IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received January 10, 2022, accepted January 24, 2022, date of publication January 27, 2022, date of current version February 10, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3147201

Authenticated Encryption Schemes: A Systematic Review

MOHAMUD AHMED JIMALE[1], MUHAMMAD REZA Z'ABA[1], MISS LAIHA BINTI MAT KIAH[1], (Senior Member, IEEE), MOHD YAMANI IDNA IDRIS[1], (Member, IEEE), NORZIANA JAMIL[2], MOESFA SOEHEILA MOHAMAD[3], AND MOHD SAUFY ROHMAD[4]

[1]Department of Computer System and Technology, Faculty of Computer Science and Information Technology, Universiti Malaya, Kuala Lumpur 50603, Malaysia
[2]College of Computing and Informatics, Universiti Tenaga Nasional, Kajang, Selangor 43000, Malaysia
[3]Information Security Laboratory, MIMOS Berhad, Kuala Lumpur 57000, Malaysia
[4]Faculty of Electrical Engineering, Universiti Teknologi MARA, Shah Alam, Selangor 40450, Malaysia

Corresponding author: Muhammad Reza Z'aba (reza.zaba@um.edu.my)

This work was supported by the Fundamental Research Grant Scheme (FRGS) of the Ministry of Higher Education, Malaysia, Project Number FP072-2019A, Reference Code FRGS/1/2019/ICT05/UM/02/1.

ABSTRACT Authenticated encryption (AE) is a cryptographic construction that simultaneously protects confidentiality and integrity. A considerable amount of research has been devoted to the area since its formal inception in 2000. Different lines of research have been proposed to enhance the available schemes in terms of security, efficiency, and design and to implement new ideas. However, a comprehensive systematic literature review (SLR) of the topic has not been provided to the best of the authors' knowledge. This study fills this gap in the literature by proposing a framework for classifying AE schemes and highlighting past contributions to help researchers familiarize themselves with the current state and directions for future research in the area. This SLR covered AE schemes proposed from 2000 to 2020. A total of 217 articles, selected from eight sources, were categorized into independent schemes, CAESAR competition schemes, and NIST lightweight competition schemes. These schemes were then classified according to their design approaches, security-related properties, and functional features. Our analysis reveals that a significant outstanding challenge in AE is to balance security, efficiency, and the provision of desirable features.

INDEX TERMS Authenticated encryption, CAESAR competition, confidentiality, integrity, message authentication code, NIST-LW competition.

I. INTRODUCTION

A. BACKGROUND

Encryption primitives used in block and stream ciphers guarantee only the confidentiality of the messages, i.e., unauthorized entities cannot view the messages. Such primitives cannot be naively used in secure communication because it is trivial for an adversary to tamper with the encrypted message (i.e., ciphertext) without being detected. This problem can be resolved by using authenticated encryption (AE) schemes. In addition to confidentiality, an AE scheme ensures the integrity and authenticity of the transmitted message. An extension of AE, called AE with associated data (AEAD), ensures the authentication of additional data without encrypting them [1]–[4]. A typical example is a network packet header, where only the payload should be encrypted, but both the header and the encrypted payload must be authenticated.

AE schemes are widely used in IPsec and Transport Layer Security (TLS). The latest version of TLS, i.e., 1.3, has eliminated its support for non-AE schemes such as the AES in cipher block chaining (CBC) mode as of August 2018 [5]. Such schemes are also used to provide end-to-end encryption in popular messaging applications, such as WhatsApp, Telegram, and Signal.

There are three conventional approaches to constructing an AE scheme, also called generic composition [6]: the encrypt-then-authenticate (EtA), encrypt-and-authenticate (E&A), and authenticate-then-encrypt (AtE) schemes. They differ in the sequence of operations and the stage they are performed. For example, EtA encrypts the message and then applies the Message Authentication Code (MAC) to the ciphertext. E&A separately encrypts each message and applies the MAC

The associate editor coordinating the review of this manuscript and approving it for publication was Chien-Ming Chen.

to it, whereas AtE applies the MAC to the message and encrypts it once it has been concatenated with the MAC tag. Bellare and Namprempre reported in 2000 that most previous approaches to the problem were weak when analyzed under several notions of security [6], [7]. Various subsequent attacks highlighted the shortcomings of the generic composition approach [8]–[12]. Although EtA has been shown to be provably secure [7], [13], it can still be attacked by exploiting the details of its implementation [7].

Owing to the delicacy of independently combining encryption and the MAC for secure construction, a single primitive that provides both confidentiality and authenticity was highly sought after. Hence, dedicated authenticated encryption (AE) schemes were developed to solve this onerous problem efficiently. Although the idea was mulled over much earlier, in 1987, by Jansen and Boekee [14], the first practical design was developed at the turn of the 21st century by Katz and Yung [15], followed swiftly by proposals by other researchers [16]–[18]. The new breed of dedicated AE schemes uses a single key, in contrast to traditional approaches that necessitate the use of two separate keys—one for encryption and the other for authentication—to differentiate their purposes [19].

To foster compatibility, six AE schemes were standardized in 2009 as ISO/IEC 19772: OCB 2.0 [20], Key Wrap [4], CCM [4], [21], EAX [22], EtM, and GCM [23]. OCB 2.0 was later removed from the 2020 edition of the ISO/IEC 19772 standard due to the security flaw discovered by Inoue *et al.* [24]. However, researchers still believed that AE schemes could be improved, and that paved the way for the Competition for Authenticated Encryption: Security, Applicability, and Robustness (CAESAR) project, which was jointly initiated in 2013 by the US National Institute of Standards and Technology (NIST) and Dan Bernstein. The final CAESAR portfolio was announced in 2018 and contained six schemes [25]–[30]. In the same year, due to the rise of the Internet of Things (IoT), which consists mainly of resource-constrained devices, the NIST solicited a call to standardize lightweight AE schemes (hereinafter referred to as NIST-LW schemes). By lightweight, we mean here that the schemes should be suitable for implementation in devices where such resources as memory and power are scarce. On March 29, 2021, NIST announced 10 finalists from 32 candidates from Round 2 of the NIST-LW competition as the final portfolio for standardization.

Our work focuses on AE schemes in the symmetric key setting. AE schemes in the asymmetric (public) key setting are known as signcryption [31]. Signcryption predated the symmetric key for several years and was motivated by Nyberg and Rueppel [35] on a digital signature scheme, which was extended by other researchers [32]–[35]. Signcryption ensures the confidentiality, authenticity, and non-repudiation of the transmitted messages to prevent the communicating parties from denying the sent messages. Due to its dependence on computationally expensive mathematical operations, such as exponentiation and factorization, signcryption is not typically used for processing bulk data. Symmetric AE schemes are much more efficient than signcryption, thus, better suited to handle such tasks. Due to the different paradigms, our work focuses only on AE schemes in the symmetric key setting.

Past work has reviewed state of the art in AE. In 2016, Abed *et al.* [36] presented an extensive categorization of AE schemes proposed for the CAESAR competition schemes. Vizár [12] and Zhang *et al.* [108] conducted similar studies on the CAESAR competition schemes. In 2017, Kavun *et al.* [37] provided a hardware implementation benchmark for commonly used AE schemes that excluded a majority of schemes proposed in the CAESAR project. Thus, there is a need for a systematic literature review that explores the status of research in the area to inform researchers, readers, and industry experts of the feature set available in AE schemes for implementation or further research.

Despite the various reviews and studies in AE, we have not come across a comprehensive systematic literature review (SLR) of the area. This work fills this gap by presenting an SLR of 217 articles throughout 2000–2020 and identifying and categorizing relevant research in AE. Here, our work complements past work by refining the categorization and including additional reviews of AE schemes proposed in the NIST lightweight AE project and those beyond the CAESAR project. We propose a framework for classifying AE schemes and apply it to the winners of the CAESAR competition in 2019, as well as the NIST-LW finalists announced on March 29, 2021.

B. CONTRIBUTIONS

This section summarizes the contributions of this work:

- Classification of AE schemes into three categories. (1) Independent schemes (Category A) that are not part of the CAESAR or NIST lightweight AE (NIST-LW) projects. These schemes were prevalent before these projects. (2) Schemes that were part of the CAESAR competition (Category B), from when the first submissions were made in 2014 until 2019, when the final portfolio was announced. (3) Schemes that were part of the NIST-LW project (Category C), from its inception in 2019 until March 2021, when ten finalists were announced.
- Proposal of a framework for classifying AE schemes according to five parameters: line of work, building blocks, modes/designs, functional features, and security-related properties. The framework is shown in Figure 1.
- Applying our classification framework to the winners of the CAESAR competition and the recently announced NIST-LW AE finalists. We show the security-related properties and functional characteristics of these schemes.
- Acquainting readers with past contributions and helping researchers or industry experts become familiar with gaps in research.

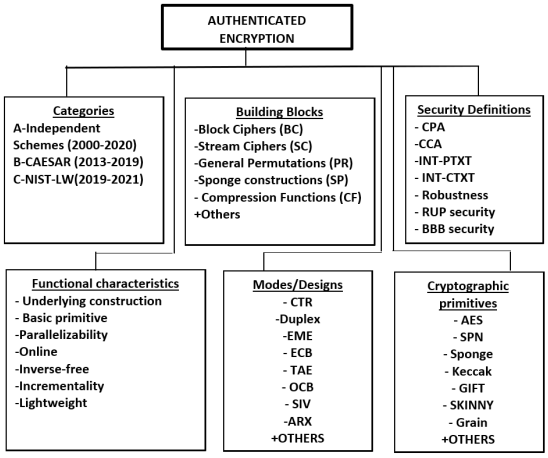

FIGURE 1. A general classification framework of AE schemes.

- Demonstration of the current state of AE schemes in terms of security, performance, and other functional features as well as gaps that need to be bridged.

C. ORGANIZATION OF THIS WORK

The remainder of this paper is organized as follows: Section II presents a general classification framework and provides an overview of AE and its essential features, security-related parameters, and functional properties. Section III explains the research methodology used in this study, and Section IV presents the results. Section V provides a discussion of the findings and possible future research in the area, and Section VI presents the conclusion of this work.

II. A GENERAL FRAMEWORK

This section provides an overview of the classification of authenticated encryption according to the framework shown in Figure 1.

A. AUTHENTICATED ENCRYPTION

Traditional encryption-only schemes ensure confidentiality and integrity/authenticity as separate services but were subsequently shown to fail to protect even confidentiality without ensuring integrity. This fact paved the way for the naissance of the notion of authenticated encryption (AE) [6], [15]. Encryption ensures the confidentiality of messages under a secret key. The sender encrypts a confidential plaintext message and transmits the ciphertext; the receiver decrypts it, returning the plaintext. The sender calculates a MAC and attaches it to the message for authentication. The receiver employs the same mechanism as the sender to make sure that the two codes match; if they do match, then he/she is assured that the message is authentic and accepts it; otherwise, a forgery is assumed, and the message is discarded.

Authenticated encryption simultaneously protects confidentiality and integrity under a secret key. In AE schemes, the decryption may return either the plaintext or a special symbol $\perp$ (bottom) instead of the plaintext, indicating an attempt of forgery. The authenticity of plaintext may also depend on unencrypted data (associated data, or the header), which is vital for routing packets such as TCP/IP information. Rogaway called this authenticated encryption with associated data (AEAD) in 2002 [38].

An authenticated encryption scheme has the following operations:

- **Encrypt and Authenticate**. Given a variable-length message, the associated variable-length data (optional), a fixed-length secret key, the ciphertext, and the corresponding fixed-length authentication tag are the output. Before encryption, the message and the associated data are equally concatenated to fixed-length blocks. If the last message and/or associated data block is shorter than a complete block, it is padded so that it is a complete block.
- **Decrypt and Verify.** Given the ciphertext, secret key, and authentication tag, the decrypted message is output if the tag is authentic; otherwise, an error message is produced.

For authenticated encryption with associated data (AEAD), the Encrypt and Authenticate operation receives an additional input, which consists of data that are authenticated but not encrypted. The message can be of arbitrary length, but the secret key and tag are fixed in size.

AEAD can be regarded as a function that receives four arguments—a secret key (K), a nonce (N), associated data (A), and plaintext (P)—as input, and a ciphertext (C) and an authentication tag (T) as an output—$E : K \times N \times H \times M \rightarrow C|T$—along with a decryption $D : K \times N \times H \times C \rightarrow M\{\perp\}$. Separated authenticated encryption with associated data also features a verification algorithm $V : K \times N \times H \times C \times T \rightarrow M\top, \perp$. The encryption algorithm is $E_K(N, H, M) = (C, T)$, and the decryption algorithm is $D_K(N, H, C) = M$ if (C,T) is valid; otherwise, it outputs $\perp$; the verification algorithm is $V_K(N, H, C, T) = \perp$ if a forgery is detected and decryption fails [17], [18], [21].

Although the intuitive method of designing an AE scheme is ''generic composition,'' which involves combing a secure encryption scheme with a secure MAC with two keys, it was subsequently proved that incorrect implementation could result in unsecured schemes. An example of an incorrect implementation is the PCBC mode in Kerberos, as shown by Rogaway *et al.* [18]. There are three ways to generally combine a MAC and an encryption scheme [6]:

- Encrypt-and-MAC-plaintext: This involves encrypting the plaintext first and then appending a tag (MAC) of the plaintext to the ciphertext. Given K_e, K_m, and M, we have E_{Ke}, $K_m(M) = E_{Ke}(M)||T_{km}(M)$, and the result is C||T. ''Decryption/verification'' is carried out by first decrypting the ciphertext to get the plain text and then recalculating the authentication tag for verification.
- MAC-then-encrypt: This involves generating an MAC on the plaintext then encrypting it together with the

plaintext: E_{Ke}, Km(M)= E_{Ke}(M||T_{km}(M)). ''Decryption/verification'' is then performed by decrypting the ciphertext to get the plaintext and the tag and verifying the tag.

