Received 11 November 2022; revised 22 December 2022; accepted 1 January 2023. Date of publication 5 January 2023; date of current version 20 January 2023.

Digital Object Identifier 10.1109/OJCOMS.2023.3234338

High-Rate Secret Key Generation Using Physical Layer Security and Physical Unclonable Functions

TASNEEM ASSAF[1] (Member, IEEE), ARAFAT AL-DWEIK[1,2,3] (Senior Member, IEEE), YOUSSEF IRAQI[4] (Senior Member, IEEE), SOBIA JANGSHER[1] (Member, IEEE), ANSHUL PANDEY[5] (Member, IEEE), JEAN-PIERRE GIACALONE[5] (Member, IEEE), ENAS E. ABULIBDEH[1] (Member, IEEE), HANI SALEH[1] (Senior Member, IEEE), AND BAKER MOHAMMAD[1] (Senior Member, IEEE)

[1] Department of Electrical Engineering and Computer Science, Khalifa University, Abu Dhabi, UAE

[2] Center for Cyber-Physical Systems, Khalifa University, Abu Dhabi, UAE

[3] Department of Electrical and Computer Engineering, Western University, London, ON N6A 3K7, Canada

[4] School of Computer Science, Mohammed VI Polytechnic University, Ben Guerir 43150, Morocco

[5] Secure Systems Research Center, Technology Innovation Institute, Abu Dhabi, UAE

CORRESPONDING AUTHOR: A. AL-DWEIK (e-mail: dweik@fulbrightmail.org)

This work was supported by the Technology Innovation Institute (TII) Project ‘PHY Layer Security for Heterogeneous UAV-Ground Wireless Networks,’ under Grant EX2020-036.

ABSTRACT Physical layer security (PLS) can be adopted for efficient key generation and sharing in secured wireless systems. The inherent random nature of the wireless channel and the associated channel reciprocity (CR) are the main pillars for realizing PLS techniques. However, for applications that involve air-to-air (A2A) transmission, such as unmanned aerial vehicle (UAV) applications, the channel does not generally have sufficient randomness to enable reliable key generation. Therefore, this work proposes a novel system design to mitigate the channel randomness constraint and enable a high-rate secret key generation process. The proposed system integrates physically unclonable functions (PUFs) and CR to generate and exchange secret keys between two nodes securely. Moreover, an adaptive and controllable artificial fading (AF) level with interleaving is used to mitigate the impact of low randomness variations in the wireless channel. Moreover, we propose a novel bit extraction scheme to reduce the number of overhead bits required to share the intermediate keys. The obtained Monte Carlo simulation results show that the proposed system can operate efficiently even when the channel is nearly flat or time-invariant. Consequently, the time required for generating and sharing a key is significantly shorter than conventional techniques. Furthermore, the results show that a key agreement can be reached at the first trial for moderate and high signal-to-noise ratios (SNRs) substantially faster than other PLS techniques. Adopting the AF into static channels managed to reduce the mismatch ratio between the generated secret sequences and degrade the eavesdropper’s capability to predict the secret keys.

INDEX TERMS Physical layer security (PLS), channel reciprocity (CR), physically unclonable function (PUF), secret key generation (SKG), static environments, artificial fading (AF), bit extraction (BE), received signal strength (RSS).

I. INTRODUCTION

Unmanned aerial vehicles (UAVs) are currently invading several sectors with applications in agriculture, logistics, transportation, energy, construction, media, entertainment, etc. Because of their operational flexibility, low cost, and small size, UAVs manifest themselves as the perfect tool for reconnaissance, surveillance, mapping, and surveying. The overall UAV market in 2021 is estimated to be $27.4 billion and is projected to reach $58.4 billion by 2026 [1]. The popularity of UAVs is highly correlated with the development of Internet of Things (IoT) technology, and UAVs are currently considered an integral element of IoT infrastructure where they are used for data collection, relaying, data distribution, etc. [2].

Multiple UAVs can be jointly assigned a remote mission requiring secure data communications in specific applications. For such applications, physical layer security (PLS) can be considered attractive due to the limited computational power and tight energy budget of the UAVs. In particular, PLS can facilitate the key generation and distribution processes and reduce the overhead signaling required for other key distribution techniques [3]. PLS techniques can be generally divided into two main categories: signal to interference plus noise ratio (SINR)-based and complexity-based PLS. The main focus of this work is the complexity-based PLS, which is associated with extracting and sharing a secret sequence by utilizing the shared channel between legitimate users. PLS mechanisms leverage wireless channels' random and reciprocal characteristics to achieve information-theoretical security [4]. Most existing complexity-based PLS schemes are designed for systems that adopt time division duplexing (TDD) to enable utilizing the channel reciprocity (CR) [3], [5], [6]. PLS generally requires rich and dynamic wireless channels. The richness of the channel is required to enable reliable key generation, while the channel dynamics are required to maximize the difference between consecutive keys. Consequently, the channel information in time [7], [8], frequency [5], [9] and space domains [10], [11] can be utilized to enable reliable key generation.

To enhance the security and randomness levels of complexity-based PLS systems, physically unclonable functions (PUFs) can be added as a second layer of security. The concept of PUFs was first introduced in [12]. The idea is that the integrated circuits (ICs) have a uniqueness in their physical structure inherited from inevitable variations during the fabrication process. These unique characteristics are unpredictable before the end of the manufacturing process and can be considered as device fingerprints. Due to their physical unclonability and high resistance to reverse engineering, PUFs have shown great promise as hardware identification primitives for cryptography applications such as authentication and secret key generation (SKG) [13]. The unclonability of PUFs means that it is infeasible to reproduce the same physical structure for a given fabrication procedure [14]. Moreover, compared to traditional cryptography techniques, PUFs require significantly less computational capacity as there is no need for permanent storage to secure the generated secret keys [15], [16]. PUFs are commonly characterized by a set of challenge-response pairs (CRPs) based on the unique circuit variations. The PUF response for a certain challenge that is measured under certain conditions, such as temperature and voltage, is called the "original response." The obtained responses from a PUF are sensitive to the environmental changes and physical conditions where the device is being tested. In other words, the readings from the PUFs are not perfectly reproducible. Therefore, error correction mechanisms such as fuzzy extractors are used to correct the mismatches with the original response [16].

The integration of a PUF in any system requires that one of the users to have a PUF circuit and the other to have the PUF emulator. The emulator can be realized as a CRPs table, which is generated and shared before the communication process [15]. Such tables correspond to a subset of the complete list of the PUF CRPs. However, using tables has several limitations, particularly scalability. To alleviate the need for tables, extensive research is currently being devoted to associating the PUF to a particular secret model that emulates the PUF CRPs behavior. For example, the secret model in the case of an arbiter PUF would be the delays of the individual stages [15]. It is also worth noting that the PUF CRPs depend on certain parameters such as temperature and voltage. Therefore, the PUF and its emulator might have some differences. However, for a well-designed PUF, the difference is small and can be generally eliminated using forward error correction schemes, which are also called secure sketch or error reconciliation schemes, in this context.

A. RELATED WORK

Complexity-based PLS techniques are used for key generation by exploiting the inherent randomness of the channel and the principle of CR between the transmitter and receiver [3], [17], [18]. Unlike classical key distribution techniques, PLS does not involve the direct exchange of keys. Therefore, it is difficult for eavesdroppers to tap the key. The PLS-based SKG is explored in the literature for various networks and channel settings [17], [19], [20], [21]. In [19], [20], [21] and the references listed therein, SKG is studied for static and dynamic environments. The dynamic environments have high temporal variations that enable generating keys with high entropy, which leads to a high key generation rate (KGR).

SKG is a challenging task in poor scattering environments where the channel randomness or variations are limited due to the channel's large coherence time or wide coherence bandwidth. Consequently, the key generation process, which requires strong time or frequency variations, will mostly fail to cause low KGR. In [20], the authors conducted an experiment inside an underground concrete tunnel to exclude most external interference sources and the effects of channel variation due to any surroundings' mobility. The obtained KGR was extremely low, about one 256 bit key every 7 minutes. In addition to the failure of the key generation process, the dominance of the independent hardware noise, i.e., additive white Gaussian noise (AWGN), at the legitimate nodes over the time or frequency selectivity of the channel, increases the key mismatch probability considerably. In the literature, several approaches were proposed to overcome such challenges, which include using relays [22], multiple-input multiple-output (MIMO) [23], intelligent reflective surface (IRS) [24], or by inducing artificial randomness [25]. In [26], [27], opportunistic randomized beamforming with a diversity mechanism is proposed. Generating artificial interference for the eavesdropper is presented in [28], [29]. An induced randomness for SKG is studied in [6] for static channels. However, the work considers that the eavesdropper's channel is independent of the legitimate users' channel, which is not generally a valid assumption in several cases of interest. Moreover, the induced randomness is not common among the system users, and its level is not guaranteed or adaptive. This can lead to high estimation errors or extra complexity, which can be avoided in the case of high channel randomness. In [26], the authors propose using IRS with discrete phase shifts for SKG. The channel coefficients are used to generate the secret keys.

Furthermore, in the existing PLS work with poor scattering or static environments, it is assumed that the legitimate users' channel is independent of the eavesdropper channel, given that the legitimate users are at least half a wavelength apart. However, this assumption is valid only in sufficiently rich scattering environments. In free space communications, which has poor scattering environments, such as air-to-air (A2A) and air-to-ground (A2G) channels, there might be a strong correlation between the channels of the legitimate and illegitimate users, even when there are large distances between the users [30]. Therefore, propagation environment reconstruction attacks can estimate the legitimate channel parameters with high accuracy [31].

The research on PUF in wireless communications applications is employed for node identification, authentication [32], and SKG [32], [33], [34], [35], [36]. In [33], quaternary PUF responses are used for key generation along with polar codes to ensure the secrecy leakage is low. The authors in [34] propose a method to produce reliable keys on field programmable gate arrays (FPGAs). The design uses a lookup table based on SLICEL components, which enables fine-tuning of the hamming weight of the PUF and increases the generated key uniqueness. A switched capacitor PUF is proposed in [35], which promises to provide a stable key for chip security with the use of metal blocks as a protective coating. An authentication and key establishment protocol based on PUF are proposed in [32].

Ideally, PUFs are unclonable. However, practical implementations have been prone to attacks such as physical cloning [37], side channel and reliability information-based attacks [38], machine learning (ML)-based modeling attacks [39], etc. The modeling attacks pose a greater threat than other attacks because, in most cases, they do not require auxiliary information and can be based only on transmitted CRPs or leaked information during the exchange of data in the different stages of the SKG protocol. ML algorithms, such as logistic regression (LR), artificial neural network (ANN), support vector machine (SVM), etc, were applied successfully in various scenarios. Several solutions have been proposed in the literature to address the ML attack of PUFs. For example, in [40], Sbox transformation is introduced as an additional nonlinear operation to enhance the PUF resilience to modeling attacks. Other techniques are also proposed in [41], [42]. These mechanisms increase the implementation complexity and, consequently, the required energy and area cost, which is infeasible for resource-constrained UAV networks.

B. MOTIVATION AND CONTRIBUTIONS

As can be noted from the cited literature, the references listed therein, and to the best of the authors' knowledge, line-of-sight (LoS) and poor scattering environments are considered the main obstacles for adopting PLS in practical systems, particularly UAV networks. In UAV communications, the channels between the legitimate users and eavesdroppers' can be correlated or have a low entropy, which is highly probable in air-to-air channels. Therefore, the assumption that the channel is time or frequency-selective is generally weak. Therefore, the key generation rate becomes slow, which may jeopardize the system's security. Therefore, this paper proposes a novel framework for high-rate SKG based on PLS by incorporating artificial fading (AF) and PUFs. The synergy of PLS and PUFs will increase resilience to ML modeling attacks because no CRPs are required to be transmitted over the air. Furthermore, in the proposed SKG, the number of side-channel transmissions is reduced, which decreases the chance for eavesdroppers' to collect more information to model the PUF. The main contributions of this work are:

1) Propose a novel SKG protocol based on the integration of PUF and CR. The proposed SKG protocol resolves the issue of static channels in the context of PLS with the aid of PUFs, which can enhance the reliability of the SKG process and increase the KGR. In the proposed SKG, CR between the legitimate users is used to generate a challenge at the communicating nodes, which is applied to the PUF or PUF emulator to generate the ultimate key.
2) Propose a novel mechanism to enhance the randomness level of PLS systems in static or low scattering environments. The proposed scheme, called AF, introduces common signal variations between legitimate nodes. The AF is an interleaved version of the channel frequency response (CFR) of the previously successful SKG session where a key agreement is achieved. The interleaving process of the CFR will significantly reduce the eavesdropper's capability to accurately estimate the legitimate users' channel, even if it could locate itself close to a legitimate user.
3) Propose an efficient bit extraction (BE) scheme by modifying the adaptive secret bit extraction (ASBE) [20]. The new BE technique can reduce the number of transmissions between the nodes and reduce the required number of side-information bits.
4) The considered PUF is realized using a configurable ring oscillator (RO), which is implemented using FPGA, and its properties are validated.

