S. Vaudenay, "Better algorithms for LWE and LWR," in *Proc. EUROCRYPT*, 2015, pp. 173–202.

[129] N. Miranda, F. Y. Yeo, and V. S. Sehrawat, "Function-private conditional disclosure of secrets and multi-evaluation threshold distributed point functions," in *Proc. CANS*, vol. 13099. Cham, Switzerland: Springer, 2021, pp. 334–354.

[130] C. Truesdell, *The Tragicomical History of Thermodynamics, 1822–1854* (Studies in the History of Mathematics and Physical Sciences). New York, NY, USA: Springer, 1980.

[131] C. E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. J.*, vol. 27, no. 3, pp. 379–423, Jul. 1948.

[132] L. Lagrange, "Recherches d'arithmétique," *Nouv. Mém. Acad.*, pp. 265–312, 1773.

[133] K. F. Gauss, *Disquisitiones Arithmeticae*. Leipzig, Germany: G. Fleischer, 1801.

[134] C. Hermite, "Extraits de lettres de M. Hermite à M. Jacobi sur différents objets de la théorie des nombres, deuxième lettre," *J. Reine Angew. Math.*, vol. 40, pp. 279–290, Jan. 1850.

[135] A. Korkine and G. Zolotarev, "Sur les formes quadratiques," *Math. Ann.*, vol. 6, pp. 336–389, Jan. 1873.

[136] H. Minkowski, *Geometrie der Zahlen*. Leipzig, Germany: Teubner, 1910.

[137] J. Stern, "Lattices and cryptography: An overview," in *Proc. PKC*, 1998, pp. 50–54.

[138] M. Ajtai and C. Dwork, "A public-key cryptosystem with worst-case/average-case equivalence," in *Proc. 29th Annu. ACM Symp. Theory Comput.*, 1997, pp. 284–293.

[139] M. Ajtai, "Generating hard instances of lattice problems (extended abstract)," in *Proc. 28th Annu. ACM Symp. Theory Comput.*, 1996, pp. 99–108.

[140] G. Grätzer, *General Lattice Theory*, 2nd ed. Basel, Switzerland: Birkhäuser, 2003.

[141] G. Grätzer, *Lattice Theory: First Concepts and Distributive Lattices* (Dover Books on Mathematics). New York, NY, USA: Dover, 2009.

[142] C. Gentry, C. Peikert, and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," in *Proc. 40th Annu. ACM Symp. Theory Comput.*, May 2008, pp. 197–206.

[143] S. Agrawal, D. Boneh, and X. Boyen, "Lattice basis delegation in fixed dimension and shorter-ciphertext hierarchical IBE," in *Proc. CRYPTO*, 2010, pp. 98–115.

[144] D. Cash, D. Hofheinz, E. Kiltz, and C. Peikert, "Bonsai trees, or how to delegate a lattice basis," in *Proc. EUROCRYPT*, 2010, pp. 523–552.

[145] X. Boyen, "Lattice mixing and vanishing trapdoors: A framework for fully secure short signatures and more," in *Proc. PKC*, 2010, pp. 499–517.

[146] D. Boneh, C. Gentry, S. Gorbunov, S. Halevi, V. Nikolaenko, G. Segev, V. Vaikuntanathan, and D. Vinayagamurthy, "Fully key-homomorphic encryption, arithmetic circuit ABE and compact garbled circuits," in *Proc. EUROCRYPT*, 2014, pp. 533–556.

[147] M. J. Song, I. Zadik, and J. Bruna, "On the cryptographic hardness of learning single periodic neurons," in *Proc. Adv. Neural Inf. Process. Syst.*, 2021, pp. 29602–29615.

[148] D. Aggarwal, D. Dadush, O. Regev, and N. Stephens-Davidowitz, "Solving the shortest vector problem in 2^n time using discrete Gaussian sampling: Extended abstract," in *Proc. 47th Annu. ACM Symp. Theory Comput.*, Jun. 2015, pp. 733–742.

[149] D. Aggarwal, D. Dadush, and N. Stephens-Davidowitz, "Solving the closest vector problem in 2^n time—The discrete Gaussian strikes again!" 2015, *arXiv:1504.01995*.

[150] N. Stephens-Davidowitz, "Discrete Gaussian sampling reduces to CVP and SVP," 2015, *arXiv:1506.07490*.

[151] S. J. Leon, Å. Björck, and W. Gander, "Gram-Schmidt orthogonalization: 100 years and more," *Numer. Linear Algebra Appl.*, vol. 20, no. 3, pp. 492–532, May 2013.

[152] D. Micciancio and O. Regev, "Worst-case to average-case reductions based on Gaussian measures," *SIAM J. Comput.*, vol. 37, no. 1, pp. 267–302, 2007.

[153] K. Chung, D. Dadush, F. Liu, and C. Peikert, "On the lattice smoothing parameter problem," in *Proc. IEEE Conf. Comput. Complex.*, Jun. 2013, pp. 230–241.

[154] C. Aguilar-Melchor, M. R. Albrecht, and T. Ricosset, "Sampling from arbitrary centered discrete Gaussians for lattice-based cryptography," in *Applied Cryptography and Network Security*, 2017, pp. 3–19.

[155] G. Barthe, S. Belaïd, T. Espitau, P.-A. Fouque, M. Rossi, and M. Tibouchi, "GALACTICS: Gaussian sampling for lattice-based constant-time implementation of cryptographic signatures, revisited," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Nov. 2019, pp. 2147–2164.

[156] Z. Brakerski, A. Langlois, C. Peikert, O. Regev, and D. Stehlé, "Classical hardness of learning with errors," in *Proc. 45th Annu. ACM Symp. Theory Comput.*, Jun. 2013, pp. 575–584.