- Encrypt-then-MAC: E_{Ke},Km(M)= C ||T_{Km} (C), where C = E_{Ke} (M) E_{Ke} and C = E_{Ke} (M). The plaintext is encrypted to produce a ciphertext C and appended a MAC of C to it. In ''Decryption+verification,'' the tag is verified first, then the ciphertext C is decrypted.

According to [6], only the third combination is assured to be secure if the encryption and MAC schemes are secure. Although this method is natural and easy to analyze, it is slow because it requires two separate keys, one for encryption and another for tag generations, and is not well-protected against implementation errors.

The alternative to generic composition is a dedicated AE scheme. Soon after 2000, AE schemes were proposed based on different structures, such as block cipher [16], stream cipher [39], compression functions [40], cryptographic sponges [41], and keyed permutations. Other dedicated schemes are not based on any underlying primitive but are considered primitives on their own [42]. Some of these schemes are two-pass schemes, which make two passes through the data: one for confidentiality and the other for integrity. They mimic generic composition but use a single key instead of two independent keys; an example is (CCM, GCM). Other AE schemes are single-pass schemes that run once through the data to achieve confidentiality and integrity simultaneously. Examples of single-pass schemes are XCBC and OCB [17], [18], [21], [22].

B. AE CATEGORIES

1) AUTHENTICATED ENCRYPTION BEYOND CAESAR AND NIST COMPETITIONS (INDEPENDENT SCHEMES)

AE schemes before the CAESAR competition, known as nonce-based authenticated encryption with associated data, were first defined in [6] and refined in [38]. They were designed to achieve semantic security by considering only deterministic schemes. The notation required the uniqueness of the nonce and stated that security was void if this condition was not fulfilled. Another important aspect of this notion is the associated data (AD)—pieces of data that should not be encrypted, so that routing devices can forward packets correctly, but need to be authenticated. In this review schemes that are not part of the CAESAR or NIST lightweight competitions are referred to as ''independent schemes.''

According to [43], although it might be theoretically easy to implement nonce uniqueness, it isn't easy in practice. In many situations, implementation errors lead to the misuse of nonces and the complete loss of confidentiality. For this reason, Rogaway and Shrimpton in 2006 proposed better security (robustness) for cases in which nonces are misused. This was the emergence of the notion of misuse-resistant authenticated encryption schemes [44].

The continual refinement of AE schemes and the introduction of several enhancements to the original definitions and notions have led to the realization that important features of AE schemes can be enhanced. This idea paved the way for the Competition for Authenticated Encryption: Security, Applicability and Robustness (CAESAR), which was jointly initiated by NIST and Bernstein [45], [46].

2) AE SCHEMES IN CAESAR COMPETITION

Despite the availability of various AE schemes that emphasize different aspects of confidentiality and integrity, many outstanding problems lead to a loss or weakening of security, whereas others affect efficiency. The need to enhance AE schemes led to the idea of the CAESAR competition in 2013 [45]. The question raised was: ''Can we come up with schemes that are as secure as AES-GCM and more efficient or ones that are as efficient but more secure, such that they can be widely adopted?'' The organizing committee had received 56 submissions by 2014. After three rounds, the competition was concluded in 2019 with six winners from three use cases: lightweight applications for constrained devices [26], [30], high-performance applications [28], [29], and defense in depth [25], [27]. The winners were Ascon [26], ACORN [30], OCB (v1.1) [28], AEGIS [29], COLM, and Deoxys [27].

3) AE SCHEMES IN NIST COMPETITION

With the experience of the CAESAR competition, researchers focused on AE applications in resource-constrained devices that could not benefit from the most prevalent schemes due to their resource intensiveness. This led to the idea of setting for another competition in lightweight cryptography.

NIST, in August 2019, published the requirements and evaluation criteria for the submission of lightweight algorithms for evaluation and standardization. By February 2019, 57 submissions had been received; after eliminating one submission, the organizers officially considered 56 submissions as candidates in round 1 [47]. After eliminating 24 candidates, including the proposals in [48]–[50], 32 candidates were announced in April 2019 as round-2 candidates [47]. In March, 2021, NIST announced 10 finalists from the 32 candidates from round 2 in the final portfolio for standardization: Ascon [51], Elephant [52], GIFT-COFB [53], Grain128-AEAD [54], ISAP [55], Photon-Beetle [56], Romulus [57], Sparkle [58], TinyJambu [59], and Xoodyak [60]

C. BUILDING BLOCKS

This section provides an overview of cryptographic structures used to build AE schemes.

1) BLOCK CIPHER-BASED STRUCTURE

A block cipher accepts a plaintext block of fixed length and a secret key as input. A key scheduling algorithm takes the secret key and derives a series of round subkeys. The input plaintext is processed iteratively by a round function where

one of the subkeys is applied. The final round outputs the corresponding ciphertext block that is equal in length to the input plaintext block. Typical block lengths are 64 and 128 bits, while the secret key ranges from 128 to 256 bits. An AE scheme includes either a dedicated block cipher specific to the scheme or uses readily available designs (often with some modifications). Popular block ciphers that are used to construct AE schemes include the AES [61], SKINNY [62], and GIFT [63].

An extension to the traditional block cipher called tweakable block cipher additionally accepts a public input value called a tweak. The tweak allows for an easy way to invoke a different permutation of the block cipher without changing the key, somewhat akin to a counter that is baked inside the block cipher itself. The idea of a tweakable block cipher dates back to the hasty pudding cipher, a candidate in the AES competition [35]. The tweakable block cipher was later formalized by Liskov *et al.* [36], [37]. At the time of writing, the tweakable block cipher SKINNY [38] is being included in a new standard called the ISO/IEC18033-7 [39].

2) STREAM CIPHER-BASED STRUCTURE

Stream ciphers encrypt messages bit by bit, adding a bit from a keystream to a plaintext bit and taking a secret key of a fixed length to generate a keystream of variable length. Stream ciphers are designed to be small and fast and are often suited for constrained resource environments that need lightweight algorithms. In addition, stream ciphers can be used as core primitives in authenticated encryption to protect confidentiality and integrity if the cipher is secure [64].

3) PERMUTATION-BASED STRUCTURE

These schemes use dedicated and keyless permutations as underlying primitive. Schemes in this category do not use permutations in a sponge-like mode but apply other techniques like XOR, Encrypt XOR, Encrypt Mix Encrypt (EME), and derivations of the Even-Mansour construction [65].

4) SPONGE-BASED STRUCTURE

The most commonly used form of keyless permutation is sponge construction. Certain schemes use keyless permutations in a sponge-like mode of operation, like the Keccak-f permutation used in the SHA3 hash function, whereas others rely on dedicated permutations. The sponge construction operates on a state of b bits at bitrate r bits and capacity c bits, where b = r+c. The sponge first absorbs its input data block by block before processing and squeezing them out afterward. Sponges can also be used for other cryptographic purposes like stream ciphers, re-seedable pseudorandom generators, and authenticated encryption [41].

5) HASH FUNCTION/COMPRESSION FUNCTION (CF)

Some AE schemes use compression functions from the SHA256 and SHA512 hash functions. A hash function maps strings of arbitrary length $\{0,1\}^*$ to a fixed-length output $\{0,1\}^n$ or hash value. Any change to even one bit of the input should produce an entirely different output and allow an adversary to find a collision, preimage, and second preimage [40].

6) OTHERS

Some AE schemes have a structure based on primitives that do not fall into the above categories, like the Type-3 Feistel schemes [66]. Other schemes are based on hybrid primitives (HB) with structures that have the characteristics of more than one cipher, like the stream cipher and the block cipher [67], [68]. Finally, dedicated schemes (DE) that are not based on any symmetric key primitive have also been developed, although there are few of them, such as those based on finite automata and algebraic methods [69], [70].

D. SECURITY-RELATED DEFINITIONS

Authenticated encryption is intended to protect confidentiality and integrity and is assumed secure only if it satisfies the relevant notions of security. This section provides a general description of the security relations, definitions, and assumptions about AE schemes. First, we discuss provable security and indistinguishability in our adversarial models. Then we consider general security notions relating to confidentiality and integrity following Rogaway and Shrimpton [44], Bellare and Namprempre [7], and Bellare *et al.* [71]. Finally, our discussion considers a security model where a computationally bounded adversary $\boldsymbol{A}$ interacts with a given set of oracle ($\boldsymbol{O}$), acting like a Blackbox to the adversary. For an AE scheme to be secure, **A**'s advantage in all cases should be negligible.

1) PROVABLE SECURITY

Provable security, also known as reductionist security, is a methodology designers use to assure that a scheme is secure relative to particular security definitions, against a given adversarial model, under specific assumptions. Cryptographers provide security proofs in a theoretical model that abstracts their underlying primitive such as PRF or PRP [72], primarily in the Standard Model or Radon Oracle Model. In the Standard Model, the adversary is limited by the amount of time and computer power it has. The Random Oracle Model assumes that Pseudorandom functions are replaced by random oracles that return random values upon invocation [73]. See figure 2 for details.

a: INDISTINGUISHABILITY OF CIPHERS (IND)

Computational indistinguishability is an essential concept in cryptography that requires that an adversary with defined capabilities and resources cannot distinguish between two ciphertexts, one encrypted with the cipher in question and another from an equal length random string. To formalize it, we resort to the concept of distributions $X = \{x_k\}_{k \subseteq N}$ One for each value of security parameter [74].

Definition 1: Two sets S_1 and S_2 are indistinguishable if for all adversaries A that outputs a bit: $|\Pr[A(X_1) = 1] - Pr[A(X_2) = 1]| \leq negl(k)$.

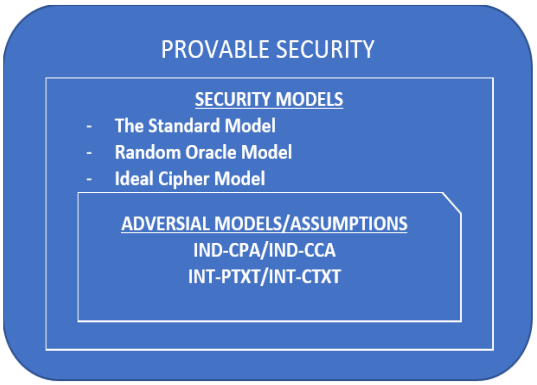

FIGURE 2. Security definitions model for AE schemes.

The definition guarantees that no efficient adversary can tell apart with non-negligible probability given a sample from X_1 or X_2, because the output is either 1 or 0 with equal probabilities.

b: PSEUDORANDOM FUNCTIONS

A pseudorandom function(PRF) is a deterministic function sampled uniformly at random from a finite function space that takes a Key K, an input x, and gives an output y that is indistinguishable from a truly random function. An adversary that can provide input and get an output to and from either a PRF or a truly random function cannot distinguish them with non-negligible probability. For some integers $k, l, L \geq 1$ of a function $F : K \times D \rightarrow R, (K = K, D = \{0,1\}^l, R = \{0,1\}^L)$. The function F_n can be in one of two worlds. In the real world, the adversary is interacting with a random instance of F, and in the random world, it is interacting with a random function F_n with the domain R. To succeed in the experiment, the job of the adversary is to distinguish between these two worlds with probability more than 1/2, with the advantage being a number between 0 and 1.

Definition 2 (Pseudorandom Functions): a Function $F{:}\{0,1\}^k \times \{0,1\}^l \rightarrow \{0,1\}^l, forl = l(k) = poly(k)$, is a pseudorandom function if for all PPT adversaries A,

$$|\Pr\left[A^{F_K(\cdot)}\left(1^k\right) = 1\right] - Pr[A^{f(\cdot)}\left(1^k\right) = 1]| \leq negl(k),$$

where $K \xleftarrow{\$} \{0,1\}^k$, and f is chosen at random from the set of functions from $\{0,1\}^l$ *to* $\{0,1\}^l$

c: PSEUDORANDOM PERMUTATIONS

A pseudorandom permutation (PRP) is a bijective PRF that adversary A cannot distinguish from a random permutation. A PRP is efficient if both the permutation and its inverse can be computed efficiently in a polynomial-time. We refer to a strong notion of security as Strong PRP when we mean a permutation that is indistinguishable even when the adversary has access to both the permutation (P) and it inverse (P^{-1}). [72], [74].

Definition 3 (A Strong Pseudorandom Permutation): A function $P{:}\{0,1\}^k \times \{0,1\}^l \rightarrow \{0,1\}^l$ *for* $l = l(k) = ply(k)$ is strong pseudorandom permutation if for all PPT adversary A,

$$|Pr[A^{P_K(\cdot),P_K^{-1}(\cdot)}(1^k) = 1] - Pr[A^{f(\cdot),f(\cdot)^{-1}}\left(1^k\right) = 1]| \leq negl(k),$$

where $K \xleftarrow{\$} \{0,1\}^k$ And f is chosen uniformly at random from the set of permutations over [75][1].

Following the approach of Abel *et al.* [36], we describe the advantage of adversary A against Chosen Plaintext Attack (CPA) and Chosen-Ciphertext-Attack (CCA).