The numerical results for the proposed and conventional SKG are compared in terms of randomness, key mismatch

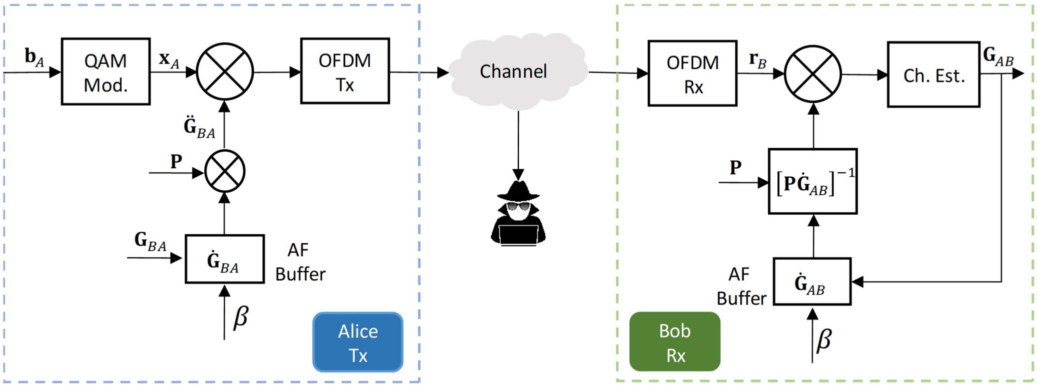


FIGURE 1. A simplified diagram for the proposed SKG system focusing on the AF process.

ratio (MMR), and the average number of sessions needed to reach a key agreement. The obtained results clearly show the superiority of the proposed scheme.

C. PAPER ORGANIZATION

The rest of the paper is organized as follows. Section II describes the signal and channel models. The intermediate key generation and sharing protocol is detailed in Section III. The proposed AF, BE, and PUF-based key generation are explained in Section IV. The numerical evaluation is presented and discussed in Section V. Section VI concludes the paper.

II. SIGNAL AND CHANNEL MODELS

This work considers two legitimate users, Alice and Bob, who aim to establish a secure and common key through an authenticated multipath wireless channel. An eavesdropper, Eve can listen to all communications between Alice and Bob passively and intends to predict the generated key. The system model is shown in Fig. 1. Orthogonal frequency-division multiplexing (OFDM) with N subcarriers is adopted for the transmission where Alice, Bob, and Eve can transmit and receive OFDM signals. Every user is assumed to be equipped with a single antenna.

The key generation process should be initiated by one of the legitimate users, i.e., Alice or Bob, and then the negotiation to generate the secret key starts. Assuming that Alice starts the key generation process, she should send an OFDM symbol to Bob. The transmitted OFDM symbol is generated by applying the data symbols' vector $\mathbf{x}_A = [x_A^0, x_A^1, \ldots, x_A^{N-1}]^T$ generated by applying $\bar{M}$-quadrature amplitude modulation (QAM) modulation to a bits sequence $\mathbf{b}_A$, to an N-point inverse discrete Fourier transform (IDFT). Then, a cyclic prefix (CP) no less than the maximum delay spread is added as a preamble to prevent inter-symbol interference (ISI). In all OFDM transmission standards, certain subcarriers are modulated using pilot symbols for channel estimation and synchronization purposes. Therefore, the vector $\mathbf{x}_A$ may consist of data and pilot symbols. The symbols x_A^n $\forall\{n\}$ are selected from an arbitrary constellation diagram and are considered to have unit average power, i.e., $\mathbb{E}[|x_A^n|^2] = 1$, where $\mathbb{E}[\,\cdot\,]$ denotes the statistical expectation. For simplicity, we consider the quadrature phase shift keying (QPSK) modulation scheme. In this work, we consider that the pilot symbols are generally distributed following the long-term evolution (LTE) resource block structure [43, Fig. 1]. The set of pilots is denoted by the vector $\mathbf{u}_A = [x_A^0, x_A^6, \ldots]$. At Bob's receiver, the CP is removed, and discrete Fourier transform (DFT) is used to separate and extract the symbols from the subcarriers. Assuming the channel is quasi-static, i.e., the channel remains fixed during one OFDM symbol period, and the CP is larger than the maximum delay spread of the channel [44], the DFT output at Bob's receiver can be represented as

$$\mathbf{r}_B = \mathbf{G}_{AB}\mathbf{x}_A + \mathbf{w}_B \tag{1}$$

where $\{\mathbf{r}_B, \mathbf{w}_B\} \in \mathbb{C}^{N\times 1}$, $\mathbf{w}_B = [w_B^0, w_B^1, \ldots, w_B^{N-1}]$ is the AWGN vector whose elements are independent and identically distributed (i.i.d.) and $w_B^n \sim \mathcal{CN}(0, 2\sigma_w^2)$. The channel matrix $\mathbf{G}_{AB} \in \mathbb{C}^{N\times N}$ is the CFR matrix, which is given by

$$\mathbf{G}_{AB} = \operatorname{diag}\left\{\left[G_{AB}^0, G_{AB}^1, \ldots, G_{AB}^{N-1}\right]\right\} \tag{2}$$

where

$$G_{AB}^n = \sum_{i=0}^{Q} g_{AB}^i \exp\left(-\frac{j2\pi in}{N}\right), \quad \forall n \tag{3}$$

and where $g_{AB}^i \sim \mathcal{CN}\left(m_{g_{AB}^i}, 2\sigma^2_{g_{AB}^i}\right)$ denotes the ith multipath component gain and $Q+1$ represents the number of multipath components. The fading gains g_{AB}^i, $i \in \{0, 1, \ldots, Q\}$, are considered independent. Therefore, the envelope of the channel matrix elements is Rician, and the channel frequency selectivity depends on the gain and delays of the channel multipath components g_{AB}^i. More specifically $|G_{AB}^i| \sim \mathcal{R}(K_{AB}^i, \Omega_{AB}^i)$, where $K_{AB}^i = \frac{|m_{g_{AB}^i}|^2}{2\sigma^2_{g_{AB}^i}}$, $K_{AB}^i \in (0, \infty)$ and $\Omega_{AB}^i = |m_{g_{AB}^i}|^2 + 2\sigma^2_{g_{AB}^i}$. A special case of interest is when the fading factor $K = 0$, which corresponds to the Rayleigh fading scenario. It is worth noting that the diagonal elements in $\mathbf{G}_{AB} \triangleq \mathbf{d}_{AB}$ are correlated with a correlation factor that depends on g_{AB}^{i} $\forall i$ [45]. Because Alice's signal is transmitted over a broadcast channel, Eve will also receive a copy, which can be written as

$$\mathbf{r}_E = \mathbf{G}_{AE}\mathbf{x}_A + \mathbf{w}_E \tag{4}$$

where $\mathbf{G}_{AE}$ is the CFR from Alice to Eve.

Under the same assumptions and conditions, and in a similar fashion, Bob sends to Alice the vector $\mathbf{x}_B$, and the DFT output at Alice can be written as

$$\mathbf{r}_A = \mathbf{G}_{BA}\mathbf{x}_B + \mathbf{w}_A \tag{5}$$

where $\mathbf{G}_{BA}$ is the CFR matrix from Bob to Alice. The IDFT output at Eve can be expressed as

$$\acute{\mathbf{r}}_E = \mathbf{G}_{BE}\mathbf{x}_B + \acute{\mathbf{w}}_E \tag{6}$$

where $\mathbf{G}_{BE}$ is the CFR matrix from Bob to Eve.

The DFT outputs $\mathbf{r}_A$ and $\mathbf{r}_B$ can be used to obtain the channel state information (CSI) for both channels, i.e., $\mathbf{G}_{AB}$ and $\mathbf{G}_{BA}$. The process typically starts by estimating the CFR at the pilot subcarriers using techniques such as the least-square (LS) or minimum mean-square error (MMSE). Then interpolation can be used to compute the channel gains at the data subcarriers [46]. The communications between Alice and Bob are assumed to be conducted using TDD where the coherence time of the channel is larger than the TDD frame. In such scenarios, the channel reciprocity principle can be incorporated to consider that $\mathbf{G}_{AB} = \mathbf{G}_{BA} \triangleq \mathbf{G}$ [4], [20], [47], [48], [49]. Moreover, given that Eve is located at a relatively far distance from Bob, then $\mathbf{G}_{AB} \neq \mathbf{G}_{AE}$. Consequently, Alice and Bob are the only nodes who know $\mathbf{G}$. Therefore, Alice and Bob can use $\mathbf{G}$ to generate a secret key on both sides and use it for secure communications [5], [6], [50].

III. INTERMEDIATE KEY GENERATION AND SHARING

Conventional PLS-based SKG is described extensively in the literature. Hence, it is stated briefly in this section for the sake of completeness and to simplify the presentation of the proposed framework. The keys generated in this work can be classified as intermediate and final keys. The intermediate keys can be generated using various PLS key-sharing techniques described in the following subsections. The intermediate keys go through the second processing stage to generate the final keys using PUFs. The intermediate key generation and sharing processes using PLS can be briefly described as follows:

1) CHANNEL PROBING

The channel probing aims at estimating $\mathbf{G}_{AB}$ and $\mathbf{G}_{BA}$, or more specifically $\mathbf{d}_{AB}$ and $\mathbf{d}_{BA}$. The process starts when Alice transmits $\mathbf{x}_A$ to Bob, who computes $\mathbf{r}_B$ and uses it to estimate $\mathbf{d}_{AB}$ as described in Section II. This work uses the LS method to estimate the channel coefficients at the pilot symbols. Then linear interpolation is used to obtain the coefficients at the data subcarriers. Similarly, Bob transmits $\mathbf{x}_B$ within the same TDD frame and Alice computes $\mathbf{r}_A$ and estimates $\mathbf{d}_{BA}$.

2) INTERMEDIATE KEY GENERATION

Once the vectors $\mathbf{d}_{AB}$ and $\mathbf{d}_{BA}$ are estimated, they can be used to generate the intermediate keys, which are denoted by $\mathbf{q}_A$ and $\mathbf{q}_B$, respectively. In PLS, both the phase and amplitude of the channel coefficients can be used to extract the key bits from $\mathbf{d}$. Nevertheless, the phase is more sensitive to hardware imperfections, so the amplitude is considered more attractive. Therefore, the amplitude, or equivalently the received signal strength (RSS) for QPSK or binary phase shift keying (BPSK) modulation schemes, $\boldsymbol{\zeta} = |\mathbf{r}|$, is typically used to generate the bits of $\mathbf{q}_A$ and $\mathbf{q}_B$. Therefore, In the literature, the BE algorithm proposed in [20], named ASBE, has received significant attention due to its ability to generate high entropy bits at a high bit rate. Nevertheless, the algorithm performance may deteriorate significantly in static or flat-fading channels where it might take about 7 minutes to generate a 256 bits key [20]. Moreover, Alice and Bob must exchange the indices of the subcarriers that were dropped during the BE process, which can be considered a significant overhead. Furthermore, it causes some information leakage about the key. To address the disadvantages of ASBE, we propose a BE mechanism in Section IV, which has less transmission overhead, a low number of side-channel transmissions, and is computationally more efficient.