[157] J. Buchmann, D. Cabarcas, F. Göpfert, A. Hülsing, and P. Weiden, "Discrete Ziggurat: A time-memory trade-off for sampling from a Gaussian distribution over the integers," in *Selected Areas in Cryptography—SAC 2013*, 2013, pp. 402–417.

[158] N. C. Dwarakanath and S. D. Galbraith, "Sampling from discrete Gaussians for lattice-based cryptography on a constrained device," *Applicable Algebra Eng., Commun. Comput.*, vol. 25, no. 3, pp. 159–180, Jun. 2014.

[159] N. Genise and D. Micciancio, "Faster Gaussian sampling for trapdoor lattices with arbitrary modulus," in *Proc. EUROCRYPT*, 2018, pp. 174–203.

[160] J. Howe, T. Prest, T. Ricosset, and M. Rossi, "Isochronous Gaussian sampling: From inception to implementation," in *Proc. PQCrypto*, 2020, pp. 53–71.

[161] C. F. F. Karney, "Sampling exactly from the normal distribution," *ACM Trans. Math. Softw.*, vol. 42, no. 1, pp. 1–14, Mar. 2016.

[162] A. Karmakar, S. S. Roy, O. Reparaz, F. Vercauteren, and I. Verbauwhede, "Constant-time discrete Gaussian sampling," *IEEE Trans. Comput.*, vol. 67, no. 11, pp. 1561–1571, Nov. 2018.

[163] D. Micciancio and M. Walter, "Gaussian sampling over the integers: Efficient, generic, constant-time," in *Proc. CRYPTO*, 2017, pp. 455–485.

[164] T. Pöppelmann, L. Ducas, and T. Güneysu, "Enhanced lattice-based signatures on reconfigurable hardware," in *Proc. CHES*, 2014, pp. 353–370.

[165] R. K. Zhao, R. Steinfeld, and A. Sakzad, "COSAC: Compact and scalable arbitrary-centered discrete Gaussian sampling over integers," in *Proc. PQCrypto*, 2020, pp. 284–303.

[166] R. K. Zhao, R. Steinfeld, and A. Sakzad, "FACCT: Fast, compact, and constant-time discrete Gaussian sampler over integers," *IEEE Trans. Comput.*, vol. 69, no. 1, pp. 126–137, Jan. 2020.

[167] L. Ducas and P. Q. Nguyen, "Faster Gaussian lattice sampling using lazy floating-point arithmetic," in *Proc. ASIACRYPT*, 2012, pp. 415–432.

[168] L. Ducas, A. Durmus, T. Lepoint, and V. Lyubashevsky, "Lattice signatures and bimodal Gaussians," in *Proc. CRYPTO*, 2013, pp. 40–56.

[169] J. Howe, C. Moore, M. O'Neill, F. Regazzoni, T. Güneysu, and K. Beeden, "Lattice-based encryption over standard lattices in hardware," in *Proc. 53rd ACM/EDAC/IEEE Design Autom. Conf. (DAC)*, Jun. 2016, pp. 1–6.

[170] E. Alkim, P. Jakubeit, and P. Schwabe, "NEWHOPE on ARM Cortex-M," in *Proc. SPACE*, 2016, pp. 332–349.

[171] J. Howe, A. Khalid, C. Rafferty, F. Regazzoni, and M. O'Neill, "On practical discrete Gaussian samplers for lattice-based cryptography," *IEEE Trans. Comput.*, vol. 67, no. 3, pp. 322–334, Mar. 2018.

[172] Y. Du and X. Ma, "On the rejection rate of exact sampling algorithm for discrete Gaussian distributions over the integers," *Theory Comput. Syst.*, vol. 66, no. 6, pp. 1099–1122, Dec. 2022.

[173] C. Gentry, "A fully homomorphic encryption scheme," Ph.D. dissertation, Stanford Univ., Stanford, CA, USA, 2009.

[174] M. R. Albrecht and A. Deo, "Large modulus ring-LWE $\geq$ module-LWE," in *Proc. ASIACRYPT*, 2017, pp. 267–296.

[175] Y. Dodis, S. Goldwasser, Y. T. Kalai, C. Peikert, and V. Vaikuntanathan, "Public-key encryption schemes with auxiliary inputs," in *Proc. TCC*, 2010, pp. 361–381.

[176] G. Asharov, A. Jain, A. López-Alt, E. Tromer, V. Vaikuntanathan, and D. Wichs, "Multiparty computation with low communication, computation and interaction via threshold FHE," in *Proc. EUROCRYPT*, 2012, pp. 483–501.

[177] J. Alperin-Sheriff and C. Peikert, "Circular and KDM security for identity-based encryption," in *Proc. PKC*, 2012, pp. 334–352.

[178] S. Garg, C. Gentry, and S. Halevi, "Candidate multilinear maps from ideal lattices," in *Proc. EUROCRYPT*, 2013, pp. 1–17.

[179] C. Gentry, "Fully homomorphic encryption using ideal lattices," in *Proc. 41st Annu. ACM Symp. Theory Comput.*, May 2009, pp. 169–178.

[180] A. Langlois, D. Stehlé, and R. Steinfeld, "GGHLite: More efficient multilinear maps from ideal lattices," in *Proc. EUROCRYPT*, 2014, pp. 239–256.