Definition 4 (PRP-Advantage Under CPA): Let $F{:}K \times D \rightarrow D$ be a family of functions and A an adversary which interacts with an oracle and return a bit, the PRP-advantage of A is given by:

$$ADV_F^{PRP-CPA}(A) = |\Pr\left[Real_F^A \Rightarrow 1\right] - Pr[Perm_D^A \Rightarrow 1]|$$

Definition 5 (PRP-Advantage Under CCA): Let $F{:}K \times D \rightarrow D$ be a family of functions, and A be q, q, μ bounded adversary, where t is time complexity, q is the number of queries, and μ is the total length of all adversarial queries. It is worth noting that PRP-CCA secure scheme is also PRP-CPA secure, but the reverse is not true. The PRP-CCA advantage of A is given by:

$$ADV_F^{PRP-CCA}(A) = |\Pr\left[Real_F^A \Rightarrow 1\right] - Pr[Perm_D^A \Rightarrow 1]|$$

Definition 6 (IND-CPA and IND-CCA): Let $\Pi(K, E, D)$ be an authenticated encryption scheme, and A as a t,q,l bound adversary that can interact with the real world (Real) and the random world (Randon) with complexity time t, making q queries of total length l. in the IND-CPA case A can have access to an encryption oracle, and in the IND-CCA case it can also have a decryption oracle. The adversary's goal is to distinguish between the two worlds. In both cases, A's advantage, with reasonable resources, should be negligible.

$$ADV_\Pi^{IND-CPA}(A) = \Pr\left[K \xleftarrow{\$} K{:}(A)^{E(.,.)} \Rightarrow 1\right] - Pr[(A)^{\$(.,.)} \Rightarrow 1]$$

$$ADV_\Pi^{IND-CCA}(A) = \Pr\left[K \xleftarrow{\$} K{:}(A)^{E(.,.)} \Rightarrow 1\right] - Pr[(A)^{\$(.,.)} \Rightarrow 1]$$

Definition 7 (INT-PTXT and INT-CTXT)): Let $\Pi(K, E, D)$ be an authenticated encryption scheme, and $A_{int-ptxt}$ and $A_{int-ptxt}$ be t,q,l bound adversaries that have access to Encryption oracle $E_k(.,.)$ and Decryption oracle $D_K(.,.)$. Adversary $A_{int-ptxt}$ wins if it submits to the decryption oracle a ciphertext that does not match a plaintext previously queried to the encryption oracle. $A_{int-ctxt}$ wins if it submits a valid ciphertext not previously produced by the encryption oracle to the encryption oracle. The scheme Π is considered secure if the advantage of $A_{int-ptxt}$ and $A_{int-ctxt}$ is negligible.

$$ADV_\Pi^{int-ptxt}(A) \leq Pr[K \xleftarrow{\$} K{:}(A)^{E(.,.),D(.,.)} \Rightarrow Forges$$

$$ADV_{\Pi}^{int-ctxt}(A) \leq Pr[K \xleftarrow{\$} K{:}(A)^{E(.,.),D(.,.)} \Rightarrow Forges$$

Shrimpton [76] introduced a variation of the standards Chosen Ciphertext security combining IND-CPA and IND-CTXT into a single notion known as IND-CCA3.

Definition 8 (IND-CCA3): Let Π=(K, E, D) be an authenticated encryption scheme, and A a t,q,l bound adversary that has access to encryption in the real world, but in decryption oracle in the random world, we replace the decryption oracle in the random world with an oracle that always returns INVALID ($\perp$). We assume that A never asks queries that it already knows the answer.

$$ADV_{\Pi}^{ind-CCA3}(A) = \Pr\left[K \xleftarrow{\$} K{:}A^{E_K(\cdot),D_K} \Rightarrow 1\right] - Pr[A^{E_K(\$|\cdot|),\perp} \Rightarrow 1]$$

Shrimpton [76] demonstrated that IND-CCA3 advantage of an adversary A on an AE is upper-bounded by the total of the maximal of A's advantage over Π INT-CTXT advantage and the maximal of A's advantage over Π IND-CPA advantage. So, the IND-CCA3 advantage over all adversaries A that run in time t and make q queries of length l, is given by:

$$ADV_{\Pi}^{CCA3}(q,t,l) \leq ADV_{\Pi}^{IND-CPA}(q,t,l) + ADV_{\Pi}^{INT-CTXT}(q,t,l)$$

d: SECURITY OF ONLINE AE SCHEMES

Bellare *et al.* [71] introduced the study of online ciphers, which can take input of large size plaintext and varying lengths and output the jth block of the ciphertext after having processed only the first j blocks of the plaintext, and they provided security definitions for them. So we define CCA3 security for the online AE schemes (OCCA3) following the approach of Abed *et al.* [36].

Definition 9 (OCCA3 Security): Let $\Pi = (K, E, D)$ be an online AE scheme and let $P \xleftarrow{\$} Operm_n$ be a random online permutation, then define an adversary A such that:

$$ADV_{\Pi}^{OCCA3}(A) = \Pr\left[\left[K \xleftarrow{\$} K{:}A^{E_K(\cdot),D_K} \Rightarrow 1\right] - \Pr\left[A^{O^P(.,.)\perp(.,.,.)} \Rightarrow 1\right]\right]$$

And $ADV_{\Pi}^{OCCA3}(q,t,l) = max_A ADV_{\Pi}^{OCCA3}(A)\}$, the maximum advantage over all OCCA3 q,t,l bounded adversaries, that as q number of queries of l blocks long with time complexity of t. Based on the definitions above and those in [36], [71], and [76], we can claim that that: $ADV_{\Pi}^{OCCA3}(A) \leq ADV_{\Pi}^{OPRP-CPA}(q,t,l) + ADV_{\Pi}^{INT-CTXT}(q,t,l)$

Definition 10 (OPRP-CCA Security): Let K be a k bit key, P a random permutation, $\psi{:}\{0,1\}^k \times (\{0,1\}^n)^* \rightarrow (\{0,1\}^n)^*$ be an online cipher. OPRP-CCA advantage of an adversary A can be defined as follows:

$$ADV_{\psi}^{OPRP-CCA}(A) = \left|\Pr\left[A^{\psi_K(\cdot),\psi_K^{-P}(\cdot)} \Rightarrow 1\right] - \Pr\left[A^{P(\cdot),A^{-P}(\cdot)} \Rightarrow 1\right]\right|$$

Then we can define $ADV_{\psi}^{OPRP-CCA}(q,t,l)$ as the maximum advantage over all OPRP-CCA adversaries making q number of queries of length l with a time of complexity of t.

e: PROTECTION AGAINST SIDE-CHANNEL ATTACKS

Apart from analyzing an AE scheme under security models mentioned in previous sections, attacks exist where the adversary does take advantage of weaknesses in the cryptographic algorithms but takes advantage of sideline information from its implementation instead. Such attacks, known as Side-Channel Attacks(SCA), are particularly dangerous when chips with sensitive information are in the hands of an adversary or are deployed where they are accessible to the general public, like IoT devices, sensor network nodes, and smarts cards [77], [78]. AE schemes use several techniques to prevent side-channel attacks include hiding [79] and masking [78], [80], [81] and re-keying [78], [82], [83], in which we do not use the target cipher only but also a session generation function that uses the master key as input on top of it.

f: NONCE-BASED AUTHENTICATED ENCRYPTION

An AE scheme may rely on a user-supplied nonce (number used once) to avoid predictability, an input to the AE scheme that is not supposed to be reused to encrypt different plaintexts under the same key [18], [38]. Why do we require that nonces be unique? Imagine that Bob receives an encrypted document sent by Alice. If Alice wishes to send the same document again to Bob, the encrypted document is the same as the first one if the same nonce is reused. If an adversary is tapping the communication, he/she can infer that the two documents are the same. Such knowledge is beneficial for an adversary and can be exploited in an attack.

Nonces do not need to be random; they just need to be different for each subsequent use. Examples include a counter that is increased with every new encryption. As nonce-based Authenticated Encryption (NAE) schemes do not handle nonce generation, implementors must ensure that the nonces are correctly used [84].

g: NONCE MISUSE-RESISTANT AE (MRAE)

Application developers are responsible for determining how nonces are generated. Such practice is prone to misuse because reusing nonces (intentionally or otherwise) can have dire consequences. Various protocols and applications have been violated due to the mishandling of nonces. Examples include Wired Equivalent Privacy (WEP) [85], WinZip [86], Microsoft Office [87], and Wi-Fi-protected access (WPA) 2 [88]. Therefore, it is desirable to have AE schemes that provide a reasonable level of protection in case of such misuse. To address this concern, in 2006, Rogaway and Shrimpton [44] proposed the notion of a nonce misuse-resistant AE (MRAE). An MRAE scheme ensures an acceptable level of security even though nonces are repeated [44].

h: RELEASE OF UNVERIFIED PLAINTEXT (RUP)

When performing decryption, a typical AEAD scheme should not release the resulting plaintext before the verification process; otherwise, the application must allocate memory to store unverified plaintexts, which may not be tolerable in resource-constrained environments. In essence, an AEAD scheme is secure under the RUP if the released information does not help an adversary forge valid ciphertexts or decrypt valid messages [89]–[91].

i: SECURITY BEYOND BIRTH BOUND (BBB)

Most AE schemes provide security up to the birthday bound, which is $O(\frac{\sigma^2}{2^n})$, where σ is the length of the ciphertext block and n is the block length. However, birthday bound security is not always adequate in cases where security beyond the birthday bound is required [92].

E. FUNCTIONAL FEATURES

In addition to security-related properties, other essential features according to which AE schemes can be classified and grouped include the following:

Underlying structure: It is the type of basic symmetric encryption algorithm used by the scheme (block cipher, stream cipher, permutation, dedicated) [18], [40], [65], [93].

Mode/design: The mode of encryption or the design philosophy according to which the scheme is implemented.

Cryptographic primitive: It is the basic primitive that the scheme uses to achieve confidentiality.

Parallelizability: The encryption of an AE scheme is parallelizable if the encryption of a block does not depend on the encryption or computation of any other block. The same definition can be provided for decryption. It reflects the ability of a scheme to process the i^{-th} block independently of the j^{-th} block [94].

Online: An encryption scheme can be categorized as either online or offline [71]. In essence, an online encryption scheme permits the computation of the i^{-th} ciphertext block after having seen the first i plaintext blocks. In other words, to encrypt the i^{-th} ciphertext block, we do not need to know any plaintext beyond this block. In the case of AE [95]–[98], if the message is viewed as the concatenation of several message blocks, it allows each block to be individually authenticated by producing a tag (i.e., intermediate tag [99]) for each block. On the contrary, an offline scheme outputs only the tag until all message blocks have been processed. An advantage of an online scheme is that the recipient can perform ciphertext block decryption and authentication on the fly at the receiving end.

Inverse free: An AE scheme is inverse free if the underlying primitives do not require their inverses to perform encryption or decryption. This is economical for implementation as the same code and circuit can be used for different purposes. An AE scheme incur additional implementation costs if inverses are needed. [26], [27].

Incrementality is the ability to update parts affected only by the last action, given a previous ciphertext–tag pair (C, T) [100]. An AE scheme provides incrementality if, given a previously computed ciphertext and a tag for a given plaintext M, encrypting another plaintext M' that differs only slightly from M is significantly faster than encrypting M' from scratch. Imagine a document that is frequently and continually updated, where the changes between edits may not be substantial, such as a set of appointment letters that are very similar in content, but differ in the name of the recipient. The concept of incremental cryptography applied to encryption has been investigated by Bellare *et al.* [101] in 1995. However, the idea of incremental cryptography itself was first applied by them to hash functions and digital signatures [102].

Single-pass: A critical indicator of the efficiency of AE schemes is the number of times the scheme processes the text for confidentiality and integrity. Two common ways are used: processing the plaintext once with one call to the underlying primitive to provide confidentiality together with integrity and processing the data more than once to provide confidentiality and integrity with separate calls to the underlying primitive. Being single pass renders a scheme more efficient [103], [104]

Lightweight: This determines whether the scheme is suitable for resource-constrained devices [91], [105]. Beyond the NIST-LW competition, dedicated to lightweight AE schemes, other schemes are not part of NIST-LW competition that demonstrate lightweight property, including but not limited to schemes in [68], [106]

F. DESIGN/MODES

Encryption modes/designs are algorithms that use an underlying primitive to provide confidentiality and authenticity. Several modes and design-specific constructions for symmetric key-authenticated encryption schemes use different underlying cryptographic primitives. Examples of designs/modes for AE schemes include CTR, Duplex, EME, ECB, TAE, OCB, SIV, and ARX. See Table 3 and Appendix for more examples of modes/designs [36], [107].

G. CRYPTOGRAPHIC PRIMITIVES

Cryptographic primitives are algorithms used to build cryptographic protocols for secure communications. They include encryption and MAC algorithms. Frequently used cryptographic primitives include AES, SPN, Sponge, TBC, Keccak, GIFT, SKINNY, and Grain. See Table 4 and Appendix for more examples of primitives [36], [107], [108].

III. METHODS AND MATERIALS

A. PLANNING THE SYSTEMATIC LITERATURE REVIEW

Our plan starts with the justification for conducting a systematic literature review of AE schemes in symmetric key setting, followed by the research questions considered and the review protocol used.

1) THE NEED FOR A REVIEW

The authors have not come across a comprehensive systematic review of AE schemes in the literature. Thus, it is important to conduct such a review to gather a catalog of AE techniques proposed in the literature and find ways to compare and categorize them in different contexts.

2) RESEARCH QUESTIONS

This SLR seeks to answer the following research questions:

- What is the current status of AE schemes?
- What criteria are available to compare and categorize AE schemes?
- What are outstanding research issues and future directions of research in AE?

B. REVIEW PROTOCOLS

This section describes the rationale and the methods of our systematic review while explaining the sources of data, search terms, and inclusion and exclusion criteria.