3) ERROR RECONCILIATION AND VERIFICATION

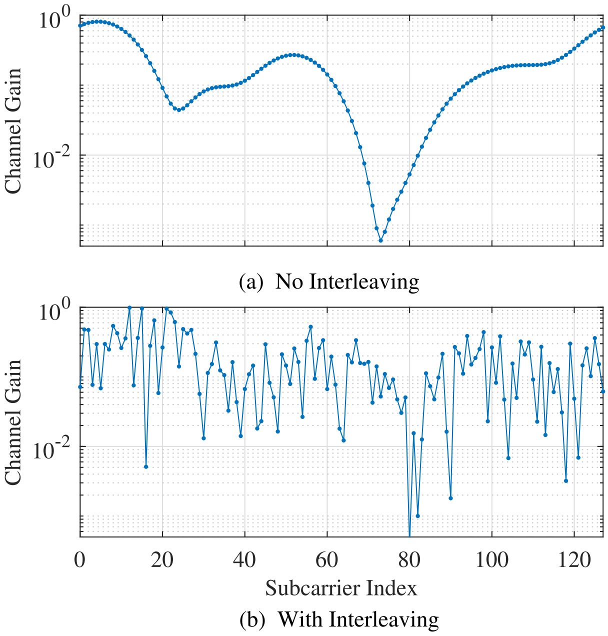
For reliable communications, the keys $\mathbf{q}_A$ and $\mathbf{q}_B$ should be identical. However, the BE process is prone to errors due to AWGN, imperfect CSI estimation, and hardware mismatch. Therefore, additional processing is necessary to guarantee that $\mathbf{q}_A = \mathbf{q}_B$, and both users should verify that they have identical keys. The verification process can be realized using cyclic redundancy check (CRC) where Alice generates the CRC bits and Bob verifies and acknowledges the CRC process outcome [51]. Therefore, Alice computes the CRC bits of $\mathbf{q}_A$, denoted as $\mathbf{c}_A^q$, and sends them to Bob. The error reconciliation eliminates discrepancies between $\mathbf{q}_A$ and $\mathbf{q}_B$. In this work, we adopt the code-offset secure sketch proposed in [6], and Bose–Chaudhuri–Hocquenghem (BCH) codes are used as the underlying coding scheme.

The process starts when Alice randomly selects a codeword $\mathbf{v}_A^q$ from the codebook of the corresponding BCH code, and then computes

$$\mathbf{s}^q = \left[\mathbf{s}_1^q, \mathbf{s}_2^q\right] = \left[\mathbf{q}_A \oplus \mathbf{v}_A^q, \mathbf{c}_A^q\right] \tag{7}$$

where $\mathbf{v}_A^q$ is a codeword with the same length as $\mathbf{q}_A$ and $\oplus$ is the exclusive or (XOR) operation. The vector $\mathbf{s}^q$ is then modulated and transmitted to Bob.

Because $\mathbf{q}_A$ and $\mathbf{q}_B$ are not necessarily equal, we can write $\mathbf{q}_A = \mathbf{q}_B \oplus \boldsymbol{\varepsilon}$, where $\boldsymbol{\varepsilon}$ is the error pattern that represents the differences between $\mathbf{q}_A$ and $\mathbf{q}_B$. Therefore, $\varepsilon_i = 1$ if



(a) No Interleaving

(b) With Interleaving

FIGURE 2. Example for the channel coefficients vector $\bar{\mathbf{d}}$ with and without interleaving of $\dot{\mathbf{d}}$.

$q_A^i = q_B^i$, otherwise $\varepsilon_i = 0$. Thus

$$\mathbf{s}^q = \left[\mathbf{s}_1^q, \mathbf{s}_2^q\right] = \left[\mathbf{q}_B \oplus \boldsymbol{\varepsilon} \oplus \mathbf{v}_A^q,\ \mathbf{c}_A^q\right]. \tag{8}$$

At Bob's side, Bob demodulates the received sequence, extracts the data bits, and computes,

$$\begin{aligned}\tilde{\mathbf{v}}_A^q &= \tilde{\mathbf{s}}_1^q \oplus \mathbf{q}_B \\ &= \mathbf{q}_B \oplus \boldsymbol{\varepsilon} \oplus \mathbf{v}_A^q \oplus \bar{\boldsymbol{\varepsilon}} \oplus \mathbf{q}_B \\ &= \mathbf{v}_A^q \oplus \boldsymbol{\varphi}\end{aligned} \tag{9}$$

where $\tilde{\mathbf{s}}_1^q$ is the demodulated version of $\mathbf{s}_1^q$ and $\bar{\boldsymbol{\varepsilon}}$ is the error vector due to the transmission and reception operations, and $\boldsymbol{\varphi} = \boldsymbol{\varepsilon} \oplus \bar{\boldsymbol{\varepsilon}}$. Then $\tilde{\mathbf{v}}_A^q$ applied to the BCH decoder to produce the estimated version of the random codeword $\mathbf{v}_A^q$, denoted as $\hat{\mathbf{v}}_A^q$. Finally, the estimated error pattern can be computed as $\hat{\boldsymbol{\varphi}} = \tilde{\mathbf{v}}_A^q \oplus \hat{\mathbf{v}}_A^q$. Consequently, the key at Bob can be updated such that $\mathbf{q}_B = \mathbf{q}_B \oplus \hat{\boldsymbol{\varphi}}$. Given that the hamming weight of $\tilde{\boldsymbol{\varphi}}$ is less than the error correction capability of the code, then we obtain $\mathbf{q}_A = \mathbf{q}_B$. Once $\mathbf{q}_B$ is computed, $\mathbf{c}_B^q$ is computed and compared to $\tilde{\mathbf{c}}_A^q$, and if they are equal, Bob sends an acknowledgment to Alice then $\mathbf{q}_A$ and $\mathbf{q}_B$ are considered as the intermediate keys. Otherwise, a negative acknowledgment is sent. In this case, steps 1 to 3 are repeated until a key agreement is achieved.

IV. PROPOSED ARTIFICIAL FADING, BIT EXTRACTION, AND PUF-BASED FINAL KEY GENERATION

A. PROPOSED ARTIFICIAL FADING

Because most PLS techniques require high channel randomness to provide a reliable key generation process, flat and slow fading channels are challenging operating channels. To resolve this issue, we propose using AF, where a frequency-selective fading channel is emulated and used at the transmitter side. The AF is mathematically similar to the widely-known pre-equalization process [52] but different in that the current and pre-equalization channels can be independent.

To implement the AF process, consider that a pre-designed fading channel whose channel matrix, denoted as $\dot{\mathbf{G}}$, can be represented as a diagonal matrix where the diagonal elements can be expressed by the vector $\dot{\mathbf{d}} = [\dot{d}_0, \dot{d}_1, \ldots, \dot{d}_{N-1}]$. Therefore, the DFT output at any user's receiver can be written as $\mathbf{r} = \mathbf{G}\dot{\mathbf{G}}\mathbf{x}+\mathbf{w}$. Because $\mathbf{G}$ and $\dot{\mathbf{G}}$ are diagonal matrices, then $\mathbf{G}\dot{\mathbf{G}} \triangleq \mathcal{G}$, which is also a diagonal matrix whose diagonal elements vector can be written as $\bar{\mathbf{d}} = \mathbf{d}\dot{\mathbf{d}}$. Given that the adjacent elements in $\mathbf{d}$ are correlated, and similarly in $\dot{\mathbf{d}}$, then the elements of $\bar{\mathbf{d}}$ will also be correlated. Consequently, all users can estimate the CSI using conventional approaches as described in Section II. In the worst case that the channel is purely flat, i.e., $d_i = 1\ \forall i$, then $\bar{\mathbf{d}} = \dot{\mathbf{d}}$, which corresponds to a frequency-selective channel, which still can be used to generate a random bit sequence. For legitimate users, the estimation process starts by equalizing the effect of $\dot{\mathbf{d}}$, which is already known, then $\mathbf{d}$ can be obtained. It is worth noting that we can estimate $\mathcal{G}$ directly. However, the estimation accuracy will be generally worse because the channel will be highly selective in this case.

Although it is difficult for Eve to estimate $\mathcal{G}$ because of the spatial decorrelation, she might attempt to increase the correlation by getting close to any of the legitimate users. To mitigate this scenario, the selection of $\dot{\mathbf{G}}$ can be performed to decorrelate the overall fading matrix $\mathcal{G}$ making it even more difficult for Eve to estimate $\mathcal{G}$ or $\mathbf{G}$. Such an approach can be efficient because most channel estimation algorithms for OFDM generally require the channel coefficients over adjacent subcarriers to be highly correlated [43].

In this work, we adopt random interleaving to decorrelate the elements of the AF vector $\dot{\mathbf{d}}$. Fig. 1 shows the AF process where each user is assumed to have a storage element called "AF buffer" to store $\dot{\mathbf{G}}$. Also, at each successful iteration where both users agree on an intermediate key $\mathbf{q}_A = \mathbf{q}_B$, the AF buffer is enabled to update $\dot{\mathbf{G}}$. The enabler of the buffer is controlled by β where $\beta = 1$ if $\mathbf{q}_A = \mathbf{q}_B$, otherwise $\beta = 0$. The interleaved $\dot{\mathbf{d}}$ is denoted as $\ddot{\mathbf{d}} = \mathbf{P}\dot{\mathbf{d}}$, where $\mathbf{P}$ is the interleaving matrix. An example for $\bar{\mathbf{d}}$ with and without $\dot{\mathbf{d}}$ interleaving is shown in Fig. 2. As noted from the figure, it will be hard to accurately estimate the channel coefficients at the non-pilot subcarriers using any interpolation scheme before eliminating the impact of $\ddot{\mathbf{d}}$. When interleaving is used, the received signal becomes

$$\begin{aligned}\mathbf{r} &= \mathbf{G}\mathbf{P}\dot{\mathbf{G}}\mathbf{x} + \mathbf{w} \\ &= \ddot{\mathcal{G}}\mathbf{x} + \mathbf{w}\end{aligned} \tag{10}$$

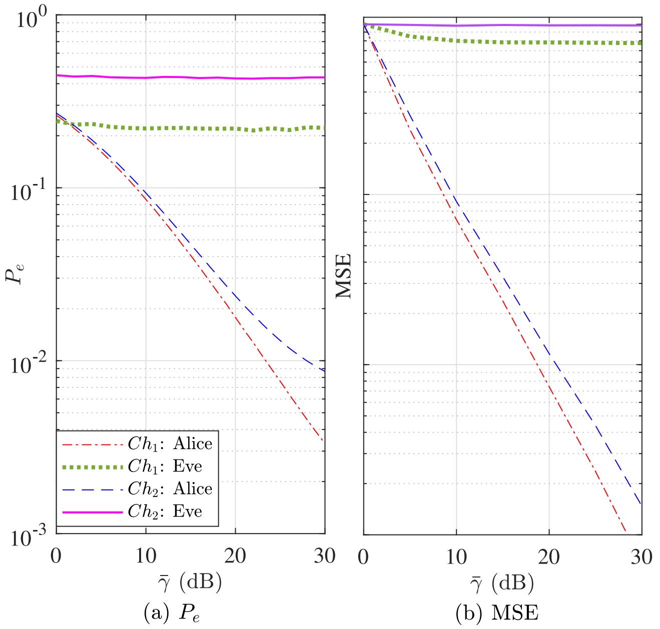
where $\ddot{\mathcal{G}} = \mathbf{G}\ddot{\mathbf{G}}$, and $\ddot{\mathbf{G}} = \mathbf{P}\dot{\mathbf{G}}$ is interleaved version of $\dot{\mathbf{G}}$. Let's denote $\zeta_n = |r^n|, \forall n$. By noting that $\ddot{\mathcal{G}}$ is a diagonal matrix, the legitimate user can initially compute

$$\left[\mathbf{P}\dot{\mathbf{G}}\right]^{-1}\mathbf{r} = \mathbf{G}\mathbf{x} + \mathbf{w}. \tag{11}$$

It is worth noting that (11) is obtained because $\ddot{\mathcal{G}}$ is a diagonal matrix. The next step for the legitimate user is to estimate the channel matrix $\mathbf{G}$ and compute $\mathbf{G}\dot{\mathbf{G}}$, which will be used for the key generation process. The AF matrix $\dot{\mathbf{G}}$ should be initially configured during the system initialization stage, and both Alice and Bob will be informed about the interleaving matrix $\mathbf{P}$. Then, $\dot{\mathbf{G}}$ will be updated continuously as outlined in Algorithm 1. Consequently, both users will synchronously update $\dot{\mathbf{G}}$. The same approach can be applied to the interleaving matrix $\mathbf{P}$. However, the random matrix $\dot{\mathbf{G}}$ can be used to generate $\mathbf{P}$.