[181] M. R. Albrecht, A. Davidson, A. Deo, and N. P. Smart, "Round-optimal verifiable oblivious pseudorandom functions from ideal lattices," in *Proc. PKC*, 2021, pp. 261–289.
[182] C. Peikert, "Public-key cryptosystems from the worst-case shortest vector problem," in *Proc. 41st Annu. ACM Symp. Theory Comput.*, May 2009, pp. 333–342.
[183] V. Lyubashevsky, C. Peikert, and O. Regev, "On ideal lattices and learning with errors over rings," in *Proc. EUROCRYPT*, 2010, pp. 1–12.
[184] A. Langlois and D. Stehlé, "Worst-case to average-case reductions for module lattices," *Des., Codes Cryptogr.*, vol. 75, no. 3, pp. 565–599, Jun. 2015.
[185] C. Grover, C. Ling, and R. Vehkalahti, "Non-commutative ring learning with errors from cyclic algebras," 2020, *arXiv:2008.01834*.
[186] J. Bruna, O. Regev, M. J. Song, and Y. Tang, "Continuous LWE," in *Proc. 53rd Annu. ACM SIGACT Symp. Theory Comput.*, 2020, pp. 694–707.
[187] V. S. Sehrawat, F. Y. Yeo, and Y. Desmedt, "Extremal set theory and LWE based access structure hiding verifiable secret sharing with malicious-majority and free verification," *Theor. Comput. Sci.*, vol. 886, pp. 106–138, Sep. 2021.
[188] M. Roşca, A. Sakzad, D. Stehlé, and R. Steinfeld, "Middle-product learning with errors," in *Proc. CRYPTO*, 2017, pp. 283–297.
[189] N. Gama, M. Izabachène, P. Q. Nguyen, and X. Xie, "Structural lattice reduction: Generalized worst-case to average-case reductions and homomorphic cryptosystems," in *Proc. EUROCRYPT*, 2016, pp. 528–558.
[190] Z. Brakerski, V. Vaikuntanathan, H. Wee, and D. Wichs, "Obfuscating conjunctions under entropic ring LWE," in *Proc. ACM Conf. Innov. Theor. Comput. Sci.*, Jan. 2016, pp. 147–156.
[191] S. Yang and X. Huang, "Universal product learning with errors: A new variant of LWE for lattice-based cryptography," *Theor. Comput. Sci.*, vol. 915, pp. 90–100, May 2022.
[192] D. Stehlé, R. Steinfeld, K. Tanaka, and K. Xagawa, "Efficient public key encryption based on ideal lattices (extended abstract)," in *Proc. ASIACRYPT*, 2009, pp. 617–635.
[193] J. Zhang and Z. Zhang, *Lattice-Based Cryptosystems—A Design Perspective* (Data Structures and Information Theory). Singapore: Springer, 2020.
[194] J. Katz and V. Lyubashevsky, *Lattice-Based Cryptography* (Cryptography and Network Security). Boca Raton, FL, USA: CRC Press, 2021.
[195] C. Peikert, O. Regev, and N. Stephens-Davidowitz, "Pseudorandomness of ring-LWE for any ring and modulus," in *Proc. 49th Annu. ACM SIGACT Symp. Theory Comput.*, Jun. 2017, pp. 461–473.
[196] B. Applebaum, D. Cash, C. Peikert, and A. Sahai, "Fast cryptographic primitives and circular-secure encryption based on hard learning problems," in *Proc. CRYPTO*, 2009, pp. 1–16.
[197] D. Micciancio and C. Peikert, "Hardness of SIS and LWE with small parameters," in *Proc. CRYPTO*, 2013, pp. 21–39.
[198] S. Goldwasser and S. Micali, "Probabilistic encryption & how to play mental poker keeping secret all partial information," in *Proc. 14th Annu. ACM Symp. Theory Comput.*, 1982, pp. 365–377.
[199] A. Bogdanov and A. Rosen, "Pseudorandom functions: Three decades later," in *Tutorials on the Foundations of Cryptography* (Information Security and Cryptography). Cham, Switzerland: Springer, 2017, pp. 79–158.
[200] T. Hastie, R. Tibshirani, and J. Friedman, *The Elements of Statistical Learning* (Springer Series in Statistics). New York, NY, USA: Springer-Verlag, 2009.
[201] D. C. Montgomery, E. A. Peck, and G. G. Vining, *Introduction to Linear Regression Analysis*, 5th ed. Hoboken, NJ, USA: Wiley, 2012.
[202] S. B. Akers and B. Krishnamurthy, "A group-theoretic model for symmetric interconnection networks," *IEEE Trans. Comput.*, vol. 38, no. 4, pp. 555–566, Apr. 1989.
[203] S. B. Akers, D. Harel, and B. Krishnamurthy, "The star graph: An attractive alternative to the n-cube," in *Interconnection Networks for High-Performance Parallel Computers*. Washington, DC, USA, 1994, pp. 145–152.
[204] J. Duato, S. Yalamanchili, and L. Ni, *Interconnection Networks* (The Morgan Kaufmann Series in Computer Architecture and Design). Amsterdam, The Netherlands: Elsevier, 2002.
[205] I.-J. Bienaymé, "Considérations àl'appui de la découverte de laplace," *Comp. Rendus de l'Académie des Sci.*, vol. 37, pp. 309–324, Jan. 1853.
[206] P. L. Chebyshev, "Des valeurs moyennes," *J. Mathématiques Pures Appliquées*, vol. 12, no. 2, pp. 177–184, 1867.