1) SEARCH DATABASES (SOURCES)

- IEEE Explore
- ACM
- ScienceDirect
- SpringerLink
- Cryptology ePrint Archive
- CAESAR competition website
- NIST-LW AE website
- Other Sources (Snowballing)

2) SEARCH TERMS

- Authenticated encryption
- Authenticated ciphers
- Authenticated encryption OR Authenticated ciphers
- AuthenticatedEncryption OR Authenticated-Encryption
- Authenticated Encryption with Associated Data
- AEAD

3) INCLUSION CRITERIA

- Journal or conference paper
- Authenticated encryption scheme
- from 2000 to 2020
- Full text available
- English language

4) EXCLUSION CRITERIA

- Language other than English
- Review papers, posters
- Abstract-only articles

C. CONDUCTING THE REVIEW

This section provides the details of the search strategy and steps of the data extraction process.

TABLE 1. AE schemes extracted from the selected sources.

Source	No. Articles	Remarks
Cryptology ePrint Archive	158	"Authenticated Encryption" Or "Authenticated Ciphers," journal and conference papers only from 2000 to 2020, "AEAD," "Authenticated Encryption With Associated Data," "Authenticatedencryption," "Authenticated-Encryption," "CAESAR," "Competition."
Ieee Explorer	138	
Acm Digital Library	22	
ScienceDirect	22	
Springerlink	171	
Caesar Competition website	56	Included all rounds and the winners
Nist Light Weight AE Competition	57	Including rounds 1 and 2
Other Sources	2	Snowballing
Total Number of Articles	626	

1) SEARCH STRATEGY

The systematic review was conducted using several databases and sources, including IEEE Explore, ACM, ScienceDirect, SpringerLink, Cryptology ePrint Archive, and the official websites of the CEASAR and NIST-LW competitions.

The search terms used were "Authenticated Encryption" or "Authenticated Ciphers," "AuthenticatedEncryption," "Authenticated Encryption with Associated Data," "AEAD," and "CAESAR" and "competition." Two articles were discovered by using snowballing search. The inclusion criteria were an English-language journal or conference paper published from 2000 to 2020, with the full text available. The exclusion criteria were a language other than English, a review paper, a poster, an article with an unclear methodology, and an abstract-only article.

A total of 626 articles (see Table 1) were returned. After removing 79 duplicates, 77 reviews, 22 articles with out-of-context titles, eight abstract-only articles, and 11 articles for which the full text was not available, 425 articles remained in the list. After an in-depth review, 208 articles were further removed to obtain 217 articles for the final review. The process is shown in the Prisma chart in Figure 3.

2) DATA EXTRACTION

After preparing the data extraction table, the authors abstracted the following elements from each article that fulfilled the inclusion criteria: scheme, building blocks, mode/design, encryption primitive, parallelizability, online, being inverse free, incrementality, being single-pass, nonce misuse resistance, being lightweight, providing BBB security, and providing security under RUP. The final eligibility

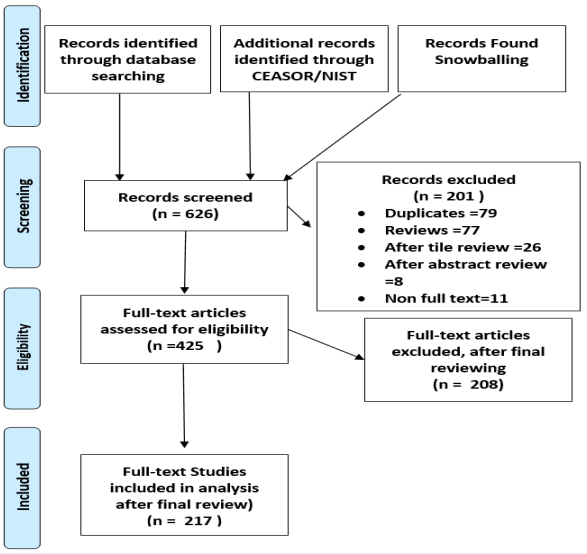

FIGURE 3. Flowchart of literature search.

of all articles was assessed. Table 1 shows the number of schemes extracted from each source.

IV. RESULTS

This section describes the articles selected and provides quantitative analyses of the results of our review.

A. SEARCH OUTCOMES

The 217 articles finally obtained for the systematic review had been published from 2000 to 2020 and were categorized into three groups. Category A consisted of schemes that were not part of the CAESAR or the NIST competition (independent schemes). Such schemes have been developed since 2000 and have continued during and after the CAESAR and NIST competitions. There were 104 schemes in this category [6], [7], [13], [15]–[18], [21]–[23], [38], [39], [41]–[45], [47], [64], [65], [68]–[70], [78], [84], [91]–[93], [95], [100], [103]–[106], [109]–[185] (2). Category B contained schemes that were part of the CAESAR competition, beginning in 2014, and had continued until the winners were declared in 2019. There were 56 schemes in this category [25]–[30], [66], [67], [97], [98], [186]–[192], [193]–[205], [206]–[230] (3). Category C contained schemes that were part of the NIST Lightweight AE Competition; they started appearing in 2019, and the finalists were announced in March 2021. There were 57 schemes in this category [3], [48]–[50], [231]–[282]. See the table in Appendix for details of the classification. The trends of the three categories are shown in Figure 4.

The upsurges in 2013–2019 and the decrease in 2020 in the chart in Figure 4 indicate the impact of the CAESAR and NIST competitions on the development of AE schemes, as well as the proliferation of desirable properties in them from 2014 to 2019. It is also worth noting that Category B (CAESAR competition) schemes appeared in 2014, 2016 and 2017. The reason is that some schemes submitted to CAESAR in 2014 were updated throughout the competition and thus, reflected in the chart. However, the original submission year was 2014.

B. CLASSIFICATION OF AE SCHEMES

The AE schemes in this systematic review were grouped into one of the three categories of independent schemes, CAESAR competition schemes, and NIST competition schemes, labeled as A, B, and C, respectively, as shown in Appendix. They were then classified based on the criteria: building blocks, modes/designs, basic primitives, security parameters (nonce misuse resistance (NMR)), BBB security, and security under RUP), and the set of functional features provided to boost performance, efficiency, or both.

1) CLASSIFICATION BASED ON BUILDING BLOCKS

The schemes were classified according to the underlying cryptographic structure used in the implementation—one of many parameters considered. Eight categories were identified in the selected studies: block cipher (BC), tweakable block cipher (TCB), dedicated construction (DE), hash function (HA), hybrid construction (HB), permutation (PR), stream cipher (SC), and sponge construction (SP). The schemes were grouped according to categories based on the line of work to which they belonged—independent schemes, schemes entered in the CAESAR competition, and those entered in the NIST lightweight AE competition.

Building blocks influence the features provided by the schemes. For instance, while the block ciphers and tweakable block ciphers are mostly favored for their security-related features, permutations seem to be predominantly used because they are light weight. For instance, six of 10 winners of the NIST-LW competition used permutations as underlying primitive. As is shown in Table 2, most independent schemes use block ciphers as building blocks, followed by sponges and stream ciphers.

Figure 5 shows that the number of schemes and the variety of building blocks soared from 2014, indicating the impact of the CEASAR and NIST competitions in prompting contributions from the cryptography community. This also explains the peak in publications from 2014 to 2020. For example, block ciphers were the only constructions used in AE, followed by stream ciphers and some dedicated structures, until sponges and permutations were developed in 2011.

As is shown in the chart in Figure 4, block ciphers (BC) were the dominant building blocks as primitives in symmetric/private key cryptography and have been advanced further since the standardization of the Advanced Encryption Standard (AES) as the algorithm of choice for protecting secret communications.

As shown in figure 6, the building blocks contribute to the magnitude and variability of functional features provided by AE schemes considered in this study.

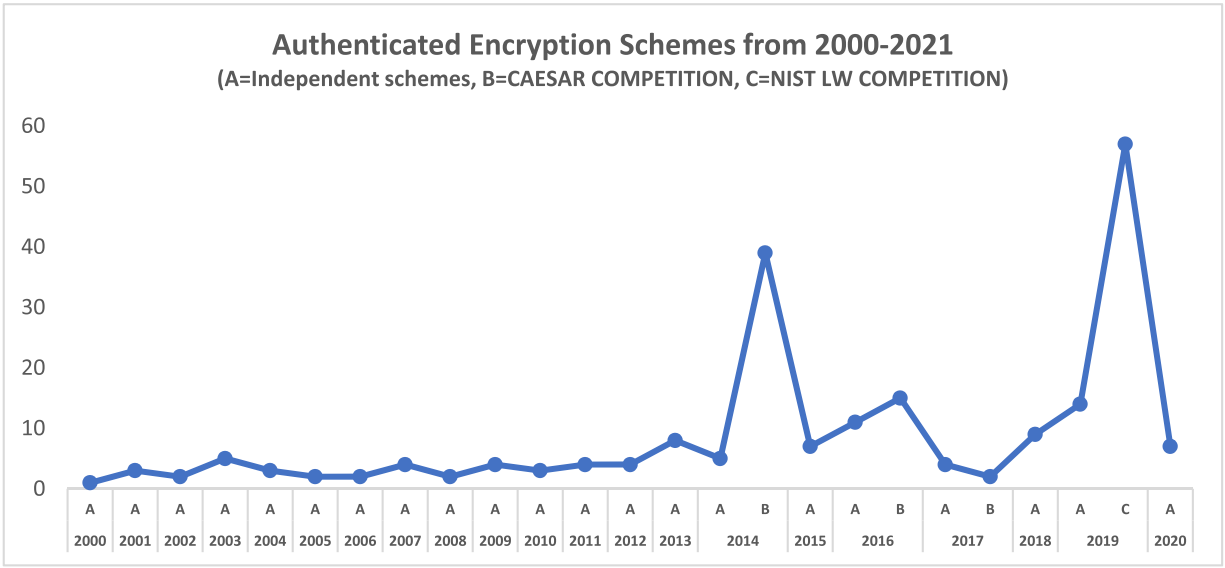

FIGURE 4. Trends of AE schemes from 2000 to 2020.

TABLE 2. AE schemes categorized according to building block.

Building blocks	Independent (Category A)	Caesar Competition (Category B)	NIST-LW Competition (Category C)	Total
Bc	50	24	18	92
Sp	14	6	19	39
Sc	15	6	6	27
Tbc	14	5	7	26
Pr	4	9	6	19
De	6	4	1	11
Hb	1	1	0	2
CF	0	1	0	1
Total	104	56	57	217

2) CLASSIFICATION ACCORDING TO MODE OR DESIGN

The collection of features provided by a scheme depends on its design philosophy, mode of operation, and cryptographic primitives. For instance, the counter mode used with a block cipher supports parallelizability by design, where sponge-based modes are serial at the algorithmic level. A total of 128 modes and design approaches were used in the selected schemes. The 15 most used modes/designs are shown in Table 3.

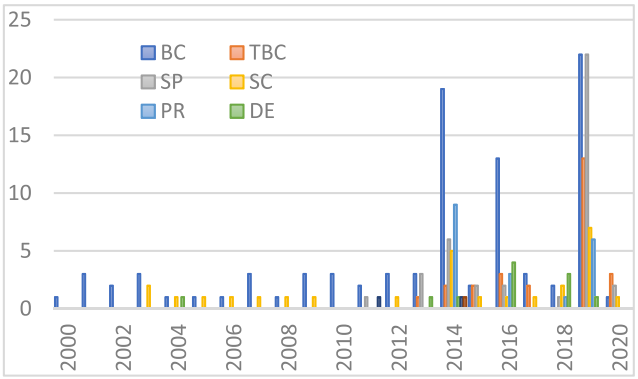

FIGURE 5. Development of building blocks of AE schemes from 2000 to 2020.

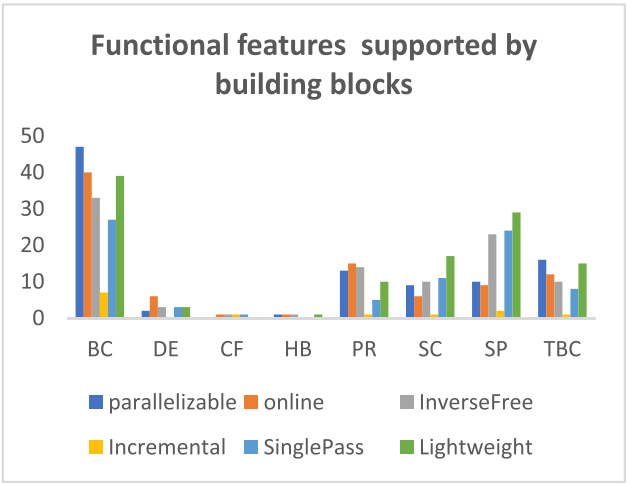

FIGURE 6. The building blocks versus functional features of the AE schemes.

The remaining 113 modes and designs included 10 used only twice, and 103 modes/designs were used only in one scheme. See the table in Appendix for a complete list of modes/designs.

TABLE 3. The 15 most used modes/designs in the reviewed articles.

Mode/Design	No. Schemes	Description
Duplex	14	Duplex design
CTR	10	Counter Mode
LFSR	10	Linear Feedback Shift Register
EME	9	Encrypt Mix Encrypt
OCB	7	Off-set Codebook Mode
TAE	6	Tweakable AE
SIV	6	Synthetic Initialization Vector
ECB	5	Electronic Code Book Mode
ETM	5	Encrypt Then MAC
Sponge	4	Sponge Construction
ARX	4	Add Rotate XOR
OTR	4	Off-set Two Round
MonkeyDuplex	4	Monkey Duplex
SPN	3	Substitution Permutation Network
XEX	3	XOR Encrypt XOR
Others	123	113 modes, Most of Them Used Only Once

TABLE 4. 15 most used cryptographic primitives in the selected articles.