To examine the impact of the channel interleaving on Eve's capability to estimate the channel between Alice and Bob, for the extreme scenario, when Bob broadcasts $\ddot{\mathcal{G}}_{BA}\mathbf{x}_B$ while Eve is very close to Alice, and thus $\ddot{\mathcal{G}}_{BA} = \ddot{\mathcal{G}}_{BE}$, and hence, $\mathbf{r}_E = \ddot{\mathcal{G}}_{BA}\mathbf{x}_B + \mathbf{w}_E$. To be able to break the system, Eve needs to know $\mathbf{P}\dot{\mathbf{G}}$, which is not known by Eve. Even if $\mathbf{P}$ is known, it is still difficult for Eve to know $\dot{\mathbf{G}}$. Therefore, unlike conventional PLS systems, spatial decorrelation is not the only source of security in the system. Furthermore, the system should never experience the considered extreme case in practical scenarios. Moreover, the channel matrix $\mathbf{G}$ continuously changes. Therefore, observing the channel for a long time should not leak information about $\mathbf{G}$, $\dot{\mathbf{G}}$, or $\ddot{\mathbf{G}}$. It is worth noting that if Eve wants to use brute-force search to solve (11), then she has to search for $\mathbf{P}\dot{\mathbf{G}}$ that maximizes the correlation between the elements of $\hat{\mathbf{G}}$, which is the estimated version of $\mathbf{G}$. However, by considering a number of subcarriers of about 256, then both $\mathbf{P}$ and $\dot{\mathbf{G}}$ will be 256 × 256 matrices. Moreover, while the elements of $\mathbf{P}$ are binary, the elements of $\dot{\mathbf{G}}$ are continuous. Consequently, the search space, in this case, is massive, theoretically infinite, and Eve would not be able to find $\mathbf{P}\dot{\mathbf{G}}$. Furthermore, assuming that Eve receiver is superior in terms of signal-to-noise ratio (SNR) has generally limited impact on her eavesdropping capability as demonstrated in Fig. 3.

To further study the impact of channel interleaving on Eve and the legitimate users, Fig. 3a shows the bit error rate (BER), P_e for Eve and Alice over Rayleigh fading channel for the worst case scenario where Eve is very close to Alice. We consider two frequency-selective fading channels, denoted as Ch_1 and Ch_2. Both channels have 5 taps with normalized delays of [0, 1, 4, 5, 11] samples. The average taps' gains for Ch_1 are [0.88, 0.07, 0.03, 0.01, 0.01] and for Ch_2 are [0.3584, 0.247, 0.0928, 0.1851, 0.1167]. It can be noted that Ch_1 and Ch_2 represent moderate and severe frequency-selective environments. As can be depicted from Fig. 3, Eve's BER is severely worse than Alice's for all cases and SNR values, which demonstrates the benefit of adopting the AF with interleaving. In addition, P_e is evaluated with and without the interleaving of $\ddot{\mathbf{d}}_{BA}$. Since Alice knows the pilot symbols and $\ddot{\mathbf{d}}_{BA}$, then she first divides $\mathbf{r}_A$ over $\ddot{\mathbf{d}}_{BA}$, and applies the channel estimation process in Section II. Clearly, for both channels Ch_1 and Ch_2, P_e is identical for the two scenarios, which implies that the interleaving process does not affect the estimation capability of the legitimate users. Furthermore, for the same setup, Fig. 3b shows the mean squared error (MSE) for the channel estimation of $\mathbf{G}_{BA}$ at Alice and Eve. It can be seen that the MSE of Alice is much lower than that of Eve.



(a) P_e

(b) MSE

FIGURE 3. (a) The BER, P_e, and (b) the MSE of Alice and Eve when applying AF over Rayleigh fading channels, Ch_1 and Ch_2.

Algorithm 1 Artificial Fading

```
Input: $l$, $\mathbf{x}$, $\mathbf{G}_l$
Initialize: $\dot{\mathbf{G}}$
if $l > 0$ then
    $\dot{\mathbf{G}} = \mathbf{G}_l$
end if
$\ddot{\mathbf{G}} = interleave(\dot{\mathbf{G}})$
$\dot{\mathbf{x}} = \ddot{\mathbf{G}}\mathbf{x}$
Output: $\dot{\mathbf{x}}$
```

Although using the AF is generally beneficial even in frequency-selective channels, it introduces an additional computational complexity of N complex multiplications at the transmitter and N complex divisions at the receiver. To reduce the complexity, the AF can be applied only when the channel does not have sufficient frequency selectivity to produce a reliable bit sequence. To decide if a channel randomness level is not adequate to generate a shared challenge, we consider a counter for the number of sessions where Alice and Bob's challenges are not matching. If the challenge sharing fails for a certain number of consecutive sessions, the channel is considered unsuitable, and AF is incorporated. It is also worth noting that the initially stored channel vector $\mathbf{d}$ should not be used permanently and should be updated frequently. Toward this goal, we use the channel produced during the last successful sequence as the new channel for the AF process.

The AF process is described in Algorithm 1, where the AF buffer is used for storing the AF coefficients. The inputs to the AF algorithm are l, $\mathbf{x}$ and $\mathbf{G}_l$ where l is the counter for the number of successful final key agreement iterations and $\mathbf{G}_l$ is the CFR of the last successful iteration. Prior to the implementation of the protocol, an initial CFR matrix $\dot{\mathbf{G}}$ with a certain fading level is generated and stored in the AF buffer. If $l > 0$ then $\dot{\mathbf{G}}$ is updated such that $\dot{\mathbf{G}} = \mathbf{G}_l$. Then, we interleave $\dot{\mathbf{G}}$ using random interleaving, $\ddot{\mathbf{G}} = \mathit{interleave}(\dot{\mathbf{G}})$, consequently, the transmitted signal can be represented as

$$\dot{\mathbf{x}} = \ddot{\mathbf{G}}\mathbf{x}. \tag{12}$$

B. PROPOSED ADAPTIVE BIT EXTRACTION

Because the elements of $\mathbf{G}_{AB}\dot{\mathbf{G}}_{AB}$ and $\mathbf{G}_{BA}\dot{\mathbf{G}}_{BA}$ are analog values, they cannot be used directly for key generation. Therefore, additional processing is required for BE. In this work, we propose a BE scheme based on the ASBE presented in [20]. In the ASBE, the number of side-channel transmissions and required overhead are significant, particularly when the channel variations are limited and/or the SNR is low.

For notational simplicity, the indices A and B will be dropped unless it is necessary to include them. The proposed BE algorithm for Alice can be explained as follows:

1) Segment $\boldsymbol{\zeta}$ into M blocks $\{\boldsymbol{\zeta}_1, \boldsymbol{\zeta}_2, \dots, \boldsymbol{\zeta}_M\}$ each of which has $\mathcal{K}$ elements. The set of indices for each block is denoted as $\mathbf{I}_m$, $m \in \{1, 2, \dots, M\}$. Because all blocks go through the same process, the block index m will be dropped unless it is necessary to include it. Moreover, the same processes are applied to all blocks.
2) Evaluate two thresholds [20], $z^+ = \mu + \alpha\sigma$ and $z^- = \mu - \alpha\sigma$, where μ, α, and σ are the mean, weight factor and standard deviation of the block, respectively.
3) Construct a $\mathcal{K} \times 3$ matrix where the first column elements are $\mathbf{j} = [1, 2, \dots, N]$, the second column elements are $\mathbf{i} = [1, 2, \dots, N]$, and the third column contains the elements of $\boldsymbol{\zeta}$. The first column elements represent the rows' numbers while the second column elements represent the indices of $\boldsymbol{\zeta}$.
4) Sort the elements of the second and third columns in a descending order based on the values of $\boldsymbol{\zeta}$ elements. Note that the elements of $\mathbf{j}$ remain unsorted.
5) Find the minimum element in the third column where $\zeta_{\{\cdot\}} > z^+$. Store the value of j for that element as $\mathcal{J}_1$.
6) Find the maximum element in third column where $\zeta_{\{\cdot\}} < z^-$. Store the value of j for that element as $\mathcal{J}_2$.
7) Assign a value of one for all elements in the third column, row 1 to row $\mathcal{J}_1$, and zero to all elements in row $\mathcal{J}_2$ to row N.
8) All rows with indices larger than $\mathcal{J}_1$ and less than $\mathcal{J}_2$ should be deleted.
9) Sort the values of columns two and three in a descending order based on the values of the second column, i.e., restore the order of the original elements.

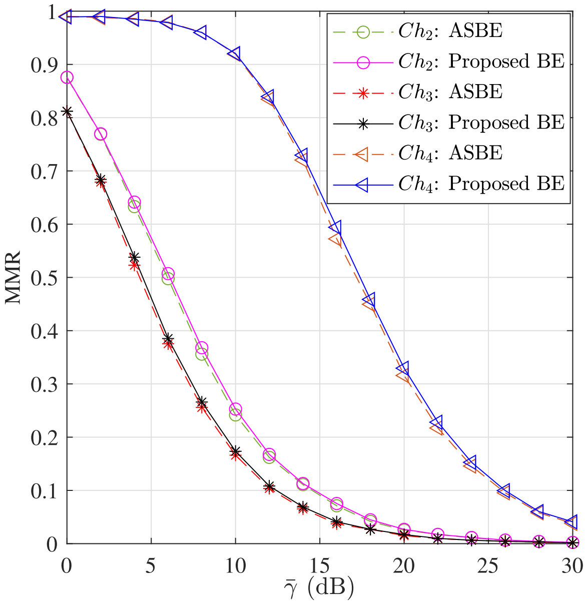
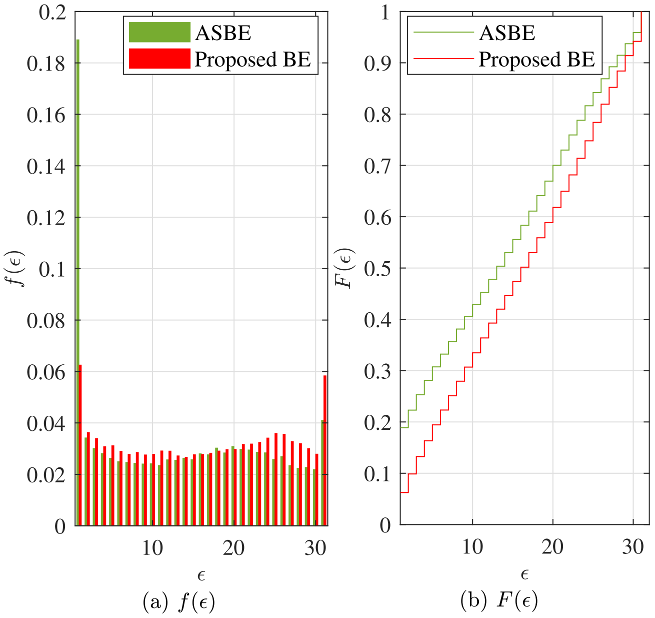


FIGURE 4. The MMR for the proposed BE technique and the ASBE for Ch_2, Ch_3 and Ch_4.

10) To minimize the mismatch between Alice and Bob's intermediate keys, Alice sends Bob the values of $\mathcal{J}_1$ and $\mathcal{J}_2$.

For Bob, steps 1 to 7 are identical to those of Alice. Bob aligns the regions by adjusting his range values such that $\mathcal{J}_{1,B} = \max\{\mathcal{J}_{1,A}, \mathcal{J}_{1,B}\}$ and $\mathcal{J}_{2,B} = \min\{\mathcal{J}_{2,A}, \mathcal{J}_{2,B}\}$. The remaining steps are also similar to those of Alice. However, Bob does not need to share his ranges with Alice. It is worth noting that unlike [20], the proposed algorithm does not leak information about the indices of the selected subcarriers, however, it tells the number of generated bits. Such information should not be critical since the key size is typically assumed to be known by Eve.

In order to compare the performance of the ASBE and the proposed BE, Fig. 4 shows the MMR for three different Rayleigh fading channels, Ch_2, Ch_3, and Ch_4, where Ch_3 and Ch_4 have 5 taps with normalized delays of $[0, 1, 4, 5, 11]$ samples and the average taps' gains are $[0.2, 0.2, 0.2, 0.2, 0.2]$ and $[0.97, 0.02, 0.005, 0.004, 0.001]$, respectively. For this figure, we consider applying the three steps: channel probing, BE with $M = 1$ and $\alpha = 0.4$, and error reconciliation. We use the same setup presented in the numerical results section for the OFDM structure and BCH code $(63, 7, 15)$ for the error reconciliation step. It can be seen that the MMR difference between both techniques is negligible, which makes the proposed mechanism outweighs the ASBE in terms of the needed overhead. Fig. 5 shows the probability mass function (PMF), $f(\epsilon)$, and the cumulative distribution function (CDF), $F(\epsilon)$, comparison where $\epsilon = \sum_{j=1}^{63} |q_A^j - q_B^j|$. The channel probing and BE mechanisms are applied where the considered frequency selective channel is Ch_2 at $\bar{\gamma} = 10$ dB. It can be seen from the PMF that the ASBE outperforms the proposed one. However, due



(a) $f(\epsilon)$ (b) $F(\epsilon)$

FIGURE 5. The PMF and CDF for the proposed BE technique and ASBE [20], $\bar{\gamma} = 10$ dB.

to the correction capability of the BCH code which can correct up to 15 errors, both techniques will have comparable MMR performance as shown in Fig. 4.