[207] G. Boole, *The Mathematical Analysis of Logic—Being an Essay Towards a Calculus of Deductive Reasoning*. Cambridge, U.K.: Cambridge Univ. Press, 2009.
[208] M. Naor and O. Reingold, "Synthesizers and their application to the parallel construction of pseudo-random functions," *J. Comput. Syst. Sci.*, vol. 58, no. 2, pp. 336–375, Apr. 1999.
[209] J. Alwen, S. Krenn, K. Pietrzak, and D. Wichs, "Learning with rounding, revisited," in *Proc. CRYPTO*, 2013, pp. 57–74.
[210] A. Bogdanov, S. Guo, D. Masny, S. Richelson, and A. Rosen, "On the hardness of learning with rounding over small modulus," in *Proc. TCC*, 2016, pp. 209–224.
[211] S. Bai, T. Lepoint, A. Roux-Langlois, A. Sakzad, D. Stehlé, and R. Steinfeld, "Improved security proofs in lattice-based cryptography: Using the Rényi divergence rather than the statistical distance," *J. Cryptol.*, vol. 31, no. 2, pp. 610–640, Apr. 2018.
[212] V. S. Sehrawat and Y. Desmedt, "Bi-homomorphic lattice-based PRFs and unidirectional updatable encryption," in *Proc. CANS*, in Lecture Notes in Computer Science, vol. 11829. Cham, Switzerland: Springer, 2019, pp. 3–23.
[213] V. S. Sehrawat, "Privacy enhancing cryptographic constructs for cloud and distributed security," Ph.D. dissertation, Univ. Texas, Dallas, TX, USA, 2019.
[214] B. Libert, S. Ling, K. Nguyen, and H. Wang, "Zero-knowledge arguments for lattice-based PRFs and applications to e-cash," in *Proc. ASIACRYPT*, 2017, pp. 304–335.
[215] J.-P. D'Anvers, A. Karmakar, S. S. Roy, and F. Vercauteren, "Saber: Module-LWR based key exchange, CPA-secure encryption and CCA-secure KEM," in *Proc. AFRICACRYPT*, 2018, pp. 282–305.
[216] H. Baan, S. Bhattacharya, S. Fluhrer, O. Garcia-Morchon, T. Laarhoven, R. Rietman, M.-J. O. Saarinen, L. Tolhuizen, and Z. Zhang, "Round5: Compact and fast post-quantum public-key encryption," in *Proc. PQCrypto*, 2019, pp. 83–102.
[217] X. Xie, R. Xue, and R. Zhang, "Training data is provided to the machine, based on which machine learning algorithms like regression are used to generate appropriate model," in *Proc. SCN*, 2012, pp. 1–18.
[218] H. Montgomery, "A nonstandard variant of learning with rounding with polynomial modulus and unbounded samples," in *Proc. PQCrypto*, 2018, pp. 312–330.
[219] S. Jukna, *Extremal Combinatorics* (Texts in Theoretical Computer Science). Cham, Switzerland: Springer, 2011.
[220] B. Bollobás, *Extremal Graph Theory*. London, U.K.: Academic, 1978.
[221] N. Alon, "Problems and results in extremal combinatorics—I," *Discrete Math.*, vol. 273, nos. 1–3, pp. 31–53, 2003.
[222] N. Alon, "Problems and results in extremal combinatorics—II," *Discrete Math.*, vol. 308, no. 19, pp. 4460–4472, Oct. 2008.
[223] N. Alon, "Problems and results in extremal combinatorics—III," *J. Combinatorics*, vol. 7, nos. 2–3, pp. 233–256, 2016.
[224] N. Alon, "Problems and results in extremal combinatorics—IV," 2020, *arXiv:2009.12692*.
[225] E. Sperner, "Ein satz über untermengen einer endlichen menge," *Mathematische Zeitschrift*, vol. 27, no. 1, pp. 544–548, 1928.
[226] P. Erdós, C. Ko, and R. Rado, "Intersection theorems for systems of finite sets," *Quart. J. Math.*, vol. 12, no. 1, pp. 313–320, 1961.
[227] A. Beimel, Y. Ishai, R. Kumaresan, and E. Kushilevitz, "On the cryptographic complexity of the worst functions," in *Proc. TCC*, 2014, pp. 317–342. [Online]. Available: https://www.microsoft.com/en-us/research/wp-content/uploads/2017/03/BIKK.pdf
[228] A. Beimel, Y. Ishai, E. Kushilevitz, and I. Orlov, "Share conversion and private information retrieval," in *Proc. IEEE 27th Conf. Comput. Complex.*, Jun. 2012, pp. 258–268.
[229] Z. Dvir and S. Gopi, "2-server PIR with sub-polynomial communication," in *Proc. 47th Annu. ACM Symp. Theory Comput.*, Jun. 2015, pp. 577–584.
[230] Z. Dvir, P. Gopalan, and S. Yekhanin, "Matching vector codes," *SIAM J. Comput.*, vol. 40, no. 4, pp. 1154–1178, Jan. 2011.
[231] K. Efremenko, "3-query locally decodable codes of subexponential length," in *Proc. 41th Annu. ACM Symp. Theory Comput.*, May 2009, pp. 39–44.
[232] S. Yekhanin, "Towards 3-query locally decodable codes of subexponential length," *J. ACM*, vol. 55, no. 1, pp. 1–16, Feb. 2008.
[233] T. Liu, V. Vaikuntanathan, and H. Wee, "Conditional disclosure of secrets via non-linear reconstruction," in *Proc. CRYPTO*, 2017, pp. 758–790.