SN	Primitive	Occurrences	Description
1.	AES	64	Advanced Encryption Algorithm
2.	SPN	12	Substitution Permutation network
3.	Sponge	9	Sponge Permutation
4.	TBC	5	Tweakable Block Cipher
5.	Keccak	4	Keccak Function
6.	Permutation	3	Keyed Permutation
7.	PRIMATE-s	3	PRIMATE-s Permutation
8.	GIFT	3	GIFT Block Cipher
9.	Prøst	3	Prost Permutation
10.	SPRING	2	SPRING Tweakable Block Cipher
11.	SKINNY	2	SKINNY Block Cipher
12.	Grain	2	Grain
13.	Deoxys-BC	2	Deoxys Block Cipher
14.	sLiSCP-light	2	sLiSCP-Light Permutation
15.	ICE	2	ICE Cipher
16.	Others	97	96 schemes used a unique primitive once, while two schemes used the same primitives

3) CLASSIFICATION BASED ON CRYPTOGRAPHIC PRIMITIVES

The workhorses of AE schemes and their encryption modes are the encryption algorithms that ensure the confidentiality of messages. They are units that carry out the task of scrambling the plaintext so that no one can easily decipher it without knowing the key. They are the gatekeepers of secure communications, and the stronger and more intelligent they are, the more reliable are the protocols or schemes. In addition to security, encryption primitives also contribute to other desirable features that enhance efficiency, performance and make for compact and elegant design. In the selected studies, 112 types of primitives were used. The 15 most common ones (those that had been used at least in two articles) are shown in Table 4. Each of the remaining 97 encryption primitives had been used only in one study. See Appendix for the complete list of encryption primitives.

4) CLASSIFICATION BASED ON SECURITY-RELATED PROPERTIES

The CAESAR and NIST-LW competitions have helped the evolution of AE schemes from enhancing essential security to supporting a set of desirable features. For example, nonce misuse resistance (Section:II.D.5), security under the release of unverified plaintext (Section II.D.6), and the provision of the beyond birthday bound security (Section II.D.7) provide an additional layer of security to AE schemes.

In the selected studies, 52 schemes (24%) provided NMR, while 165 (76%) did not offer it. Only 28 out of the 217 schemes (13%) provided BBB security while 189 schemes (87%) did not. Only 20 of the 217 schemes (9%) offered security under RUP. The chart in Figure 7 shows the

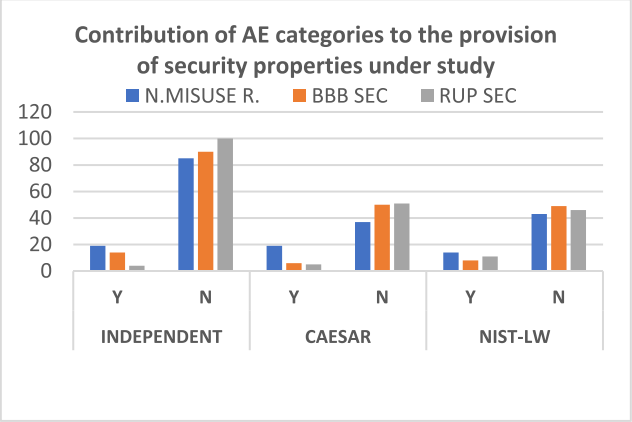

FIGURE 7. Security features: Nonce misuse resistance, BBB security, and RUP security.

number of schemes with and without the security features discussed in this section.

Figure 8 shows that 19 independent schemes, 19 CAESAR schemes, and 14 NIST schemes provided security in the case of nonce misuse. A total of 85 independent schemes, 37 CAESAR schemes, and 43 NIST schemes did not offer protection when nonces were repeated. Fourteen independent schemes, six CAESAR schemes, and eight NIST-LW schemes provided security beyond the birthday bound. Four independent schemes, five CAESAR schemes, and 11 NIST-LW schemes provided RUP security.

The set of security features, such as the functional characteristics, have been developed throughout the evolution of AE schemes. As shown in Figure 9, the target security features were initially absent from published AE schemes from 2000 to 2003. They grew with the number of schemes

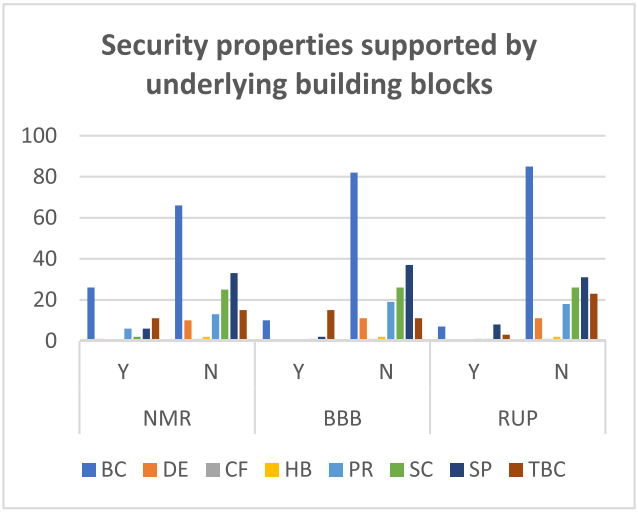

FIGURE 8. How underlying building blocks support security properties.

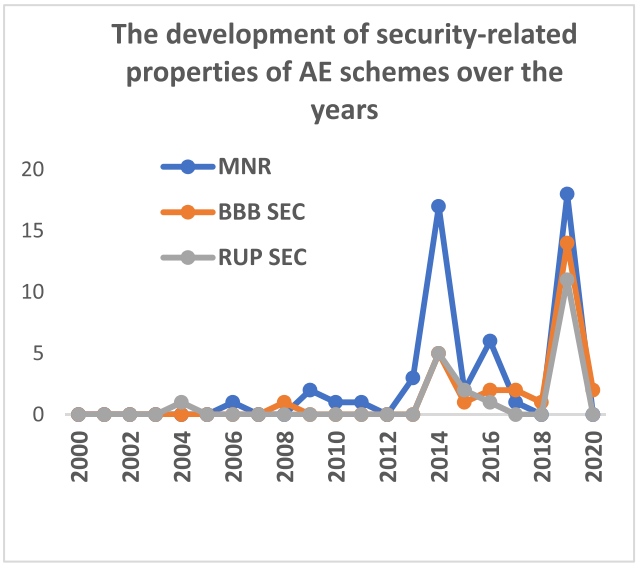

FIGURE 9. The growth of security-related properties of AE schemes over the years.

and were strongly influenced by CAESAR and NIST-LW schemes.

5) CLASSIFICATION BASED ON FUNCTIONAL FEATURES

The selected schemes were also classified based on six important functional features: parallelizability, being online, being inverse free, incrementality, being single pass, and being lightweight. As shown in the chart in Figure 10, the 217 schemes considered in this review varied in their ability to satisfy different functional criteria.

Parallelizability: A total of 98 schemes were parallelizable, 113 were not, five schemes supported this only in encryption, and one scheme supported it for decryption only.

Online: A total of 90 schemes considered in the review were online schemes, 126 were offline schemes, and one scheme was online in encryption.

Inverse free: A total of 95 of the schemes were inverse free (they could use either encryption or decryption but not both) while 122 schemes were not inverse free.

Incrementality: Only 13 of the selected schemes supported incrementality, 202 did not support it, and two supported it in associated data processing.

Single pass: Seventy-nine schemes were single pass while 138 schemes were not.

Lightweight: Whether a scheme is lightweight (designed to support devices with constrained resources) is important in cryptography because a balance is needed between security and efficiency in some cases. Although the NIST competition for lightweight AE targeted schemes with this property, some independent schemes and those in the CAESAR competition are also resource-efficient. A total of 114 of the 217 schemes were lightweight. This clearly shows the effect of NIST schemes as they are all supposed to be lightweight. Figure 9 shows a graphic representation of how the schemes in the study support functional features.

Table 5 shows the schemes as categorized into three parts—independent schemes, CAESAR competition schemes, and NIST lightweight competition schemes—and their support for functional features.

It is interesting to observe how the tweakable block cipher, despite the relatively small number of schemes that use it, noticeably contributed to the variety of functional features and security-related properties of AE schemes. See Figure 5 and Figure 11 for a comparison. Note also how sponges competed with block ciphers and tweakable block ciphers in the context of lightweight schemes, while the first two were dominant in terms of parallelizability. This underlines the relationship between building blocks and the availability of the AE features examined.

Carefully looking into the information acquired from this section regarding the development of AE schemes and trending set of features reveals the continued desire of researchers to achieve the best combination of features possible, which still seems an interesting research problem in the future. The 217 articles in this study tried to balance the security features and other desirable features. Still, none of them achieved all the security features with a complete set of other desirable properties. For instance, none of the schemes in the study that provided BBB security, security under RUP, and NMR security were online or incremental. See Section V for possible future work and open problems.

V. DISCUSSION & FUTURE WORK

This section answers the research questions posed at the outset and discusses research-related issues and possible directions for future work in authenticated encryption in the symmetric key setting.

Research question 1: What is the current status of authenticated encryption schemes?

TABLE 5. How categories of the selected schemes support functional features.

PROPERTY	INDEPENDENT				CAESAR				NIST-LW			
	Y	N	EN	AD	Y	N	EN	DE	Y	N	EN	DE
Parallelizability	40	62	2	0	34	18	3	1	27	30	0	0
Online	31	72	1	0	46	10	0	0	13	44	0	0
Inverse free	24	80	0	0	34	22	0	0	37	20	0	0
Incrementality	5	97	0	2	8	48	0	0	0	57	0	0
Single pass	37	67	0	0	14	42	0	0	28	29	0	0
Lightweight	32	72	0	0	25	31	0	0	57	0	0	0

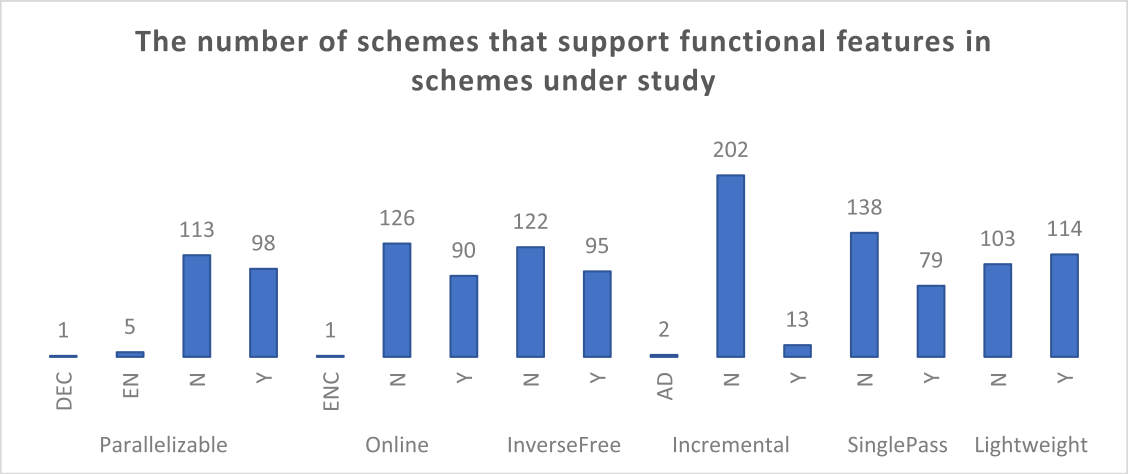

FIGURE 10. Functional features of the schemes in the review (Y = supports the feature, N = does not support the feature, EN = supports only in encryption, DEC = supports only in decryption, AD = supports only associated data processing).

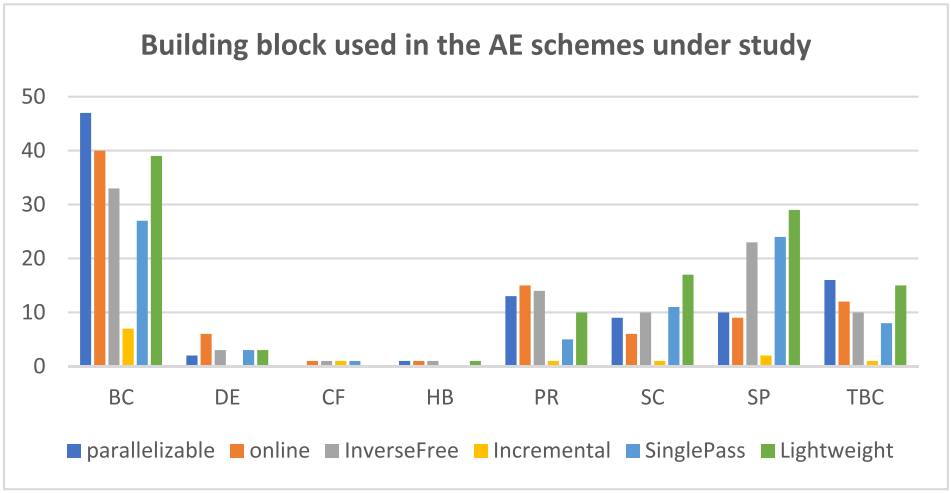

FIGURE 11. Building blocks contributed to the richness of functional features of AE schemes.

Our findings reveal that a vast amount of research has been conducted on AE. We identified 217 articles extracted from eight sources. The articles focused on simultaneously protecting confidentiality and integrity by using diverse approaches.