C. PROPOSED PUF-BASED FINAL KEY GENERATION

In principle, PUF utilizes the nano-scale manufacturing process variations of semiconductor devices to produce unique keys [16]. Mathematically, for a υ-bit input (called υ-bit challenge) and ς-bit output (called ς-bit response) PUF circuit can be represented by a Boolean function $f : \{0, 1\}^{\upsilon} \rightarrow \{0, 1\}^{\varsigma}$. The unclonability and uniqueness proprieties of PUFs are exploited to enhance the security level of the PLS-based SKG protocol as well as the KGR. In the proposed protocol, we input the intermediate keys, $\mathbf{q}_A$ and $\mathbf{q}_B$, to the PUF or equivalently its emulator and the produced hashed responses are considered as the final secret keys. It should be mentioned that the intermediate or final keys will not be distributed or shared at any step of the protocol. The previously mentioned characteristics of PUFs allow us to accept any number of bits (length) for the intermediate keys and this will not affect the secrecy level of the system. Consequently, unlike the conventional PLS-based SKG, we do not need to wait until a specific number of bits is obtained from the RSS, thus utilizing the PUF leads to high KGR [6], [20]. In order to avoid transmitting the intermediate keys through the channel, both Alice and Bob should have the same set of CRPs obtained by the PUF. Due to the low computational and storage capabilities of UAVs, it is not feasible to store the CRPs at any node. Therefore, we propose to consider a PUF emulator at one side and the actual PUF at the other side. PUFs manufacturers can provide the legitimate parties by the PUF parameters such as gate delays and reliability distribution against voltage and temperature variations. In this paper, we assume that we can emulate the actual PUF using a set of gate delays and reliability models.

For the proposed protocol, we assume that Bob is equipped with a configurable RO PUF [53], which is a delay-based PUF that uses the RO frequencies as the random source for generating the responses, and Alice has its emulator. It is worth noting that professional UAVs are usually equipped with adequate processing power and some custom application-specific integrated circuits (ASICs) to facilitate several types of operations [54]. Therefore, the RO PUF can be implemented using around 0.006 mm^2 area using 22 nm technology, which is fairly small. Another possibility is to use external mini FPGA board and connect it to the UAV motherboard through any of the available communications ports. Due to the sensitivity of PUFs to temperature and voltage variations, we consider that the emulator response is similar to the PUF response that is generated at room temperature with a fixed voltage of 3 V, which is denoted as the typical response. Also, we assume that any attempt to tamper or separate the PUF will destroy it [55]. The process to generate the final key starts by inputting the intermediate keys $\mathbf{q}_B$ and $\mathbf{q}_A$ to the PUF and its emulator at Bob's and Alice's sides, respectively. The detailed steps are as follows:

1) *Response Generation:* Alice will input $\mathbf{q}_A$ to the PUF emulator whereas Bob will input $\mathbf{q}_B$ to the PUF. The responses $\mathbf{y}_A$ and $\mathbf{y}_B$ are produced at Alice's and Bob's sides, respectively. Ideally speaking, the responses should be identical under any environmental setting, however, practically it is not the case.
2) *Error Reconciliation and Verification:* The aim of this step is to ensure that $\mathbf{y}_A$ and $\mathbf{y}_B$ are identical in the presence of temperate and voltage variations. Therefore, the error reconciliation mechanism described in Section III can be applied. In this work, we consider that the encoder is located at Alice's side and the decoder is at Bob's side. Moreover, the verification of the responses agreement is performed using CRC at Alice's and Bob's sides, $\mathbf{c}_A^p$ and $\mathbf{c}_B^p$, respectively. At Alice's side, we compute
$$\mathbf{s}^p = \left[\mathbf{s}_1^p, \mathbf{s}_2^p\right] = \left[\mathbf{y}_A \oplus \mathbf{v}_A^p, \mathbf{c}_A^p\right] \tag{13}$$
Then, Alice modulates and transmits $\mathbf{s}^p$ to Bob who detects $\tilde{\mathbf{s}}^p$ and computes $\tilde{\mathbf{v}}_A^p$ as in (9). Once $\mathbf{q}_B$ is obtained, Bob calculates $\mathbf{c}_A^P$ to compare it with $\tilde{\mathbf{c}}_A^P$. If both CRCs are equal, then Bob will send an acknowledgment to Alice. Otherwise, a negative acknowledgment is to be sent. In the latter case, the final key generation steps 1 and 2 are repeated until a key generation agreement is reached.
3) *Hash Generation:* Some information about the shared challenges and responses is leaked to Eve during the error reconciliation steps. Thus, we utilize universal hash functions (UHFs) [56] to generate the final keys, $\mathbf{K}_A = H(\mathbf{y}_A)$ and $\mathbf{K}_B = H(\mathbf{y}_B)$, to enhance the randomness level.

D. PUF MODELING ATTACK

We assume that Eve is aware of the proposed SKG protocol, including the decided parameters of the proposed BE and error reconciliation steps. As mentioned earlier in Section I, ML attacks are challenging for PUFs due to the possibility of modeling them using the transmitted CRPs and side-channel information without physical intervention. The key generation protocol can be considered secure if Eve is not able to predict the correct keys given the knowledge of the used techniques and having full access to the transmitted data. We also assume that the benefit of an attack diminishes if Eve needs to continuously employ significant computing power beyond a reasonable time span [57]. In Fig. 1, we call the model resulting from the ML attack as "PUF prediction model." In our scheme, the following 4 secrets are shared over the channel: $\mathbf{s}^q$, $\mathbf{s}^p$, $\mathcal{J}_1$ and $\mathcal{J}_2$. We assume that the attacker has access to all data transmitted between Alice and Bob. The ML attacks require Eve to collect a sufficient subset of CRPs and side-channel information to build an accurate PUF. As presented earlier in Sections III and IV-C, the intermediate and final keys generation stages do not require any explicit transmission of the PUF CRPs. Moreover, the shared data $\mathbf{s}^q$ and $\mathbf{s}^p$ will not be useful for Eve unless she has the correct $\mathbf{v}^q$ and $\mathbf{v}^p$ to be able to accurately obtain $\mathbf{q}$ and $\mathbf{y}$ which is very unlikely because $\mathbf{v}$ is a codeword that corresponds to a random binary vector. As for $\mathcal{J}_1$ and $\mathcal{J}_2$, they only represent the range of the dropped indices during the BE step. Actually, if the RSS is not known, then these indices do not reveal useful information for Eve. Therefore, we can consider that the proposed SKG is secure since the leaked information is not significant to produce a subset of CRPs to model the PUF over a reasonable time span.

Fig. 6 shows the cross-correlation between Alice and Bob ρ_{AB}, and Alice and Eve ρ_{AE} [58, eq. (2.75)] in the best-case scenario for Eve, where she is located in the middle between Alice and Bob. This means that her fading channel is the same as the legitimate channel. However, the AF coefficients are known only to legitimate users. We assess the correlation between $\mathbf{q}_A$ and $\mathbf{q}_B$ and $\mathbf{q}_A$ and $\mathbf{q}_E$. Two Rayleigh fading channels are considered Ch_1 and Ch_2, and the OFDM, AF, BE and error reconciliation parameters are presented in Section V. It is clear that the level of correlation between Alice and Eve is considerably lower than between Alice and Bob, which is due to the impact of the induced AF at Alice's transmitters. Consequently, the intermediate key MMR between Eve and the legitimate users will be considerably high. Therefore, with regards to the PUF, it is challenging for Eve to estimate the challenge. Thus, generating a CRPs model is highly unlikely.

E. COMPUTATIONAL COMPLEXITY

Although the new generation of professional UAVs have high computational capabilities [54], it is still necessary to evaluate the complexity of the main processing blocks of the proposed SKG systems. As can be noted from the proposed system description, the main operations performed by a given UAV are the BCH encoding and decoding for the secure sketch, the BE, AF application and elimination, CRC generation and verification, the PUF and PUF emulator, and finally, the OFDM modulation and demodulation. It is also required to compute the power of the channel estimates. Except for the PUF/emulator, the complexity of most operations is dominated by multiplication and division operations. If we denote the complex multiplication (CM) and complex dividion (CD) operations by M_C and D_C, then the complexity can be generally evaluated as follows.

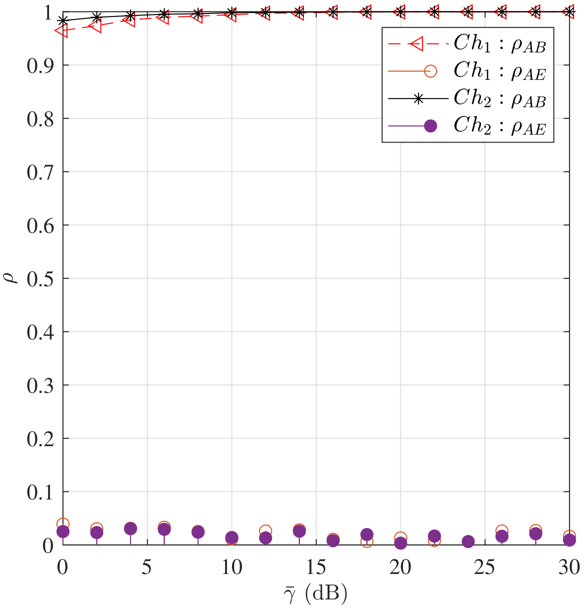


FIGURE 6. The cross-correlation ρ_{AB} and ρ_{AE} over Rayleigh fading channel for Ch_1 and Ch_2.

The Radix-2 fast Fourier transform (FFT) and inverse fast Fourier transform (IFFT) requires $N \log_2 N$ CMs. The least-square channel estimation requires N CDs. The channel estimates magnitude computation requires N CMs. The BE requires N CMs to compute the thresholds. The AF application and elimination require N CMs and CDs, respectively. It is worth noting that the multiplication process associated with interleaving is not considered because it is a simple 0 or 1 multiplication. The CRC computation is computed using a linear feedback shift register, so it does not encounter any arithmetic operation. The BCH encoding can be realized using simple digital logic devices. If hard decision decoding is adopted, then the decoder complexity is comparable to the encoder complexity. It is worth noting that the CRC and error reconciliation are applied at the intermediate and final key generation stages. The RO PUF can be implemented using a custom ASICs, which requires about 0.006 mm^2 area using 22 nm technology, which is fairly small. Another possibility is to use external mini FPGA board and connect it to the UAV motherboard through any of the available communications ports. The PUF emulator complexity depends on the adopted method. The lookup table can be considered the least demanding approach because a limited number of challenge-response pairs can be stored and used during a given mission, and it can be updated for consequent missions. It is worth noting that the computational power can be evaluated based on the computational complexity as described in [59]. Overall, it can be concluded that the proposed scheme's computational complexity and computational power are suitable for most professional UAVs.

V. NUMERICAL RESULTS

This section presents a wide range of numerical results to evaluate the performance of the proposed SKG protocol. The simulation results are obtained using a computing machine that runs Intel Xeon CPU E5-2640 processor, clock frequency of 2.5 GHz, 16 GB RAM, and 64 bit operating system. The software tool used to generate the results is MATLAB R2022b. The system model considers an OFDM system with $N = 256$ subcarriers that are modulated using QPSK. The number of CP samples, pilot and null subcarriers are $N_c = 64$, $N_p = 25$ and $N_n = 53 \times 2$, respectively. The null subcarriers split equally and are located at the edges of the subcarriers. The number of OFDM symbols considered to assess the performance of the proposed protocol is 1.2×10^4 for each simulation point. The wireless channel is modeled as a quasi-static Rician frequency-selective fading channel with $K \in \{-\infty, 15\}$ dB, where the channel remains fixed during a given OFDM symbol but changes randomly between adjacent symbols. The case where $K = -\infty$ corresponds to the Rayleigh fading. Two multipath fading channel models are considered in this section, Ch_1 and Ch_2 are defined in Section IV. Moreover, in order to examine the proposed protocol under practical conditions, we vary the correlation factor ρ_{AB} between the channels of Alice and Bob. For notational simplicity, we denote ρ_{AB} as ρ. The chosen correlation values are $\rho = \{1, 0.88\}$. As for the proposed BE, we chose $M = 2$ and $\alpha = 0.4$. For the AF, the initially stored $\dot{\mathbf{G}}$ in the AF buffer is the FFT of $[0.246 - 0.599i, 0.594 - 0.141i, 0, 0, -0.619 + 0.0938i, 0.211 + 0.876i, 0, 0, 0, 0, 0, 0.0713 + 0.619i, 0, 0, \dots, 0]$, where the length of the vector is equal to N. For conciseness, we denote the proposed SKG as (P. SKG) and the conventional SKG presented in [20] as (C. SKG).