[234] V. S. Sehrawat and Y. Desmedt, "Access structure hiding secret sharing from novel set systems and vector families," in *Proc. COCOON*, in Lecture Notes in Computer Science, vol. 12273. Cham, Switzerland: Springer, 2020, pp. 246–261.

[235] M. Polak, U. Romańczuk, V. Ustimenko, and A. Wróblewska, "On the applications of extremal graph theory to coding theory and cryptography," *Electron. Notes Discrete Math.*, vol. 43, pp. 329–342, Sep. 2013.

[236] S. R. Blackburn, "Frameproof codes," *SIAM J. Discrete Math.*, vol. 16, no. 3, pp. 499–510, Jan. 2003.

[237] Z. Wang, "Connections between extremal combinatorics, probabilistic methods, Ricci curvature of graphs, and linear algebra," Ph.D. dissertation, Univ. South Carolina, Columbia, SC, USA, 2020.

[238] B. Sudakov, "Recent developments in extremal combinatorics: Ramsey and Turán type problems," in *Proc. Int. Congr. Mathematicians*, Jun. 2011, pp. 1–12.

[239] L. Gargano, J. Körner, and U. Vaccaro, "Capacities: From information theory to extremal set theory," *J. Combinat. Theory A*, vol. 68, no. 2, pp. 296–316, Nov. 1994.

[240] V. Grolmusz, "Superpolynomial size set-systems with restricted intersections mod 6 and explicit Ramsey graphs," *Combinatorica*, vol. 20, no. 1, pp. 71–86, Jan. 2000.

[241] M. M. Hong, Y. Ishai, V. I. Kolobov, and R. W. F. Lai, "On computational shortcuts for information-theoretic PIR," in *Proc. TCC*, 2020, pp. 504–534.

[242] D. Gerbner and B. Patkos, *Extremal Finite Set Theory*. Boca Raton, FL, USA: CRC Press, 2018.

[243] B. Bollobás, *Combinatorics*. Cambridge, U.K.: Cambridge Univ. Press, 1986.

[244] J. Spencer, *Ten Lectures Probabilistic Method*. Philadelphia, PA, USA: SIAM, 1987.

[245] D. Ellis, "Intersection problems in extremal combinatorics: Theorems, techniques and questions old and new," 2021, *arXiv:2107.06371*.

[246] P. Frankl and N. Tokushige, "Invitation to intersection problems for finite sets," *J. Combinat. Theory A*, vol. 144, pp. 157–211, Nov. 2016.

[247] A. M. Raigorodskii and D. D. Cherkashin, "Extremal problems in hypergraph colourings," *Russian Math. Surv.*, vol. 75, no. 1, pp. 89–146, Feb. 2020.

[248] D. Kleitman, "Extremal hypergraph problems," in *Surveys Combinatorics* (London Mathematical Society Lecture Note Series), B. Bollobás, Ed. Cambridge, U.K.: Cambridge Univ. Press, 1979, pp. 44–65.

[249] P. Borg, "Intersecting families of sets and permutations: A survey," 2011, *arXiv:1106.6144*.

[250] R. Ahlswede and L. H. Khachatrian, "The complete intersection theorem for systems of finite sets," *Eur. J. Combinatorics*, vol. 18, no. 2, pp. 125–136, Feb. 1997.

[251] R. K. Guy, "How to factor a number," in *Proc. Manitoba Conf. Numer. Math.*, 1975, pp. 49–89.

[252] D. H. Lehmer and E. Lehmer, "A new factorization technique using quadratic forms," *Math. Comput.*, vol. 28, no. 126, pp. 625–635, 1974.

[253] D. Shanks, *Solved and Unsolved Problems in Number Theory*. Providence, RI, USA: Amer. Math. Soc., 1985, p. 202.

[254] H. Freudenthal, "Oktaven, ausnahmegruppen und oktavengeometrie," *Geometriae Dedicata*, vol. 19, pp. 7–63, Jan. 1985.

[255] M. R. de Traubenberg and M. J. Slupinski, "Commutation relations of $\mathfrak{g}_2$ and the incidence geometry of the Fano plane," 2022, *arXiv:2207.13946*.

[256] M. Rausch de Traubenberg and M. J. Slupinski, "Incidence geometry of the Fano plane and Freudenthal's ansatz for the construction of (split) octonions," 2022, *arXiv:2203.03261*.

[257] J. C. Baez, "The octonions," *Bull. Amer. Math. Soc.*, vol. 39, no. 2, pp. 145–205, 2002.

[258] Y. Wang and Q. M. Malluhi, "Privacy preserving computation in cloud using noise-free fully homomorphic encryption (FHE) schemes," in *Proc. ESORICS*, 2016, pp. 301–323.

[259] E. Malekian and A. Zakerolhosseini, "OTRU: A non-associative and high speed public key cryptosystem," in *Proc. 15th CSI Int. Symp. Comput. Archit. Digit. Syst.*, Sep. 2010, pp. 83–90.

[260] Z. Lipiǹski, "Symmetric and asymmetric cryptographic key exchange protocols in the octonion algebra," *Applicable Algebra Eng., Commun. Comput.*, vol. 32, no. 1, pp. 81–96, Jan. 2021.

[261] N. Koblitz, "Number theory," in *A Survey of Number Theory and Cryptography*, R. P. Bambah, V. C. Dumir, and R. J. Hans-Gill, Eds. Gurgaon, India: Hindustan Book Agency, 2000, pp. 217–239.

[262] S. Y. Yan, *Primality Testing and Integer Factorization in Public-Key Cryptography*, 2nd ed. Cham, Switzerland: Springer, 2008.

[263] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Commun. ACM*, vol. 21, no. 2, pp. 120–126, Feb. 1978.

[264] J. Plücker, *System der Analytischen Geometrie, auf Neue Betrachtungsweisen gegründet, und Insbesondere Eine Ausführliche Theorie der Curven Dritter Ordnung Enthalend*. Berlin, Germany: Duncker & Humblot, 1835.

[265] T. P. Kirkman, "On a problem in combinations," *Cambridge Dublin Math. J.*, vol. 2, pp. 191–204, Jan. 1847.

[266] J. Steiner, "Combinatorische Aufgaben," *J. Reine Angewandte Mathematik*, vol. 10, no. 45, pp. 181–182, 1853.

[267] M. Reiss, "Über eine steinersche combinatorische aufgabe," *J. Reine Angew. Math.*, vol. 56, pp. 326–344, Jan. 1859.

[268] M. Noether, "Über die gleichungen achten grades und ihr auftreten in der theorie der curven vierter ordnung," *Math. Ann.*, vol. 15, pp. 87–110, Jan. 1879.

[269] E. Netto, "Zur theorie der triplesysteme," *Math. Ann.*, vol. 42, pp. 143–152, Jan. 1893.

[270] E. H. Moore, "Concerning triple systems," *Math. Ann.*, vol. 43, pp. 271–285, Jan. 1893.