In addition to the essential security-related requirements, the relevant methods had such features as protection against cryptanalysis, robustness if nonces are repeated (nonce misuse resistance), security under the release of plaintext,

TABLE 6. Classification of CAESAR winners and NIST-LW finalists.

Con	Construction	Mode/ design	Primitive	Parallelizable	Online	Inverse free	Incremental AE	Single pass	N. misuse Resist	Lightweight	BBB security	RUP security
A-CEASAR WINNERS												
COLM	BC	EME	aes	●	●	-	-	●	●	-	-	-
Ascon	PR	Duplex	Ascon	-	●	●	-	-	●	●	-	-
Deoxys	TBC	TAE	Deoxys-BC	●	●	-	-	-	-	●	-	-
OCB 1.1	BC	TAE	AES	●	●	-	-	-	-	-	-	-
ACORN	SC	LFSR	ACCORN	●	●	●	-	-	-	●	-	-
AEGIS	DE	AES	AEGIS	Enc	●	●	-	-	-	-	-	-
B-NIST-LW FINALISTS												
Ascon	SP	Duplex	SPN	-	●	●	-	●	●	-	-	
Elephant	SP	CTR	Spongent	●	-	●	-	-	-	-	-	
GIFT-COFB	BC	COFB	SPN	-	-	●	-	-	-	-	-	
Grain-128	SC	LFSR	Grain-128	●	-	●	-	-	-	-	-	
ISAP	SP	ISAP	Keccak-p	-	-	●	-	●	-	-	●	
PHOTON-Beetle	SP	Beetle	SPN	-	-	●	-	●	-	-	-	
Romulus	TBC	Romulus	Skinny	-	-	●	-	-	●	●	-	
Sparkle	PR	ARX	Sparkle	●	-	-	-	●	-	-	-	
TinyJAMBU	PR	TinyJAMBU	TinyJAMBU	●	-	-	-	-	●	-	-	
Xoodyak	SP	Cyclist	Xoodoo	-	-	●	-	●	-	-	●	

and security beyond the traditional birthday bound limit (BBB security). The schemes considered here also enhanced performance and efficiency, intended to support resource-constrained devices. Finally, a classification framework was proposed according to which the articles were grouped and classified.

Past reviews of the area were also identified, such as [36], [37], [108], [283]. However, they are limited in scope and the range of time covered. This systematic literature review filled this gap by examining three main lines of work on AE schemes from January 2000 to December 2020.

Research Question 2: What criteria are there to compare and categorize authenticated encryption schemes?

For this systematic review, 217 AE schemes were selected and categorized into three groups. Schemes that had been developed before the CAESAR competition (Category A), schemes submitted as part of the CAESAR competition (Category B), and schemes that were submitted as part of the NIST lightweight competition (Category C). The schemes were then further classified according to their security-related features, building blocks, design characteristics, and desirable functional features.

The above categorization revealed that Category A covered 47.9% of the schemes examined, while 26.3% belonged to Category B and 25.8% to Category C. While featuring techniques proposed from 2000 to 2020, Category A was still slightly smaller in size than the two other categories combined. This result emphasizes the impact of the CAESAR and NIST-LW competitions on the number and features of AE schemes.

The schemes were further classified based on their building blocks. The result showed that: 42% of the schemes used block ciphers (BC), 12% of them used tweakable block ciphers, 18% used sponge construction (SP), 12% used stream ciphers (SC), 9% used permutations, 5.2% used dedicated constructions, 1% used hybrid constructions, and 0.5% used hash functions.

TABLE 7. List of the schemes selected for SLR with collection of features they support.

Scheme	Construction	Mode/ design	Primitive	Parallelizable	Online	Inverse-free	Incremental AE	Single-pass	N. misuse Resist	Lightweight	BBB security	RUP security	Category	Round
[6]	BC	Generic	AES	•	-	-	-	-	-	-	-	-	A	-
[16]	BC	IAPM	Aes	•	-	-	-	•	-	-	-	-	A	-
[15]	BC	RPC	AES	•	-	-	-	•	-	-	-	-	A	-
[18]	BC	OCB	AES	•	•	-	-	•	-	-	-	-	A	-
[17]	BC	XCBC XECB	AES	•	-	-	•	•	-	-	-	-	A	-
[38]	BC	OCB	AES	•	-	-	-	•	-	-	-	-	A	-
[22]	BC	EAX	Aes	-	•	•	-	-	-	•	-	-	A	-
[111]	SC	XEX	Vernam cipher	•	-	-	-	•	-	•	-	-	A	-
[21]	BC	CCM	AES	Enc	-	•	-	-	-	•	-	-	A	-
[112]	BC	CWC	AES	•	•	•	-	-	-	-	-	-	A	-
[110]	SC	LFSR	Helix	-	-	-	-	•	-	•	-	-	A	-
[95]	BC	DTM	DCBC	-	•	-	-	-	-	-	-	•	A	-
[70]	DE	Quantum states	BB84	-	-	-	-	•	-	-	-	-	A	-
[39]	SC	VMPC-MAC	VMPC	-	-	-	-	•	-	-	-	-	A	-
[113]	BC	CCFB CCFB+H	AES	-	-	-	-	-	-	•	-	-	A	-
[93]	SC	Vest CIPHER	VEST-8	-	-	-	-	•	-	-	-	-	A	-
[114]	SC	IEP	RC4	-	-	-	-	-	-	•	-	-	A	-
[44]	BC	SIV	AES	•	•	-	-	-	•	-	-	-	A	-
[23]	BC	GCM	AES	•	-	•	-	-	-	-	-	-	A	-
[115]	BC	GFN	LIRKES	-	-	-	-	-	-	•	-	-	A	-
[116]	BC	CTR	AES	-	-	-	-	•	-	-	-	-	A	-
[117]	SC	ETM	Dragon	-	-	-	-	-	-	•	-	-	A	-
[92]	BC	CIP	AES	•	-	-	-	-	-	-	•	-	A	-
[64]	SC	Rabbit-MAC	Rabbit	-	-	-	-	-	-	•	-	-	A	-
[118]	BC	BTM	AES	-	-	•	-	-	•	-	-	-	A	-
[119]	BC	CTR	AES	-	-	-	-	-	•	-	-	-	A	-
[120]	SC	LFSR	PingPong	-	-	•	•	•	-	•	-	-	A	-
[121]	BC	RTC	Marvin	•	-	-	•	-	-	•	-	-	A	-
[122]	BC	SCMA	CTR-OFB	-	-	•	-	•	•	•	-	-	A	-
[123]	BC	AE+	AES	-	•	-	-	•	-	-	-	-	A	-
[124]	BC	OCB	AES	•	•	-	-	•	-	-	-	-	A	-
[41]	SP	SpongeWrap	Permutation	-	-	-	-	•	-	-	-	-	A	-
[68]	HB	Hummingbird	Hummingbird-2	-	-	-	-	-	-	•	-	-	A	-
[125]	BC	TCH	AES, THREEFISH	-	•	-	-	-	•	-	-	-	A	-
[126]	BC	AtE	aes	•	-	-	-	-	-	-	-	-	A	-
[127]	BC	JCM	AES	-	-	-	-	-	-	•	-	-	A	-
[128]	BC	CBC	AES	-	-	-	-	-	-	-	-	-	A	-
[129]	SC	ASC-1	4R-AES	-	-	-	-	•	-	-	-	-	A	-
[130]	BC	DLAE	AES	-	-	-	-	•	-	-	-	-	A	-
[106]	SP	APE	permunation	-	Enc	-	-	-	•	•	-	-	A	-
[131]	BC	COPA	AES	•	•	-	-	-	•	-	-	-	A	-
[42]	DE	SPN	FIDES	-	•	-	-	•	-	•	-	-	A	-
[132]	BC	RBS	RBS	-	-	-	-	-	-	•	-	-	A	-
[133]	TBC	OTR	PRP	•	•	•	-	•	-	-	-	-	A	-
[134]	SP	Duplex	SPN	•	-	-	-	•	-	-	-	-	A	-
[135]	SP	CBEAM	SPN	-	-	-	-	-	-	•	-	-	A	-
[136]	BC	CMCC	AES	-	-	-	-	-	•	-	-	-	A	-
[65]	PR	JHAE	JH	•	•	•	-	•	-	-	-	-	A	-
[137]	PR	AESQ	AES	•	•	•	-	-	Int	-	-	-	A	-
[43]	BC	EME	AES	•	•	-	-	•	•	-	-	-	A	-
[138]	SP	Triplex	Sponge	•	-	-	•	-	•	-	-	-	A	-
[139]	PR	ICEPOLE	duplex	•	•	•	-	-	•	-	-	-	A	-
[91]	SP	sp-AELM	Sponge	-	•	-	-	-	-	•	-	•	A	-
[105]	SC	LFSR	TriviA	Enc	-	-	-	-	-	•	-	-	A	-
[84]	BC	GCM-SIV	AES	•	-	•	-	-	•	-	-	-	A	-
[140]	BC	OAE2	AES	-	•	-	-	-	-	-	-	-	A	-
[141]	SP	Duplex	SPN	-	-	•	-	-	-	-	-	-	A	-
[142]	TBC	ETE	MiniAE	•	-	-	-	•	-	-	-	•	A	-
[143]	TBC	SCT	CTRT	•	-	•	Ad	-	•	-	•	-	A	-

TABLE 7. *(Continued.)* **List of the schemes selected for SLR with collection of features they support.**

Scheme	Construction	Mode/ design	Primitive	Parallelizable	Online	Inverse-free	Incremental AE	Single-pass	N. misuse Resist	Lightweight	BBB security	RUP security	Category	Round
[147]	BC	EME	AES	•	•	-	-	•	•	•	-	-	B	-
[144]	BC	RIV	AES	•	•	-	-	-	•	-	-	•	A	-
[145]	BC	XCAU	AES	-	-	-	-	-	-	-	-	-	A	-
[146]	BC	DIV	DTE	-	-	-	-	-	•	-	-	-	A	-
[103]	TBC	LAE3	SPRING	-	-	-	-	•	-	-	-	-	A	-
[103]	BC	LAE1	SPRING	-	-	-	-	-	-	-	-	-	A	-
[148]	SP	Isap	Sponge	-	-	-	-	-	-	-	-	-	A	-
[149]	BC	DCT	SPRP	-	-	-	-	-	-	-	•	-	A	-
[150]	BC	SIV	TBC	•	-	-	-	-	-	-	•	-	A	-
[69]	DE	EtM	FASKC	-	-	-	-	-	-	-	-	-	A	-
[104]	BC	OCB	TBC	•	•	-	-	•	-	-	-	-	A	-
[100]	BC	XEX	AES	•	-	-	•	-	-	-	-	-	A	-
[151]	BC	ZETA	AES	-	-	-	-	-	-	•	-	-	A	-
[152]	BC	CEP	AES	-	-	-	-	-	-	-	-	-	A	-
[153]	SC	AENOTP	DBAES	-	-	•	-	•	-	-	-	-	A	-
[154]	TBC	XKX	TSPRP	-	-	-	-	•	-	-	•	-	A	-
[155]	DE	SPN	UFN	-	•	-	-	-	-	-	-	-	A	-
[156]	SP	Beetle	SPN	-	-	•	-	•	-	•	-	-	A	-
[157]	DE	LinHAE	LHF	-	-	-	-	-	-	-			A	-
[158]	PR	IAPM	Keccak	•	•	-	-	•	-	-	-	-	A	-
[159]	SC	KAS-AE	MLE	-	-	-	-	-	-	-	-	-	A	-
[160]	BC	SEAB	SPN	-	•	•	-	-	-	-	-	-	A	-
[161]	SC	EtM	XUBA	-	-	-	-	-	-	-	-	-	A	-
[162]	BC	RWCTR	AXU	•	-	-	-	-	-	-	•	-	A	-
[163]	DE	DCAE	SCML	•	•	-	-	•	-	•	-	-	A	-
[164]	TBC	PAEF	ForkSnunny	•	-	-	-	-	-	•	-	-	A	-
[165]	TBC	XTX	ZOTR	•	-	•	-	-	-	-	•	-	A	-
[166]	TBC	EtM	TEDT	-	•	-	Ad	-	•	-	•	-	A	-
[167]	SP	SpookChain	TETSponge	-	•	-	-	-	-	•	•	-	A	-
[168]	BC	COFB	Aes, GIFT	-	-	•	-	-	-	•	-	-	A	-
[169]	SP	T-sponge	SALE	-	-	-	-	-	-	-	-	-	A	-
[170]	BC	SimpleENC, SimpleENCsmall	Aes	-	•	•	-	-	-	-	-	-	A	-
[171]	SP	TETSponge	SPN	-	-	-	-	•	Enc	-	-	-	A	-
[172]	SC	LFSR	Grain-128AEAD	-	-	-	-	-	-	•	-	-	A	-
[173]	BC	CTR	AES	-	-	-	-	-	•	•	-	-	A	-
[174]	TBC	OCB3	AES	•	•	-	-	•	-	-	•	-	A	-
[176]	TBC	PFB	SKINNY	-	•	•	-	-	-	•	•	-	A	-
[177]	TBC	Romulus/Remus	TBC	-	-	•	-	•	•	•	•	-	A	-
[286]	BC	CTR	AES	•	-	-	-	-	-	-	-	-	A	-
[66]	PR	JHAE	SPN	-	•	•	-	•	-	-	-	-	B	1
[206]	BC	PCMAC	AES	•	-	-	-	•	-	-	-	-	B	1
[208]	BC	ECB	AES	•	-	-	-	-	•	-	-	-	B	1
[208]	BC	CTR	AES	•	-	•	-	-	•	-	-	-	B	1
[209]	BC	CTR	AES	•	•	•	-	•	-	-	-	-	B	1
[67]	HB	Enchilada	ChaCha, Rijndael	•	•	•	-	-	-	-	-	-	B	1
[213]	BC	ECB	AES	Enc	•	-	-	•	-	-	-	-	B	1
[214]	TBC	TAE	KIASU-BC,AES	•	•	-	-	-	-	•	•	-	B	1
[214]	TBC	EME	KIASU-BC	•	•	-	-	-	•	•	•	-	B	1
[215]	PR	Sponge	Prøst	•	•	•	-	-	•	-	-	-	B	1
[215]	PR	OTR	Prøst	•	•	•	-	-	-	-	-	-	B	1
[215]	PR	Sponge	Prøst	-	•	-	-	-	•	-	-	-	B	1
[217]	BC	LAC	LBlock	•	•	-	-	•	-	•	-	-	B	1
[218]	SC	ARX	Wheesht	-	•	•	-	-	-	•	-	-	B	1
[219]	BC	PFB	AES	Enc	•	•	•	-	-	-	-	-	B	1
[220]	BC	ECB	AES	•	•	-	•	-	-	-	-	-	B	1
[221]	BC	ECB	AES	•	-	-	-	-	-	•	-	-	B	1
[224]	BC	CBC	AES	-	-	•	-	-	•	•	-	-	B	1
[225]	SC	MAG	MAGV2	-	•	•	-	-	-	-	-	-	B	1
[226]	DE	Algebraic methods	quaternion feld	-	-	-	-	-	-	-	-	-	B	1