The PUF considered in this paper is presented in [53]. As tested in the paper, the uniqueness and uniformity are almost 50%. Also, in order to reflect the impact of temperature and voltage changes on the PUF responses, we use the presented reliability distribution in terms of the intra-hamming distance, which is obtained by conducting several experiments on FPGA. The reliability distribution of [53] is shown in Fig. 7. As mentioned earlier in Section I, the emulator response is considered as the original response. The reference temperature and voltage are, respectively, set as 26^oC and $3V$. The length of the response of the PUF and its emulator is 127 bits.

We have implemented the proposed configurable RO PUF of [53] on FPGA to verify its reliability. Due to the area limitation of the FPGA, the lengths of the challenge and response are chosen to be 32 bits. First, to ensure that the PUF can produce the same response to a certain challenge given fixed temperature and voltage, we ran it for 2500 times at 25^o C and $3V$. As expected, the same response is obtained in every run. Fig. 7 shows the intra-hamming distance distribution of the 32 bits responses under 4 different temperatures $[40^o, 50^o, 60^o, 70^o]$ C with reference temperature 25^o C. For each temperature value, 5×10^3 responses are produced. As can be noted, most of the measurements have 1 to 3 errors when compared to the reference response, which can be corrected using the utilized error-correcting code-based secure sketch.

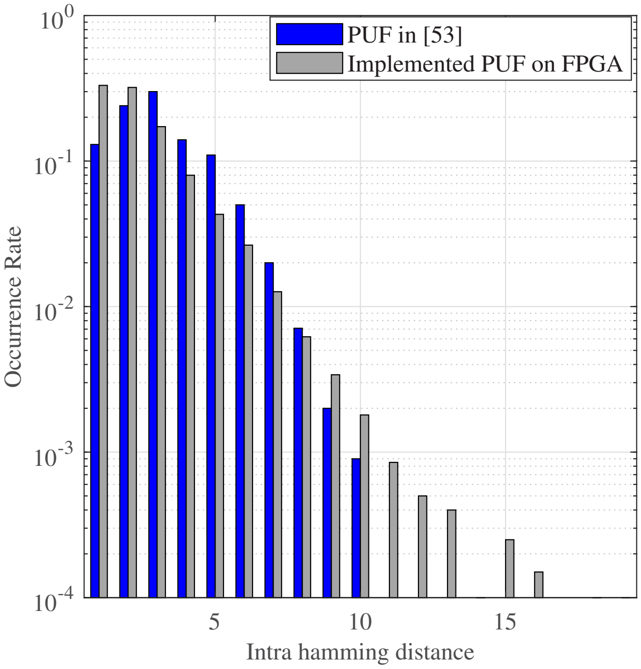
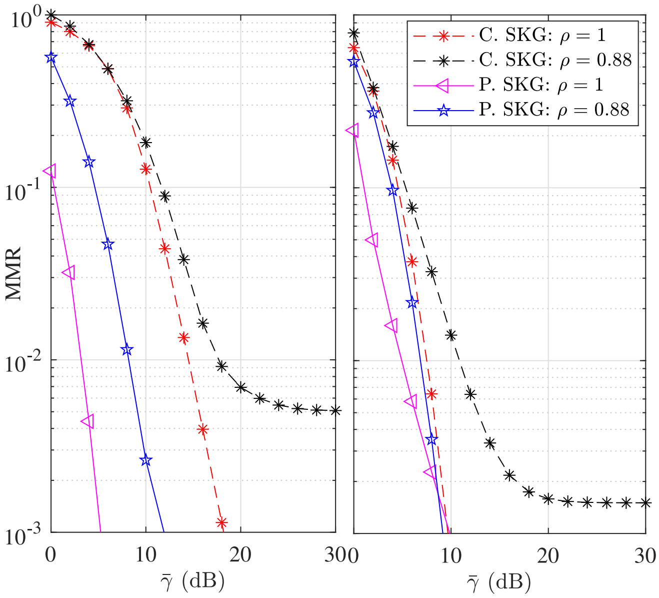


FIGURE 7. The intra-hamming distance distribution for the RO PUF presented in [53] and the implemented RO PUF on FPGA.

As for the error reconciliation step in the intermediate and final SKG stages, we use error-correcting code-based secure sketch [6]. We consider BCH as the underlying code where we use (63, 7, 15) for the intermediate SKG and (127, 8, 31) for the final SKG stage. It should be noted that the error correction capability is related to the rate of the code. It should be noted that, unlike the C. SKG, for the intermediate key generation stage, we do not restrict the number of generated bits to be 63 bits as the PUF can generate uncorrelated responses and cannot be predicted by Eve. If the length of $\mathbf{q}_A$ or $\mathbf{q}_B$ is less than 63 bits, we append the vector by zeros.

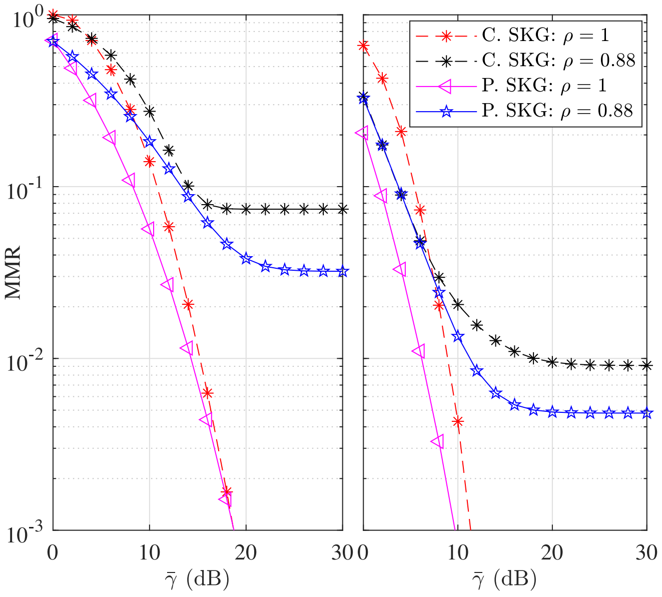
Due to the multiple signals exchanges, we amplify the responses $\mathbf{y}_A$ and $\mathbf{y}_B$ privacy by applying SHA-256 hash function [56]. The outputs of the SHA-256 functions are the final keys of Alice and Bob, $\mathbf{K}_A$ and $\mathbf{K}_B$, respectively, with a length of 256 bits.

Figures 8 and 9 show the MMR for the final keys by applying the P. SKG protocol and the C. SKG for $K = \{-\infty, 15\}$ dB over Ch_1 and Ch_2. We consider the ASBE



(a) Ch_1 (b) Ch_2

FIGURE 8. The key MMR for the P. SKG and the C. SKG protocols for $K = 15$ dB.



(a) Ch_1 (b) Ch_2

FIGURE 9. The key MMR for the P. SKG and the C. SKG protocols for Rayleigh fading.

scheme for the conventional protocol. For all the presented scenarios, as the SNR increases, the MMR decreases, which results from the reduced impact of the independent noise and the dominance of the multipath fading. Let's start with the case of $\rho = 1$, i.e., perfect CR, to study the impact of the channel frequency selectivity on the key MMR. First, for both multipath channels, as K decreases, the MMR decreases. This is due to the impact of the higher correlation and common variations between Alice and Bob for the more severe channel (Rayleigh fading). Moreover, it can be noticed that Ch_1 results in higher MMR than Ch_2 due to the lower frequency selectivity level, which leads to higher noise dominance. As mentioned previously in Section I, the channel measurements of the uplink and downlink are asymmetric due to hardware imperfections. Therefore, we vary the amount of correlation between Alice and Bob. Clearly, as ρ decreases, the key MMR increases, as the entire protocol depends on the level of matching between $|\mathbf{r}_A|$ and $|\mathbf{r}_B|$. Moreover, as can be noted from both figures, our proposed protocol performs significantly better than the conventional SKG protocol. This is due to the impact of the AF on the correlation between Alice and Bob. In other words, by applying the AF on both sides, the amount of common variations and correlation increase, which is similar to the impact of increasing the fading selectivity level, which increases the probability to agree on a shared key.

Fig. 10 shows the average number of sessions required for Alice and Bob to agree on a key, $\mathbf{K}_A = \mathbf{K}_B$ for the P. SKG and C. SKG protocols. It can be noted that for both protocols, as the SNR increases, the average number of sessions decreases, which is due to the reduced impact of the noise. Also, the P. SKG results in lower values due to the utilization of PUF and AF. The use of PUF does not restrict us on any intermediate key length, hence unlike the C. SKG protocol, we can generate the final keys from any number of bits and this does not affect the secrecy level of the system. In other words, instead of waiting until we get 63 bits for the $\mathbf{q}$ in the C. SKG, in our protocol, we append the $\mathbf{q}$ with zeros to get 63 bits. Also, due to the higher correlation between Alice and Bob resulting from applying AF, the average number of times required to achieve a key agreement is lower than the C. SKG.

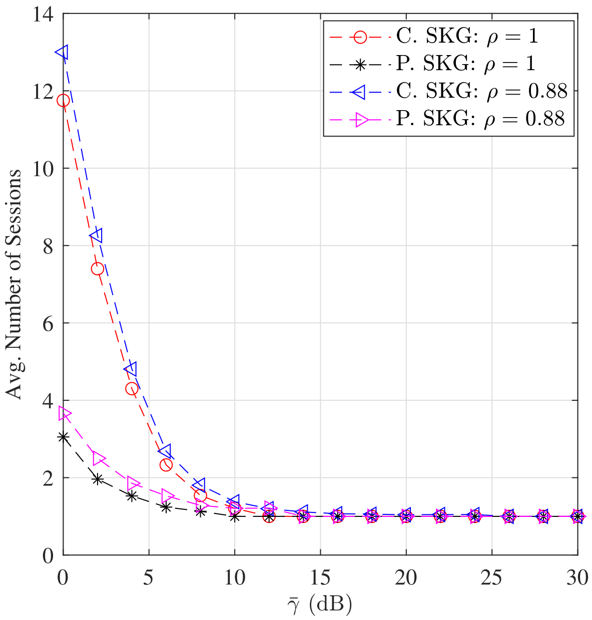


FIGURE 10. The average number of sessions required until a key agreement for P. SKG and the C. SKG protocols for Rayleigh fading channel.

TABLE 1. National institute of science and technology (NIST) for keys generated by P. SKG.

	Ch_1		Ch_2	
Test	$\rho = 1$	$\rho = 0.88$	$\rho = 1$	$\rho = 0.88$
Frequency	0.7042	0.6510	0.4461	0.5464
Block frequency	0.6708	0.3568	0.5088	0.4323
Cumulative sums (Fwd)	0.4470	0.6600	0.5690	0.8285
Cumulative sums (Rev)	0.6339	0.9981	0.7179	0.9067
Runs	0.9436	0.2593	0.5349	0.5149
FFT	0.5806	0.1566	0.7813	0.4588
Approx. Entropy	0.4511	0.4545	0.7647	0.5929
Serial	$0.4249, 0.1473$	$0.3537, 0.2297$	$0.8275, 0.7706$	$0.9132, 0.8924$

TABLE 2. NIST for keys generated by C. SKG [20].

	Ch_1		Ch_2	
Test	$\rho = 1$	$\rho = 0.88$	$\rho = 1$	$\rho = 0.88$
Frequency	0.5190	0.4744	0.2575	0.6387
Block frequency	0.2016	0.0.2101	0.3670	0.3292
Cumulative sums (Fwd)	0.3918	0.4936	0.4717	0.5103
Cumulative sums (Rev)	0.2307	0.8386	0.6995	0.8600
Runs	0.4613	0.1557	0.5349	0.3461
FFT	0.3538	0.7545	0.8570	0.5914
Approx. Entropy	0.2103	0.2806	0.3699	0.3292
Serial	$0.4279, 0.9592$	$0.3640, 0.7437$	$0.4653, 0.5442$	$0.3016, 0.4924$

In order to assess the randomness of the final keys generated by the proposed SKG protocol, we use the NIST suite [60]. The suite consists of 15 tests and computes a probability value for each test, called p-value. For practical considerations related to the minimum input length required for every test, we decided to compute 8 tests [20]. The key can be considered random with 99% confidence if the corresponding p-values are greater than 0.01. We run our proposed protocol using the same coefficients and parameters listed previously for $\bar{\gamma} = 16$ dB. Table 1 shows the p-values of the NIST tests. Since the final keys pass all the tests as shown in Table 1, they are considered random with 99% confidence.

For comparison purposes, we ran the NIST test for the C. SKG protocol as shown in Table 2. For a fair comparison with the settings of our protocol, we ensure that the length of the keys input to the hash generation step is 127 bits. We can note from Table 2 that the keys produced by this protocol pass the NIST test and are hence considered random.