[271] J. J. Sylvester, "Note on a nine schoolgirls problem," *Messenger Math.*, vol. 22, pp. 159–160, Jan. 1893.

[272] J. Power, "On the problem of the fifteen schoolgirls," *Quart. J. Pure Appl. Math.*, vol. 8, pp. 236–251, Jan. 1867.

[273] A. Clebsch and F. Lindemann, *Vorlesungen Über Geometrie*. Sterling Ford, LA, USA: Wentworth Press, 2016.

[274] E. Witt, "Über steinersche systeme," *Abhandlungen Mathematischen Seminar Universitat Hamburg*, vol. 12, pp. 265–275, Jan. 1938.

[275] D. R. Stinson and S. A. Vanstone, "A combinatorial approach to threshold schemes," in *Proc. CRYPTO*, 1987, pp. 330–339.

[276] C. Blundo and D. R. Stinson, "Anonymous secret sharing schemes," *Des., Codes Cryptogr.*, vol. 2, pp. 357–390, Mar. 1996.

[277] A. Fazeli, A. Vardy, and E. Yaakobi, "Codes for distributed PIR with low storage overhead," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Jun. 2015, pp. 2852–2856.

[278] R. Wilson, "The early history of block designs," *Rendiconti Seminario Matematico Messina*, vol. 9, no. 25, pp. 267–276, 2003.

[279] C. J. Colbourn and A. Rosa, *Triple Systems* (Oxford Mathematical Monographs). Oxford, U.K.: Oxford Univ. Press, 1999.

[280] C. J. Colbourn and J. H. Dinitz, *Handbook of Combinatorial Designs* (Discrete Mathematics and Its Applications). Boca Raton, FL, USA: CRC Press, 2006.

[281] P. Keevash, "The existence of designs," 2019, *arXiv:1401.3665*.

[282] E. Alkim, L. Ducas, T. Pöppelmann, and P. Schwabe, "Post-quantum key exchange—A new hope," in *Proc. USENIX Secur. Symp.*, 2016, pp. 327–343.

[283] J. W. Bos, C. Costello, M. Naehrig, and D. Stebila, "Post-quantum key exchange for the TLS protocol from the ring learning with errors problem," in *Proc. IEEE Symp. Secur. Privacy*, Jan. 2015, pp. 553–570.

[284] A. Khalid, J. Howe, C. Rafferty, F. Regazzoni, and M. O'Neill, "Compact, scalable, and efficient discrete Gaussian samplers for lattice-based cryptography," in *Proc. IEEE Int. Symp. Circuits Syst.*, Jun. 2018, pp. 1–5.

[285] K. Schäcke. (2004). *On the Kronecker Product*. [Online]. Available: https://www.math.uwaterloo.ca/~hwolkowi/henry/reports/kronthesisschaecke04.pdf

[286] M. Ali, *Reconfigurable Antenna Design and Analysis*. Norwood, MA, USA: Artech House, 2021.

[287] Y. J. Guo and P.-Y. Qin, *Handbook of Antenna Technologies*, Z. N. Chen, D. Liu, H. Nakano, X. Qing, and T. Zwick, Eds. Cham, Switzerland: Springer, 2016, pp. 2987–3032.

[288] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels," *IEEE Trans. Antennas Propag.*, vol. 53, no. 11, pp. 3776–3784, Nov. 2005.

[289] R. Mehmood, J. W. Wallace, and M. A. Jensen, "Key establishment employing reconfigurable antennas: Impact of antenna complexity," *IEEE Trans. Wireless Commun.*, vol. 13, no. 11, pp. 6300–6310, Nov. 2014.