TABLE 7. *(Continued.)* **List of the schemes selected for SLR with collection of features they support.**

Scheme	Construction	Mode/ design	Primitive	Parallelizable	Online	Inverse-free	Incremental AE	Single-pass	N. misuse Resist	Lightweight	BBB security	RUP security	Category	Round
[229]	SC	LFSR	Sablier	•	•	•	-	-	-	-	-	-	B	1
[230]	BC	iFeed	AES	•	•	•	•	•	-	-	-	-	B	1
[193]	BC	ECB	AES	-	•	-	-	-	•	-	-	•	B	2
[194]	SP	SpongeWrap	PRIMATEs	-	•	•	-	-	-	•	-	-	B	2
[194]	SP	Duplex	PRIMATEs	-	•	•	-	-	-	•	-	-	B	2
[194]	SP	Duplex	PRIMATEs	-	•	-	-	-	•	•	-	•	B	2
[195]	BC	PPAE	AESQ	•	•	•	•	-	•	-	-	-	B	2
[196]	SC	NFSR	Trivia	•	-	•	-	•	•	•	•	•	B	2
[197]	HA	OMD	SHA256	-	•	•	•	•	-	-	-	-	B	2
[198]	SP	ARX	Priplex	•	-	-	•	-	-	•	-	•	B	2
[199]	BC	TAE	SCREAM	•	•	•	-	-	-	•	•	-	B	2
[200]	BC	TAE	AES	•	•	-	-	-	-	•	-	-	B	2
[200]	BC	EME	AES	•	•	-	-	-	-	•	-	-	B	2
[201]	SC	SIV	ChaCha	-	-	•	-	-	•	-	-	-	B	2
[202]	PR	Duplex	Sponge	•	•	•	-	-	-	-	-	-	B	2
[203]	SP	Duplex	Sponge	-	•	•	-	•	-	-	-	-	B	2
[204]	PR	XEX	TEM	•	•	-	-	-	•	•	-	•	B	2
[205]	BC	EME	AES	•	•	-	-	-	•	-	•	-	B	2
[287]	BC	EME	AES	Dec	•	•	-	•	-	•	-	-	B	3
[25]	BC	EME	aes	•	•	-	-	•	•	-	-	-	B	3
[98]	SP	Duplex, LRX	Sponge	•	•	•	-	•	-	-	-	-	B	3
[186]	PR	MonkeyWrap	Keccak-f	-	•	•	-	-	-	•	-	-	B	3
[97]	PR	Motorist	Keccak-p	•	•	•	•	-	-	•	-	-	B	3
[26]	PR	Duplex	Ascon	-	•	•	-	-	•	•	-	-	B	3
[27]	TBC	TAE	Deoxys-BC	•	•	-	-	-	-	•	-	-	B	3
[27]	TBC	EME	Deoxys-BC	•	•	-	-	-	•	•	-	-	B	3
[28]	BC	TAE	AES	•	•	-	-	-	-	-	-	-	B	3
[188]	BC	OTR	AES	•	•	•	-	•	-	-	-	-	B	3
[189]	DE	Tiaoxin	AES round	•	•	•	-	-	-	-	-	-	B	3
[30]	SC	LFSR	ACCORN	•	•	•	-	-	-	•	-	-	B	3
[190]	BC	OFB	AES	-	•	•	-	-	•	•	-	-	B	3
[191]	DE	LRX	MORUS	-	•	•	-	-	-	-	-	-	B	3
[29]	DE	AES	AEGIS	Enc	•	•	-	-	-	-	-	-	B	3
[192]	TBC	EME	AES	•	-	•	•	-	•	-	•	-	B	3
[94]	BC	CFB	AES	-	•	•	-	-	-	•	-	-	B	3
[267]	SC	LFSR	Bleep64	-	•	-	-	•	-	•	-	-	C	1
[48]	SP	MonkeyDuplex	LED	-	-	•	-	•	-	•	-	-	C	1
[271]	DE	CLAE	CLAE	-	-	-	-	-	•	•	-	-	C	1
[279]	SP	Duplex	Spoge	-	-	•	-	•	-	•	-	-	C	1
[274]	BC	FleaxAEAD	KDP	•	-	-	-	-	-	•	-	-	C	1
[281]	SC	LFSR	Fountain	•	-	-	-	-	-	•	-	-	C	1
[49]	SP	SPN	GAGE	•	-	•	-	•	-	•	-	-	C	1
[288]	SP	LFSR	HERN	-	-	-	-	-	-	•	-	-	C	1
[278]	BC	LAEM	Simon	•	-	•	-	•	-	•	-	•	C	1
[262]	TBC	EGFN	AES	•	•	-	-	-	•	•	-	-	C	1
[272]	BC	AXR	Limdolen	•	-	-	-	-	•	•	-	-	C	1
[50]	BC	PANORAmA	QARMA	•	-	-	-	-	-	•	•	-	C	1
[282]	SC	Quartet	Quartet	•	-	-	-	-	-	•	-	-	C	1
[269]	BC	Remus	ICE	-	-	•	-	-	•	•	•	-	C	1
[275]	SP	Duplex	Sponge	-	-	•	-	•	-	•	-	-	C	1
[268]	BC	CTR	GIFT	-	•	•	-	-	-	•	-	-	C	1
[264]	BC	SIV	Rijndael	-	-	•	-	-	•	•	-	•	C	1
[265]	TBC	SIV	TEM-PHOTON	-	-	•	-	-	•	•	-	•	C	1
[276]	PR	ARX	SNEIK	-	-	•	-	-	-	•	-	-	C	1
[277]	SP	MonkeyDuplex	SPN	-	-	•	-	•	-	•	-	-	C	1
[270]	TBC	SIV	ICE	-	-	•	-	-	•	•	•	-	C	1
[263]	SC	TRIAD	TRIAD	•	-	-	-	•	-	•	-	-	C	1
[266]	BC	TRIFLE	TRIFLE-BC	-	-	•	-	-	•	•	-	-	C	1
[273]	SP	Sponge	Yarar´a	-	-	•	-	•	-	•	-	-	C	1
[231]	PR	sLiSCP	Simeck	•	•	•	-	•	-	•	-	-	C	2

TABLE 7. *(Continued.)* **List of the schemes selected for SLR with collection of features they support.**

Scheme	Construction	Mode/ design	Primitive	Parallelizable	Online	Inverse-free	Incremental AE	Single-pass	N. misuse Resist	Lightweight	BBB security	RUP security	Category	Round
[254]	SP	Duplex	SPN	•	•	•	-	•	•	•	-	-	C	3
[256]	BC	CTR	AES	-	-	-	-	•	-	•	-	-	C	2
[3]	SP	DrySponge	Sponge	-	-	•	-	•	-	•	-	-	C	2
[244]	SP	CTR	Spongent	•	-	•	-	-	-	•	-	-	C	3
[247]	TBC	ESTATE	TweAES	-	-	•	-	-	•	•	-	•	C	2
[235]	TBC	PAEF	forkcipher	•	•	-	-	-	-	•	-	-	C	2
[238]	BC	COFB	SPN	-	-	•	-	-	-	•	-	-	C	3
[243]	SP	Gimli	Gimli-24	•	-	-	-	•	-	•	-	•	C	2
[257]	SC	LFSR	Grain-128	•	-	•	-	-	-	•	-	-	C	3
[248]	BC	HyFB	GIFT-128	-	-	•	-	•	-	•	-	-	C	2
[253]	SP	ISAP	Keccak-p	-	-	•	-	•	-	•	-	•	C	3
[261]	SP	MonkeyDuplex	SPN	-	-	•	-	•	-	•	-	•	C	2
[236]	BC	OTR	TweGIFT	•	•	•	-	•	-	•	•	•	C	2
[236]	BC	OCB	TweGIFT	•	•	•	-	•	-	•	•	•	C	2
[249]	BC	mixFeed	AES	-	•	•	-	-	-	•	-	-	C	2
[250]	PR	PHOTON	PHOTON	-	•	•	-	-	-	•	-	-	C	2
[245]	SP	Duplex	SimP	-	•	•	-	•	-	•	-	•	C	2
[239]	SP	Beetle	SPN	-	-	•	-	•	-	•	-	-	C	3
[255]	BC	OCB	Pyjamask	•	•	-	-	•	-	•	-	-	C	2
[258]	TBC	Romulus	Skinny	-	-	•	-	-	•	•	•	-	C	3
[259]	BC	SAEB	AES	-	•	•	-	-	-	•	-	-	C	2
[246]	BC	CTR	Saturnin	•	-	-	-	-	-	•	-	-	C	2
[240]	PR	ARX	Sparkle	•	-	-	-	•	-	•	-	-	C	3
[241]	TBC	OCB3	SKINNY-128-384	•	-	-	-	-	-	•	•	-	C	2
[234]	SP	MonkeyDuplex	sLiSCP-light	-	-	•	-	•	-	•	-	-	C	2
[233]	SP	Sponge	sLiSCP-light	•	-	•	-	•	-	•	-	-	C	2
[242]	SP	S1P	Spook	-	-	-	-	•	•	•	•	-	C	2
[252]	SC	Duplex	DECK	-	-	-	-	•	-	•	-	-	C	2
[237]	BC	SUNDAE	GIFT-128	-	-	•	-	-	•	•	-	-	C	2
[260]	PR	TinyJAMBU	TinyJAMBU-128	•	-	-	-	-	•	•	-	-	C	3
[232]	PR	sLiSCP	WAGE	•	-	•	-	-	-	•	-	-	C	2
[251]	SP	Cyclist	Xoodoo	-	-	•	-	•	-	•	-	•	C	3
[181]	BC	EtM	AES	-	-	-	-	-	-	-	-	-	A	-
[185]	SP	Duplex	Friet-P	-	-	-	-	•	-	-	-	-	A	-
[183]	TBC	TAE	PBF_plus	-	-	-	-	-	-	•	-	-	A	-
[78]	TBC	OCB+R1	TBC	•	•	-	-	•	-	-	•	-	A	-
[180]	SC	SIV	Salsa2- or ChaCha	•	•	•	-	-	-	-	-	-	A	-
[179]	TBC	QCB	TBC	•	•	-	-	•	-	-	•	-	A	-
[178]	SP	Duplex	Permutation	•	-	•	-	-	-	•	-	-	A	-

When classified based on encryption modes and design approaches, the schemes showed a significant variation. A total of 128 design and encryption modes were observed; 20% of the schemes used the counter (CTR) mode, duplex design, encrypt–mix–encrypt (EME), linear feedback-shift register (LFSR), and a collection of hybrid modes and designs. Table 3 shows the 15 most commonly used modes and designs, and Appendix shows a complete list of schemes along with the designs and modes used.

When classified according to the cryptographic primitives that the schemes used, 112 primitives were identified. AES was the most used primitive, representing 54% of the total, followed by the substitution permutations network (10%) and sponge functions (7%). Table 4 shows the 15 most common primitives in the selected articles, and Appendix shows a complete list of the primitives identified.

Another classification used in this study was based on desirable security features, namely, robustness in the face of nonce repetition or nonce misuse resistance (NMR), security beyond the birthday bound (BBB security), and security under release of unverified plaintext (RUP). We noted that 24% of the 217 articles had proposed methods that could resist security violations if nonces were repeated, 13% supported BBB security, and 9% of the schemes offered security in case of RUP.

The selected schemes were also classified according to whether they supported six desirable functional features: parallelizability, online capabilities, inverse free, incrementality, single pass, and lightweight. The result showed that 45% of

the selected schemes were parallelizable, 52% were not parallelizable, 2% supported parallelizability in encryption, and less than 0.5% supported processing associated data. In addition, 41% of the schemes were online, 58% were offline, and less than 1% were online only for the encryption process.

A total of 44.3% of the schemes were inverse free, meaning that they needed only encryption or decryption but not both. On the other hand, 6.19% were incremental, 92.86% of the schemes examined were not, and a 0.9% supported incrementality in the associated data processing. Of the considered schemes, 36% were single-pass schemes, while 64% needed more than one pass for processing encryption and authentication, 52% were suitable for resource-constrained environments, and 48% were not tailored to work in such environments.