VI. CONCLUSION

This work proposed a novel framework that integrates PLS with PUF to strengthen the secrecy and improve the efficiency of the key generation and sharing processes for dynamic and static wireless channels. More specifically, in the case of flat fading or poor scattering environments, we proposed a novel technique denoted as AF, which overlays a user-defined frequency-selective fading over the actual channel experienced between the legitimate users. Although AF results in higher computational complexity, it leads to a significant drop in the MMR compared to the conventional PLS-based SKG protocols. Further, it results in a lower average number of sessions needed to agree on a shared key. Furthermore, we proposed an efficient BE scheme that has reduced overhead, less number of side-channel transmissions, and increased secrecy, as compared to conventional schemes. The obtained numerical results showed a significant reduction in the MMR of the proposed protocol when compared to existing conventional SKG protocols. It is also shown that we can achieve a key agreement in a single session for moderate and high SNR ranges in rich scattering environments or equivalently when AF and PUF mechanisms are applied.

Our future work will focus on extending the proposed system to a UAV swarm where a group key can be generated and shared. Such an extension is generally not straightforward because each UAV would require a PUF emulator or a lookup table for all other UAVs PUFs, which is prohibitively expensive. Moreover, using other advanced error correction schemes for the secure sketch process will be considered to reduce the number of sessions required to reach a key agreement. The use of multiple antennas at the UAVs to enhance the channel entropy will also be considered.

APPENDIX
LIST OF ACRONYMS

A2A	air-to-air.
A2G	air-to-ground.
AF	artificial fading.
ANN	artificial neural network.
ASBE	adaptive secret bit extraction.
ASIC	application-specific integrated circuit.
AWGN	additive white Gaussian noise.
BCH	Bose–Chaudhuri–Hocquenghem.
BE	bit extraction.
BER	bit error rate.
BPSK	binary phase shift keying.
CD	complex dividion.
CDF	cumulative distribution function.
CFR	channel frequency response.
CM	complex multiplication.
CP	cyclic prefix.
CR	channel reciprocity.
CRC	cyclic redundancy check.
CRP	challenge-response pair.
CSI	channel state information.
DFT	discrete Fourier transform.
FFT	fast Fourier transform.
FPGA	field programmable gate array.
i.i.d.	independent and identically distributed.
IC	integrated circuit.
IDFT	inverse discrete Fourier transform.
IFFT	inverse fast Fourier transform.
IoT	Internet of Things.
IRS	intelligent reflective surface.
ISI	inter-symbol interference.
KGR	key generation rate.
LoS	line-of-sight.
LR	logistic regression.
LS	least-square.
LTE	long-term evolution.
MIMO	multiple-input multiple-output.
ML	machine learning.
MMR	mismatch ratio.
MMSE	minimum mean-square error.
MSE	mean squared error.
NIST	national institute of science and technology.
OFDM	orthogonal frequency-division multiplexing.
PLS	physical layer security.
PMF	probability mass function.
PUF	physically unclonable function.
QAM	quadrature amplitude modulation.
QPSK	quadrature phase shift keying.
RO	ring oscillator.
RSS	received signal strength.
SINR	signal to interference plus noise ratio.
SKG	secret key generation.
SNR	signal-to-noise ratio.
SVM	support vector machine.
TDD	time division duplexing.
UAV	unmanned aerial vehicle.
UHF	universal hash function.
XOR	exclusive or.

REFERENCES

[1] "Unmanned aerial vehicle (UAV) market search report," MarketsandMarkets Res., Northbrook, IL, USA, Rep. AS 2802, Jun. 2021. [Online]. Available: https://www.marketsandmarkets.com/Market-Reports/unmanned-aerial-vehicles-uav-market-662.html

[2] A. Al-Dweik and Y. Iraqi, "High throughput wireless links for time-sensitive WSNs with reliable data requirements," *IEEE Sensors J.*, vol. 21, no. 21, pp. 24890–24898, Nov. 2021.

[3] J. M. Hamamreh, H. M. Furqan, and H. Arslan, "Classifications and applications of physical layer security techniques for confidentiality: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1773–1828, 2nd Quart., 2019.

[4] J. Zhang, T. Q. Duong, A. Marshall, and R. Woods, "Key generation from wireless channels: A review," *IEEE Access*, vol. 4, pp. 614–626, 2016.

[5] Y. Peng, P. Wang, W. Xiang, and Y. Li, "Secret key generation based on estimated channel state information for TDD-OFDM systems over fading channels," *IEEE Trans. Wireless Commun.*, vol. 16, no. 8, pp. 5176–5186, Aug. 2017.

[6] N. Aldaghri and H. Mahdavifar, "Physical layer secret key generation in static environments," *IEEE Trans. Inf. Forensics Security*, vol. 15, pp. 2692–2705, 2020.

[7] H. Qin et al., "Power allocation and time-domain artificial noise design for wiretap OFDM with discrete inputs," *IEEE Trans. Wireless Commun.*, vol. 12, no. 6, pp. 2717–2729, Jun. 2013.

[8] S. Gollakota and D. Katabi, "Physical layer wireless security made fast and channel independent," in *Proc. IEEE INFOCOM*, 2011, pp. 1125–1133.

[9] T. Akitaya, S. Asano, and T. Saba, "Time-domain artificial noise generation technique using time-domain and frequency-domain processing for physical layer security in MIMO-OFDM systems," in *Proc. IEEE ICC Workshop*, 2014, pp. 807–812.

[10] S. Liu, Y. Hong, and E. Viterbo, "Practical secrecy using artificial noise," *IEEE Commun. Lett.*, vol. 17, no. 7, pp. 1483–1486, Jul. 2013.

[11] S. Liu, Y. Hong, and E. Viterbo, "Artificial noise revisited," *IEEE Trans. Inf. Theory*, vol. 61, no. 7, pp. 3901–3911, Jul. 2015.

[12] R. Pappu, "Physical one-way functions," *Science*, vol. 297, no. 5589, pp. 2026–2030, 2002.

[13] S. Taneja, A. B. Alvarez, and M. Alioto, "Fully synthesizable PUF featuring hysteresis and temperature compensation for 3.2% native BER and 1.02 fJ/b in 40 nm," *IEEE J. Solid-State Circuits*, vol. 53, no. 10, pp. 2828–2839, Oct. 2018.

[14] B. Chatterjee, D. Das, S. Maity, and S. Sen, "RF-PUF: Enhancing IoT security through authentication of wireless nodes using in-situ machine learning," *IEEE Internet Things J.*, vol. 6, no. 1, pp. 388–398, Feb. 2019.

[15] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: A tutorial," *Proc. IEEE*, vol. 102, no. 8, pp. 1126–1141, Aug. 2014.

[16] P. Mall, R. Amin, A. K. Das, M. T. Leung, and K.-K. R. Choo, "PUF-based authentication and key agreement protocols for IoT, WSNs, and smart grids: A comprehensive survey," *IEEE Internet Things J.*, vol. 9, no. 11, pp. 8205–8228, Jun. 2022.

[17] K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," *IEEE Wireless Commun.*, vol. 18, no. 4, pp. 6–12, Aug. 2011.

[18] D. Wang, B. Bai, W. Zhao, and Z. Han, "A survey of optimization approaches for wireless physical layer security," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1878–1911, 2nd Quart., 2019.

[19] N. Patwari, J. Croft, S. Jana, and S. K. Kasera, “High-rate uncorrelated bit extraction for shared secret key generation from channel measurements,” *IEEE Trans. Mobile Comput.*, vol. 9, no. 1, pp. 17–30, Jan. 2010.

[20] S. N. Premnath et al., “Secret key extraction from wireless signal strength in real environments,” *IEEE Trans. Mobile Comput.*, vol. 12, no. 5, pp. 917–930, May 2013.

[21] H. Koorapaty, A. A. Hassan, and S. Chennakeshu, “Secure information transmission for mobile radio,” *IEEE Commun. Lett.*, vol. 4, no. 2, pp. 52–55, Feb. 2000.

[22] S. Xiao, Y. Guo, K. Huang, and L. Jin, “Cooperative group secret key generation based on secure network coding,” *IEEE Commun. Lett.*, vol. 22, no. 7, pp. 1466–1469, Jul. 2018.

[23] D. Qin and Z. Ding, “Exploiting multi-antenna non-reciprocal channels for shared secret key generation,” *IEEE Trans. Inf. Forensics Security*, vol. 11, pp. 2693–2705, 2016.

[24] J. Zhang, H. Du, Q. Sun, B. Ai, and D. W. K. Ng, “Physical layer security enhancement with reconfigurable intelligent surface-aided networks,” *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 3480–3495, 2021.

[25] S. Naderi, D. B. da Costa, and H. Arslan, “Joint random subcarrier selection and channel-based artificial signal design aided PLS,” *IEEE Wireless Commun. Lett.*, vol. 9, no. 7, pp. 976–980, Jul. 2020.

[26] X. Hu, L. Jin, K. Huang, X. Sun, Y. Zhou, and J. Qu, “Intelligent reflecting surface-assisted secret key generation with discrete phase shifts in static environment,” *IEEE Wireless Commun. Lett.*, vol. 10, no. 9, pp. 1867–1870, Sep. 2021.

[27] P. Viswanath, D. N. C. Tse, and R. Laroia, “Opportunistic beamforming using dumb antennas,” *IEEE Trans. Inf. Theory*, vol. 48, no. 6, pp. 1277–1294, Jun. 2002.

[28] N. Ebrahimi, H.-S. Kim, and D. Blaauw, “Physical layer secret key generation using joint interference and phase shift keying modulation,” *IEEE Trans. Microw. Theory Techn.*, vol. 69, no. 5, pp. 2673–2685, May 2021.

[29] D. Chen, Z. Qin, X. Mao, P. Yang, Z. Qin, and R. Wang, “SmokeGrenade: An efficient key generation protocol with artificial interference,” *IEEE Trans. Inf. Forensics Security*, vol. 8, no. 11, pp. 1731–1745, 2013.

[30] W. Trappe, “The challenges facing physical layer security,” *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 16–20, Jun. 2015.

[31] Z. Ji et al., “Vulnerabilities of physical layer secret key generation against environment reconstruction based attacks,” *IEEE Wireless Commun. Lett.*, vol. 9, no. 5, pp. 693–697, May 2020.

[32] M. A. Qureshi and A. Munir, “PUF-RAKE: A PUF-based robust and lightweight authentication and key establishment protocol,” *IEEE Trans. Dependable Secure Comput.*, vol. 19, no. 4, pp. 2457–2475, Jul./Aug. 2022.

[33] Y. Bai and Z. Yan, “A novel key generation scheme using quaternary PUF responses and wiretap polar coding,” *IEEE Commun. Lett.*, vol. 25, no. 7, pp. 2142–2145, Jul. 2021.

[34] M. A. Usmani, S. Keshavarz, E. Matthews, L. Shannon, R. Tessier, and D. E. Holcomb, “Efficient PUF-based key generation in FPGAs using per-device configuration,” *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 27, no. 2, pp. 364–375, Feb. 2019.

[35] Y. Zhang, Z. He, M. Wan, J. Liu, H. Gu, and X. Zou, “A SC PUF standard cell used for key generation and anti-invasive-attack protection,” *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 3958–3973, 2021.

[36] G. E. Suh and S. Devadas, “Physical unclonable functions for device authentication and secret key generation,” in *Proc. ACM/IEEE Des. Autom. Conf.*, 2007, pp. 9–14.

[37] M. N. Aman, K. C. Chua, and B. Sikdar, “Mutual authentication in IoT systems using physical unclonable functions,” *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1327–1340, Oct. 2017.

[38] S. Zeitouni, Y. Oren, C. Wachsmann, P. Koeberl, and A.-R. Sadeghi, “Remanence decay side-channel: The PUF case,” *IEEE Trans. Inf. Forensics Security*, vol. 11, pp. 1106–1116, 2016.

[39] P. Gope, O. Millwood, and B. Sikdar, “A scalable protocol level approach to prevent machine learning attacks on physically unclonable function based authentication mechanisms for Internet of medical things,” *IEEE Trans. Ind. Informat.*, vol. 18, no. 3, pp. 1971–1980, Mar. 2022.

[40] V. Suresh, R. Kumar, M. Anders, H. Kaul, V. De, and S. Mathew, “A 0.26% BER, 10^{28} challenge-response machine-learning resistant strong-PUF in 14nm CMOS featuring stability-aware adversarial challenge selection,” in *Proc. IEEE Symp. VLSI Circuits*, 2020, pp. 1–2.