[290] Y. Pan, Z. Xu, M. Li, and L. Lazos, "Man-in-the-middle attack resistant secret key generation via channel randomization," in *Proc. MobiHoc*, 2021, pp. 231–240.
[291] J. Zhang, G. Li, A. Marshall, A. Hu, and L. Hanzo, "A new frontier for IoT security emerging from three decades of key generation relying on wireless channels," *IEEE Access*, vol. 8, pp. 138406–138446, 2020.
[292] Y. Pan, M. Li, Y. Hou, R. M. Gerdes, and B. A. Cetiner, *Proactive and Dynamic Network Defense*, C. Wang and Z. Lu, Eds. Cham, Switzerland: Springer, 2019, pp. 115–137.
[293] M. P. Daly, "Physical layer encryption using fixed and reconfigurable antennas," Ph.D. dissertation, Univ. Illinois, Champaign, IL, USA, 2012.
[294] G. Danezis and C. Diaz. (2008). *A Survey of Anonymous Communication Channels*. [Online]. Available: http://ftp.research.microsoft.com/pub/tr/TR-2008-35.pdf
[295] M. Edman and B. Yener, "On anonymity in an electronic society: A survey of anonymous communication systems," *ACM Comput. Surv.*, vol. 42, no. 1, pp. 1–35, Dec. 2009.
[296] S. J. Phillips and N. C. Phillips, "Strongly ideal secret sharing schemes," *J. Cryptol.*, vol. 5, no. 3, pp. 185–191, Oct. 1992.
[297] W. Kishimoto, K. Okada, K. Kurosawa, and W. Ogata, "On the bound for anonymous secret sharing schemes," *Discrete Appl. Math.*, vol. 121, pp. 193–202, Jan. 2002.
[298] Y. P. Deng, L. F. Guo, and M. L. Liu, "Constructions for anonymous secret sharing schemes using combinatorial designs," *Acta Mathematicae Applicatae Sinica*, vol. 23, pp. 67–78, Jan. 2007.
[299] V. S. Sehrawat, Y. Shah, V. K. Choyi, A. Brusilovsky, and S. Ferdi, "Certificate and signature free anonymity for V2V communications," in *Proc. IEEE Veh. Netw. Conf. (VNC)*, Nov. 2017, pp. 139–146.
[300] A. Beimel and M. K. Franklin, "Weakly-private secret sharing schemes," in *Proc. TCC*, 2007, pp. 253–272.
[301] V. Daza and J. Domingo-Ferrer, "On partial anonymity in secret sharing," in *Proc. EuroPKI*, 2007, pp. 193–202.
[302] C. Gehrmann, "Topics in authentication theory," Ph.D. dissertation, Lund Univ., Lund, Sweden, 1997.
[303] R. Olimid and A. Paskin-Cherniavsky, "On cryptographic anonimity and unpredicatbility in secret sharing," *Cryptol. ePrint Arch.*, vol. 2015, pp. 1–10, Jan. 2015. [Online]. Available: https://ia.cr/2015/1234
[304] M. Guillermoand, K. M. Martin, and C. M. O'Keefe, "Providing anonymity in unconditionally secure secret sharing schemes," *Des., Codes Cryptogr.*, vol. 28, pp. 227–245, Jan. 2003.
[305] Y. Ishai, E. Kushilevitz, R. Ostrovsky, and A. Sahai, "Cryptography from anonymity," in *Proc. 47th Annu. IEEE Symp. Found. Comput. Sci. (FOCS)*, Oct. 2006, pp. 239–248.
[306] D. Huang, "Pseudonym-based cryptography for anonymous communications in mobile ad hoc networks," *Int. J. Secur. Netw.*, vol. 2, nos. 3–4, pp. 272–283, Apr. 2007.
[307] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
[308] Y. Wu, A. Khisti, C. Xiao, G. Caire, K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 679–695, Apr. 2018.
[309] W. Shi, X. Jiang, J. Hu, Y. Teng, Y. Wang, H. He, R. Dong, F. Shu, and J. Wang, "Physical layer security techniques for future wireless networks," 2021, *arXiv:2112.14469*.
[310] S. Leung-Yan-Cheong and M. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. IT-24, no. 4, pp. 451–456, Jul. 1978.
[311] M. S. Kumar, R. Ramanathan, and M. Jayakumar, "Key less physical layer security for wireless networks: A survey," *Eng. Sci. Technol., Int. J.*, vol. 35, Nov. 2022, Art. no. 101260.
[312] L. H. Ozarow and A. D. Wyner, "Wire-tap channel II," *AT&T Bell Laboratories Tech. J.*, vol. 63, no. 10, pp. 2135–2157, Dec. 1984.
[313] M. Nafea and A. Yener, "A new wiretap channel model and its strong secrecy capacity," *IEEE Trans. Inf. Theory*, vol. 64, no. 3, pp. 2077–2092, Mar. 2018.
[314] M. Nafea and A. Yener, "Generalizing multiple access wiretap and wiretap II channel models: Achievable rates and cost of strong secrecy," *IEEE Trans. Inf. Theory*, vol. 65, no. 8, pp. 5125–5143, Aug. 2019.
[315] Z. Goldfeld, P. Cuff, and H. H. Permuter, "Semantic-security capacity for wiretap channels of type II," *IEEE Trans. Inf. Theory*, vol. 62, no. 7, pp. 3863–3879, Jul. 2016.
[316] L. Kong, Y. Ai, L. Lei, G. Kaddoum, S. Chatzinotas, and B. Ottersten, "An overview of generic tools for information-theoretic secrecy performance analysis over wiretap fading channels," *EURASIP J. Wireless Commun. Netw.*, vol. 2021, no. 1, pp. 1–10, Dec. 2021.
[317] J. Barros and M. R. D. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Inf. Theory*, Jul. 2006, pp. 356–360.
[318] S. Eberz, M. Strohmeier, M. Wilhelm, and I. Martinov, "A practical man-in-the-middle attack on signal-based key generation protocols," in *Proc. Eur. Symp. Res. Comput. Secur.*, 2012, pp. 235–252.
[319] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel," in *Proc. 14th ACM Int. Conf. Mobile Comput. Netw.*, Sep. 2008, pp. 128–139.
[320] L. Wang and A. M. Wyglinski, "Detection of man-in-the-middle attacks using physical layer wireless security techniques," *Wireless Commun. Mobile Comput.*, vol. 16, no. 4, pp. 408–426, Mar. 2016.
[321] Y. Pan, "Enhance wireless network performance and security with reconfigurable antennas," Ph.D. dissertation, The University of Arizona, Tucson, AZ, USA, 2021.
[322] M. Mitev, A. Chorti, E. V. Belmega, and H. V. Poor, "Protecting physical layer secret key generation from active attacks," *Entropy*, vol. 23, no. 8, p. 960, Jul. 2021.
[323] H. Pirayesh and H. Zeng, "Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 24, no. 2, pp. 767–809, 2nd Quart., 2022.
[324] J. Alman and V. V. Williams, "A refined laser method and faster matrix multiplication," in *Proc. SIAM Symp. Discrete Algorithms*, 2021, pp. 522–539.
[325] J. Blasiak, H. Cohn, J. A. Grochow, K. Pratt, and C. Umans, "Matrix multiplication via matrix groups," in *Proc. Innov. Theor. Comput. Sci. Conf. (ITCS)*, in Leibniz International Proceedings in Informatics, vol. 251, 2023, pp. 19:1–19:16.
[326] D. Harvey and J. van der Hoeven, "Integer multiplication in time $O(n\log n)$," *Ann. Math.*, vol. 193, no. 2, pp. 563–617, 2021.
[327] M. Ajtai, R. Kumar, and D. Sivakumar, "A sieve algorithm for the shortest lattice vector problem," in *Proc. 33rd Annu. ACM Symp. Theory Comput.*, Jul. 2001, pp. 601–610.
[328] U. Fincke and M. Pohst, "Improved methods for calculating vectors of short length in a lattice, including a complexity analysis," *Math. Comput.*, vol. 44, no. 170, pp. 463–471, 1985.
[329] N. Gama, N. Howgrave-Graham, H. Koy, and P. Q. Nguyen, "Rankin's constant and blockwise lattice reduction," in *Proc. CRYPTO*, 2006, pp. 112–130.
[330] N. Gama and P. Q. Nguyen, "Finding short lattice vectors within Mordell's inequality," in *Proc. 40th Annu. ACM Symp. Theory Comput.*, May 2008, pp. 207–216.
[331] N. Gama, P. Q. Nguyen, and O. Regev, "Lattice enumeration using extreme pruning," in *Proc. EUROCRYPT*, 2010, pp. 257–278.
[332] A. K. Lenstra, H. W. Lenstra, and L. Lovász, "Factoring polynomials with rational coefficients," *Mathematische Annalen*, vol. 261, no. 4, pp. 515–534, Dec. 1982.
[333] P. Q. Nguyen and B. Vallée, *The LLL Algorithm: Survey and Applications* (Information Security and Cryptography). Cham, Switzerland: Springer, 2010.
[334] P. Q. Nguyen and T. Vidick, "Sieve algorithms for the shortest vector problem are practical," *J. Math. Cryptol.*, vol. 2, no. 2, pp. 181–207, Jan. 2008.
[335] D. Micciancio and P. Voulgaris, "Faster exponential time algorithms for the shortest vector problem," in *Proc. 21st Annu. ACM-SIAM Symp. Discrete Algorithms*, Jan. 2010, pp. 1468–1480.
[336] D. Micciancio and P. Voulgaris, "A deterministic single exponential time algorithm for most lattice problems based on Voronoi cell computations," in *Proc. 42nd ACM Symp. Theory Comput.*, Jun. 2010, pp. 351–358.
[337] M. Pohst, "On the computation of lattice vectors of minimal length, successive minima and reduced bases with applications," *ACM SIGSAM Bull.*, vol. 15, no. 1, pp. 37–44, Feb. 1981.
[338] C. P. Schnorr, "A hierarchy of polynomial time lattice basis reduction algorithms," *Theor. Comput. Sci.*, vol. 53, nos. 2–3, pp. 201–224, 1987.
[339] C. P. Schnorr and M. Euchner, "Lattice basis reduction: Improved practical algorithms and solving subset sum problems," *Math. Program.*, vol. 66, nos. 1–3, pp. 181–199, Aug. 1994.
[340] C. P. Schnorr and H. H. Hörner, "Attacking the Chor–Rivest cryptosystem by improved lattice reduction," in *Proc. EUROCRYPT*, 1995, pp. 1–12.

[341] P. Q. Nguyen and D. Stehlé, "An LLL algorithm with quadratic complexity," *SIAM J. Comput.*, vol. 39, no. 3, pp. 874–903, Jan. 2009.
[342] E. W. Postlethwaite and F. Virdia, "On the success probability of solving unique SVP via BKZ," in *Proc. PKC*, 2021, pp. 68–98.
[343] R. Lindner and C. Peikert, "Better key sizes (and attacks) for LWE-based encryption," in *Topics in Cryptology—CT-RSA 2011*, 2011, pp. 319–339.
[344] M. R. Albrecht, C. Cid, J.-C. Faugère, R. Fitzpatrick, and L. Perret, "On the complexity of the BKW algorithm on LWE," *Des., Codes Cryptogr.*, vol. 74, no. 2, pp. 325–354, Feb. 2015.
[345] A. Blum, A. Kalai, and H. Wasserman, "Noise-tolerant learning, the parity problem, and the statistical query model," *J. ACM*, vol. 50, no. 4, pp. 506–519, Jul. 2003.
[346] Q. Guo and T. Johansson, "Faster dual lattice attacks for solving LWE—With applications to CRYSTALS," in *Proc. ASIACRYPT*, 2021, pp. 33–62.
[347] S. Nakamura and M. Yasuda, "Dynamic self-dual DeepBKZ lattice reduction with free dimensions and its implementation," *Discrete Appl. Math.*, vol. 304, pp. 220–229, Dec. 2021.
[348] T. Mukherjee and N. Stephens-Davidowitz, "Lattice reduction for modules, or how to reduce ModuleSVP to ModuleSVP," in *Proc. CRYPTO*, 2020, pp. 213–242.
[349] A. Budroni, Q. Guo, T. Johansson, E. Mårtensson, and P. S. Wagner, "Improvements on making BKW practical for solving LWE," *Cryptography*, vol. 5, no. 4, p. 31, Oct. 2021.
[350] Q. Guo, E. Mårtensson, and P. S. Wagner, "Modeling and simulating the sample complexity of solving LWE using BKW-style algorithms," *Cryptogr. Commun.*, vol. 15, no. 2, pp. 331–350, Mar. 2023.

VIPIN SINGH SEHRAWAT received the Ph.D. degree in computer science from The University of Texas at Dallas. His research interests include cryptography, combinatorics, and industrial mathematics and their applications to information security. During his employments with InterDigital Communications, The University of Texas at Dallas, Seagate Technology, and Circle Internet Financial. He worked on numerous research projects in cryptography and information security—many of which led to patents and publications.

FOO YEE YEO, photograph and biography not available at the time of publication.

DMITRIY VASSILYEV received the Master of Science degree in operation research from the University of Colorado. He is currently a Staff Data Scientist and a member of Seagate Technology Operations & Technology Advanced Analytics Group (OTAAG) Team. He is also a Data Scientist with over eight years of successful experience in data analytics and six years of experience in data management. He has been working on various data science and optimization projects in the areas of manufacturing, marketing, machinery, data center operations, aerospace, and telecommunications for industry leading companies, such as Seagate, AC Nielsen, and CenturyLink. He has a decade of experience in teaching and tutoring mathematics from middle school to college levels.