[41] Y. Cao, C. Q. Liu, and C. H. Chang, “A low power diode-clamped inverter-based strong physical unclonable function for robust and lightweight authentication,” *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 65, no. 11, pp. 3864–3873, Nov. 2018.

[42] A. Venkatesh, A. B. Venkatasubramaniyan, X. Xi, and A. Sanyal, “0.3 pJ/bit machine learning resistant strong PUF using subthreshold voltage divider array,” *IEEE Trans. Circuits Syst. II, Exp. Brief*, vol. 67, no. 8, pp. 1394–1398, Aug. 2020.

[43] A. Saci, A. Al-Dweik, A. Shami, and Y. Iraqi, “One-shot blind channel estimation for OFDM systems over frequency-selective fading channels,” *IEEE Trans. Commun.*, vol. 65, no. 12, pp. 5445–5458, Dec. 2017.

[44] A. Al-Dweik, F. Kalbat, S. Muhaidat, O. Filio, and S. M. Ali, “Robust MIMO-OFDM system for frequency-selective mobile wireless channels,” *IEEE Trans. Veh. Technol.*, vol. 64, no. 5, pp. 1739–1749, May 2015.

[45] M. A. Al-Jarrah, K.-H. Park, A. Al-Dweik, and M.-S. Alouini, “Error rate analysis of amplitude-coherent detection over Rician fading channels with receiver diversity,” *IEEE Trans. Wireless Commun.*, vol. 19, no. 1, pp. 134–147, Jan. 2020.

[46] A. Saci, A. Al-Dweik, and A. Shami, “Direct data detection of OFDM signals over wireless channels,” *IEEE Trans. Veh. Technol.*, vol. 69, no. 11, pp. 12432–12448, Nov. 2020.

[47] O. A. Topal, G. K. Kurt, and B. Özbek, “Key error rates in physical layer key generation: Theoretical analysis and measurement-based verification,” *IEEE Wireless Commun. Lett.*, vol. 6, no. 6, pp. 766–769, Dec. 2017.

[48] J. Zhang et al., “Experimental study on key generation for physical layer security in wireless communications,” *IEEE Access*, vol. 4, pp. 4464–4477, 2016.

[49] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-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.

[50] K. Moara-Nkwe, Q. Shi, G. M. Lee, and M. H. Eiza, “A novel physical layer secure key generation and refreshment scheme for wireless sensor networks,” *IEEE Access*, vol. 6, pp. 11374–11387, 2018.

[51] A. Ahmed, A. Al-Dweik, Y. Iraqi, H. Mukhtar, M. Naeem, and E. Hossain, “Hybrid automatic repeat request (HARQ) in wireless communications systems and standards: A contemporary survey,” *IEEE Commun. Surveys Tuts.*, vol. 23, no. 4, pp. 2711–2752, 4th Quart., 2021.

[52] M. Jana, A. Medra, L. Lampe, and J. Mitra, “Pre-equalized faster-than-Nyquist transmission,” *IEEE Trans. Commun.*, vol. 65, no. 10, pp. 4406–4418, Oct. 2017.

[53] D. Deng, S. Hou, Z. Wang, and Y. Guo, “Configurable ring oscillator PUF using hybrid logic gates,” *IEEE Access*, vol. 8, pp. 161427–161437, 2020.

[54] “UAV navigation group.” Accessed: Dec. 19, 2022. [Online]. Available: https://www.uavnavigation.com

[55] M. Kirkpatrick et al., “System on chip and method for cryptography using a physically unclonable function,” U.S. Patent 8 750 502 B2, Mar. 22, 2012.

[56] FIPS PUB, “Secure hash standard (SHS),” Nat. Inst. Stand. Technol., Gaithersburg, MD, USA, Rep. FIPS 180-4, 2015.

[57] S. S. Zalivaka, A. A. Ivaniuk, and C.-H. Chang, “Reliable and modeling attack resistant authentication of arbiter PUF in FPGA implementation with trinary quadruple response,” *IEEE Trans. Inf. Forensics Security*, vol. 14, pp. 1109–1123, 2019.

[58] S. K. Maitra, *Digital Signal Processing: A Computer-Based Approach*, 4th ed. New York, NY, USA: McGraw-Hill Educ., 2011.

[59] M. Tariq, A. Al-Dweik, B. Mohammad, H. Saleh, and T. Stouraitis, “Computational power evaluation for energy-constrained wireless communications systems,” *IEEE Open J. Commun. Soc.*, vol. 1, pp. 308–319, 2020.

[60] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, *A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications*. McLean, VA, USA: Booz-Allen Hamilton Inc., 2001.

TASNEEM ASSAF (Member, IEEE) received the B.Sc. degree in communications engineering from Khalifa University (KU), UAE, in 2014, the master's degree in electrical engineering from the American University of Sharjah, UAE, in 2016, and the Ph.D. degree in electrical engineering from KU in 2021. Her research focuses on smart grids, optimization, wireless communications, and physical-layer security.

ARAFAT AL-DWEIK (Senior Member, IEEE) received the M.S. degree (*summa cum laude*) and the Ph.D. degree (*magna cum laude*) in electrical engineering from Cleveland State University, Cleveland, OH, USA.

He served with Efficient Channel Coding, Inc., Cleveland; the Department of Information Technology, Arab American University, Palestine; and the University of Guelph, ON, Canada. Since 2003, he has been with the Department of Electrical Engineering, Khalifa University, UAE. He is currently an Adjunct Research Professor with Western University, the University of Guelph, and the University of Manchester, U.K. He is a recipient of the Fulbright Scholarship, the Hijjawi Award for Applied Sciences, the Fulbright Alumni Development Grant, the Dubai Award for Sustainable Transportation, and the Leader–Founder Award in UAE. He serves as an Editor for the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY and *IET Communications*. He is a registered Professional Engineer in the Province of Ontario, Canada.

YOUSSEF IRAQI (Senior Member, IEEE) received the M.Sc. and Ph.D. degrees in computer science from the University of Montreal, Canada, in 2000 and 2003, respectively. He is currently an Associate Professor with the School of Computer Science, Mohammed VI Polytechnic University, Morocco. Before that, he was with the Department of Electrical Engineering and Computer Science, Khalifa University (KU), UAE, for 12 years. Before joining KU, he was the Chair of the Department of Computer Science, Dhofar University, Oman, for four years. From 2004 to 2005, he was a Research Assistant Professor with the David R. Cheriton School of Computer Science, University of Waterloo, Canada. He has published more than 130 research papers in international journals and refereed conference proceedings. His research interests include resource management in wireless networks, blockchain, trust and reputation management, cloud computing, and stylometry. In 2008, he received the IEEE Communications Society Fred W. Ellersick Paper Award in the field of communications systems. He is on many technical program committees of international conferences and is always approached for his expertise by international journals in his field.

SOBIA JANGSHER (Member, IEEE) received the B.E. degree in electronics engineering and the M.S. degree in communication system engineering from the National University of Science and Technology, Pakistan, and the Ph.D. degree in wireless communication from The University of Hong Kong, Hong Kong. From November 2015 to January 2021, she was working as an Assistant Professor with the Institute of Space Technology, Islamabad, Pakistan. She is currently associated with the Department of Electrical Engineering and Computer Science, Khalifa University, Abu Dhabi, UAE. Her research mainly focuses on optimization/resource allocation for IRS systems, multiple access schemes, and small cell networks.

ANSHUL PANDEY (Member, IEEE) received the B.Tech. degree in electronics and communication engineering from the Indian Institute of Information Technology Design and Manufacturing, Jabalpur, India, in 2012, the M.Tech. degree in advance networks from the Indian Institute of Information Technology and Management, Gwalior, India, in 2016, and the Ph.D. degree from the Department of Electronics and Communication Engineering, Indian Institute of Information Technology Allahabad, India, in 2021. He is currently working as a Senior Researcher with the Secure Systems Research Center, Technology Innovation Institute, Abu Dhabi, UAE. His research interests include cooperative relaying for wireless vehicular networks, physical-layer security, reconfigurable intelligent surfaces, and signal processing.

JEAN-PIERRE GIACALONE (Member, IEEE) received the engineering degree from the École nationale supérieure d'électrotechnique, d'électronique, d'informatique, d'hydraulique et des télécommunications, Toulouse, France. He is the Vice President of Secure Communications Engineering, Secure Systems Research Centre, Technology Innovation Institute, Abu Dhabi, UAE. He is responsible for researching secure communications, focusing on improving the resilience of cyber–physical and autonomous systems. He has worked as an Expert in software architecture for advanced driving assistance systems with Renault and as a Principal Engineer and an Architect with Intel's Mobile Systems Technologies Group. He holds 19 patents and has coauthored 15 research papers accepted for publication in international journals and conference proceedings.

ENAS E. ABULIBDEH (Member, IEEE) received the B.Sc. and M.Sc. degrees in computer engineering from Jordan University of Science and Technology in 2013 and 2016, respectively. She is currently pursuing the Ph.D. degree with the Electrical and Computer Engineering Department, Khalifa University. Her research interests include physical unclonable function and its application for hardware security.

HANI SALEH (Senior Member, IEEE) received the Bachelor of Science degree in electrical engineering from the University of Jordan, the Master of Science degree in electrical engineering from the University of Texas at San Antonio, and the Ph.D. degree in computer engineering from the University of Texas at Austin.

In 2012, he joined Khalifa University as an Assistant Professor, where he has been an Associate Professor of Electronic Engineering since 2017. He was the Co-Founder of the Khalifa University Research Center from 2012 to 2018. He has also been the Co-Founder and a Theme-Lead with the System on Chip Research Center, Khalifa University, since 2019, where he led multiple IoT projects for the development of wearable blood glucose monitoring SOC, mobile surveillance SOC, and AI accelerators for edge devices. He has a total of 19 years of industrial experience in ASIC chip design, microprocessor/microcontroller design, DSP core design, graphics core design, and embedded systems design. Prior joining Khalifa University, he worked for many leading semiconductor design companies, including Apple Incorporation, Intel (ATOM mobile microprocessor design), AMD (Bobcat mobile microprocessor design), Qualcomm (QDSP DSP core design for mobile SOC's), Synopsys (designed the I2C DW IP included in Synopys DesignWare library), Fujitsu (SPARC compatible high performance microprocessor design), and Motorola Australia.

BAKER MOHAMMAD (Senior Member, IEEE) received the B.S. degree in ECE from the University of New Mexico, Albuquerque, the M.S. degree in ECE from Arizona State University, Tempe, and the Ph.D. degree in ECE from the University of Texas at Austin in 2008. He is the Director of the System on Chip Center and a Professor of EECS with Khalifa University. He is a member of Mohammed bin Rashid Academy of Scientists. Prior joining Khalifa University, he was a Senior Staff Engineer/Manager with Qualcomm, Austin, TX, USA, for six years, where he was engaged in designing high performance and low-power DSP processors used for communication and multimedia application. Before joining Qualcomm, he worked for 10 years with Intel Corporation on a wide range of microprocessors design from high performance, server chips > 100Watt (IA-64), to mobile embedded processor low power sub 1 watt (xscale). He has over 16 years of industrial experience in microprocessor design, emphasizing memory, low power circuit, and physical design. His research interests include VLSI, power-efficient computing, embedded memory and in-memory computing, nueromorphic computing, emerging technology, such as memristor, STTRAM, hardware accelerators for cyber–physical system and AI. He is also engaged in a microwatt range computing platform for wearable electronics and WSN focusing on energy harvesting, power management, and power conversion, including efficient dc/dc and ac/dc converters. He has authored/coauthored over 100 referred journals and over 100 conference proceedings, more than four books, more than 20 U.S. patents, multiple invited seminars/panelists, and the presenter of more than four conference tutorials, including one tutorial on energy harvesting and power management for WSN at the 2015 (ISCAS). He has received several awards, including the KUSTAR Staff Excellence Award in intellectual property creation, IEEE Transactions on Very Large Scale Integration (VLSI) Systems Best Paper Award, the 2016 IEEE MWSCAS Myrill B. Reed Best Paper Award, the Qualcomm Qstar Award for excellence on performance and leadership, the SRC Techon Best Session Papers for 2016 and 2017, the 2009 Best Paper Award for Qualcomm Qtech Conference, and Intel Involve in the Community Award for volunteer and impact on the community. He participates in many technical committees at IEEE conferences and reviews for IEEE Transactions on Very Large Scale Integration (VLSI) Systems, IEEE Circuits and Systems journals. He serves as an advisory board for Technology Innovation Institute secure system and is an Associate Editor for IEEE Access, IEEE Transactions on Very Large Scale Integration (VLSI) Systems, and *Scientific Reports* journals.