A. CLASSIFICATION OF CAESAR WINNERS AND NIST FINALISTS BASED ON OUR FRAMEWORK

We applied our classification framework to winners of the CAESAR competition and finalists of the NIST-LW competition to determine the extent to which they provide the security-related properties and functional features of interest. Table 6 summarizes the results.

Research Question 3: What are the research-related issues and directions of future research on authenticated encryption?

The clear challenge in developing authenticated encryption schemes is that of striking a balance between properties with sometimes conflicting effects. From our findings, it is clear that researchers attempt to achieve efficient performance without compromisings security. We found that the only scheme that is parallelizable, online, single pass, inverse free, and incremental, the one proposed in [230], fails to satisfy all three properties of NMR, RUP security, and BBB security. Similarly, the only scheme that was NMR secure, RUP secure, and provided BBB security, the one in [196], was not online and did not provide incrementality, two important features influencing the performance of AE schemes.

One direction of research in the future should be to develop schemes that provide the maximum possible security with some performance gains by considering the prevalence of constrained devices of the future. With the rise of cloud and edge computing, another direction of research is the application of homomorphic encryption and searchable encryption, allowing users to access data saved in the cloud without allowing the hosting service provider to read or understand it. In this review, the authors found only one study related to homomorphic encryption [157].

With the potential exhibited by quantum computing, many researchers have claimed that current cryptographic algorithms would be rendered ineffective under it. Quantum authenticated encryption is thus expected to become a popular subject of research in the near future. It is also widely believed that quantum attacks do not threaten symmetric cryptography, but recent work [284], [285] has shown that many AE modes can be compromised in the superposition model. Therefore, in this review, the authors found only two sources [179], [286] related to quantum AE.

Protection against side-channel attacks (SCA) on sponge-based AE schemes and parallel and incremental schemes remains an open problem. Improving the flexibility of AE schemes is also another good topic in research. The AEAD components can be flexibly arranged in the overall process. For instance, to process the plaintext before or after the associated data in environments where such flexibility is essential. As this study focused on AE in the symmetric key setting, conducting a comprehensive systematic literature review of AE schemes in the public key setting is also an open problem.

VI. CONCLUSION

Since its first formal inception in 2000, research on AE has evolved significantly, adding different dimensions to the original idea of protecting confidentiality and integrity in one primitive, to the development of different modes of encryption, building blocks, and encryption primitives. The CAESAR competition was held to solicit submissions of AE schemes with different characteristics, with the AES-GCM as a reference to further propel research in the area. The resulting schemes have contributed considerably to the development of AE. Furthermore, the NIST-LW competition has helped the development of AE schemes that are suitable for resource-constrained environments.

AE schemes play an important in secure communications. For instance, Transport Layer Security (TLS), one of the most widely used protocols to protect communications over a network, has removed support for non-AE schemes as of August 2018. Despite the importance of AE and the availability of many relevant schemes, a systematic literature review that can help researchers become acquainted with past work and possible future research directions had been hitherto lacking. This review fills this gap by analyzing 217 articles were selected from eight sources. We categorized, classified, and analyzed the relevant methods based on design, security-related features, and desirable functional features. We also identified open challenges in the area.

APPENDIX

Appendix shows a list of the schemes selected for SLR with the collection of features they support. See Table 7.

REFERENCES

[1] P. Hawkes and G. G. Rose. (2003). *A Mode of Operation with Partial Encryption and Message Integrity*. Cryptology ePrint. [Online]. Available: https://eprint.iacr.org/2003/001.pdf
[2] J. Jonsson, "On the security of CTR + CBC-MAC," in *Selected Areas in Cryptography (SAC)*. Berlin, Germany: Springer, 2003, pp. 76–93.
[3] S. Riou. *DryGASCON, Lightweight Cryptography Standardization Process Round 1 Submission*. NIST. Accessed: Jul. 17, 2021. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/drygascon-spec-round2.pdf
[4] M. Dworkin, *Recommendation for Block Cipher Modes of Operation—The CCM Mode for Authentication and Confidentiality*, document NIST, SP 800-38C, 2007.
[5] (2018). *The Transport Layer Security (TLS) Protocol Version 1.3, E. Rescorla*. [Online]. Available: https://tools.ietf.org/pdf/rfc8446.pdf

[6] M. Bellare and C. Namprempre, "Authenticated encryption: Relations among notions and analysis of the generic composition paradigm," in *Advances in Cryptology—ASIACRYPT*. Berlin, Germany: Springer, 2000, pp. 531–545.

[7] M. Bellare and C. Namprempre, "Authenticated encryption: Relations among notions and Analysis of the generic composition paradigm," *J. Cryptol.*, vol. 21, no. 4, pp. 469–491, Oct. 2008, doi: 10.1007/s00145-008-9026-x.

[8] M. Bellare, T. Kohno, and C. Namprempre, "Breaking and provably repairing the SSH authenticated encryption scheme: A case study of the encode-then-encrypt-and-MAC paradigm," *ACM Trans. Inf. Syst. Secur.*, vol. 7, no. 2, pp. 206–241, May 2004, doi: 10.1145/996943.996945.

[9] A. Boldyreva and V. Kumar, "Provable-security analysis of authenticated encryption in Kerberos," *IET Inf. Secur.*, vol. 5, no. 4, pp. 207–219, 2011, doi: 10.1049/iet-ifs.2011.0041.

[10] J. P. Degabriele and K. G. Paterson, "On the (in)security of IPsec in MAC-then-encrypt configurations," in *Proc. 17th ACM Conf. Comput. Commun. Secur. (CCS)*, 2010, pp. 493–504, doi: 10.1145/1866307.1866363.

[11] K. G. Paterson and G. J. Watson, "Authenticated-encryption with padding: A formal security treatment," in *Cryptography Security: From Theory to Applications: Essays Dedicated to Jean-Jacques Quisquater Occasion His 65th Birthday*, D. Naccache, Ed. Berlin, Germany: Springer, 2012, pp. 83–107.

[12] S. Vaudenay, "Security flaws induced by CBC padding–applications to SSL, IPSEC, WTLS," in *Advances in Cryptology—EUROCRYPT*. Berlin, Germany: Springer, 2002, pp. 534–545.

[13] H. Krawczyk, "The order of encryption and authentication for protecting communications (or: How secure is SSL)," in *Advances in Cryptology—CRYPTO*. Berlin, Germany: Springer, 2001, pp. 310–331.

[14] C. J. A. Jansen and D. E. Boekee, "Modes of blockcipher algorithms and their protection against active eavesdropping," in *Advances in Cryptology—EUROCRYPT*. Berlin, Germany: Springer, vol. 87, 1987, pp. 281–286.

[15] J. Katz and M. Yung, "Unforgeable encryption and chosen ciphertext secure modes of operation," in *Fast Software Encryption*. Berlin, Germany: Springer, 2001, pp. 284–299.

[16] C. S. Jutla, "Encryption modes with almost free message integrity," in *Advances in Cryptology—EUROCRYPT*. Berlin, Germany: Springer, 2001, pp. 529–544.

[17] V. D. Gligor and P. Donescu, "Fast encryption and authentication: XCBC encryption and XECB authentication modes," in *Fast Software Encryption*. Berlin, Germany: Springer, 2002, pp. 92–108.

[18] P. Rogaway, M. Bellare, J. Black, and T. Krovetz, "OCB: A block-cipher mode of operation for efficient authenticated encryption," presented at the 8th ACM Conf. Comput. Commun. Secur., Philadelphia, PA, USA, 2001.

[19] K. Martin, *Everyday Cryptography*. Oxford, U.K.: Oxford Press, 2012.

[20] P. Rogaway, "Efficient instantiations of tweakable blockciphers and refinements to modes OCB and PMAC," in *Advances in Cryptology—ASIACRYPT*. Berlin, Germany: Springer, 2004, pp. 16–31.

[21] D. Whiting, R. Housley, and N. Ferguson, *Counter With CBC-MAC (CCM)*, document RFC Editor, 2003.

[22] M. Bellare, P. Rogaway, and D. Wagner, "EAX: A conventional authenticated-encryption mode," *Cryptol. ePrint Arch.*, pp. 389–407, Sep. 2003. [Online]. Available: https://eprint.iacr.org/2003/069

[23] M. Dworkin, *Recommendation for Block Cipher Modes of Operation-Galois/Counter Mode (GCM) and GMAC*. Gaithersburg, MD, USA: NIST, Nov. 2007.

[24] A. Inoue, T. Iwata, K. Minematsu, and B. Poettering, "Cryptanalysis of OCB2: Attacks on authenticity and confidentiality," *J. Cryptol.*, vol. 33, no. 4, pp. 1871–1913, Oct. 2020, doi: 10.1007/s00145-020-09359-8.

[25] E. Andreeva. *COLM v1*. NIST. Accessed: Feb. 3, 2021. [Online]. Available: https://competitions.cr.yp.to/round2/colm.pdf

[26] C. Dobraunig, M. Eichlseder, F. Mendel, and M. Schläffer. *Ascon v2*. NIST. Accessed: Feb. 3, 2021. [Online]. Available: http://competitions.cr.yp.to/round1/asconv1.pdf

[27] J. Jean, I. Nikolić, and T. Peyrin. *Deoxys v1.41*. NIST. Accessed: Jan. 17, 2021. [Online]. Available: http://competitions.cr.yp.to/round1/deoxysv1.pdf

[28] T. Krovetz and P. Rogaway. *OCB (v1.1)*. NIST. Accessed: Jan. 14, 2021. [Online]. Available: http://competitions.cr.yp.to/round1/ocbv1.pdf

[29] H. Wu and B. Preneel. *AEGIS—A Fast Authenticated Encryption Algorithm (v1.1)*. NIST. Accessed: Jan. 14, 2021. [Online]. Available: http://competitions.cr.yp.to/round1/aegisv1.pdf

[30] H. Wu. *ACORN—A Lightweight Authenticated Cipher (v3)*. NIST. Accessed: Feb. 2, 2021. [Online]. Available: http://competitions.cr.yp.to/round1/acornv1.pdf

[31] Y. Zheng, "Digital signcryption or how to achieve cost(signature & encryption) ? cost(signature) + cost(encryption)," in *Advances in Cryptology—CRYPTO*, vol. 97. Berlin, Germany: Springer, 1997, pp. 165–179.

[32] H. Petersen, "Authenticated encryption schemes with low communication costs," *Electron. Lett.*, vol. 30, no. 15, pp. 1212–1213, Jul. 1994, doi: 10.1049/el:19940856.

[33] C. L. Hsu and T.-C. Wu, "Authenticated encryption scheme with (t, n) shared verification," *IEE Proc. Comput. Digit. Techn.*, vol. 145, no. 2, pp. 117–120, Mar. 1998, doi: 10.1049/ip-cdt:19981905.

[34] K. Chen, "Authenticated encryption scheme based on quadratic residue," *Electron. Lett.*, vol. 34, no. 22, pp. 2115–2116, Oct. 1998, doi: 10.1049/el:19981408.

[35] J. H. An, "Authenticated encryption in the public-key setting: Security notions and analyses," Cryptol. ePrint Arch., Tech. Rep. 2003/069, Sep. 2001. [Online]. Available: https://eprint.iacr.org/2003/069

[36] F. Abed, C. Forler, and S. Lucks, "General classification of the authenticated encryption schemes for the CAESAR competition," *Comput. Sci. Rev.*, vol. 22, pp. 13–26, Nov. 2016, doi: 10.1016/j.cosrev.2016.07.002.

[37] E. B. Kavun, H. Mihajloska, and T. Yalçin, "A survey on authenticated encryption-ASIC designer's perspective," *ACM Comput. Surv.*, vol. 50, no. 6, pp. 1–21, Nov. 2018, doi: 10.1145/3131276.

[38] P. Rogaway, "Authenticated-encryption with associated-data," in *Proc. 9th ACM Conf. Comput. Commun. Secur. (CCS)*, 2002, pp. 98–107, doi: 10.1145/586110.586125.

[39] B. Zoltak. (2004). *VMPC-MAC: A Stream Cipher Based Authenticated Encryption Scheme*. Cryptology ePrint Archive. [Online]. Available: https://eprint.iacr.org/2004/301.pdf

[40] S. Cogliani, D. S. Maimut, D. Naccache, R. P. do Canto, R. Reyhanitabar, S. Vaudenay, and D. Vizár, "OMD: A compression function mode of operation for authenticated encryption," in *Selected Areas in Cryptography—SAC*. Cham, Switzerland: Springer, 2014, pp. 112–128.

[41] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche. (2011). *Duplexing the Sponge: Single-Pass Authenticated Encryption and Other Applications*. Cryptology ePrint Archive. [Online]. Available: https://eprint.iacr.org/2011/499.pdf.

[42] B. Bilgin, A. Bogdanov, M. Knežević, F. Mendel, and Q. Wang, "Fides: Lightweight authenticated cipher with side-channel resistance for constrained hardware," in *Cryptographic Hardware and Embedded Systems—CHES*. Berlin, Germany: Springer, 2013, pp. 142–158.

[43] N. Datta and M. Nandi, "ELmE: A misuse resistant parallel authenticated encryption," in *Information Security and Privacy*. Cham, Switzerland: Springer, 2014, pp. 306–321.

[44] P. Rogaway and T. Shrimpton. (2006). *Deterministic Authenticated-Encryption: A Provable-Security Treatment of the Key-Wrap Problem*. Cryptology ePrint Archive. [Online]. Available: https://eprint.iacr.org/2006/221.pdf

[45] D. J. Bernstein, "Failures of secret-key cryptography," in *Proc. 20th Int. Workshop-FSE*. Singapore, Mar. 2013.

[46] C. Competitions. *CAESAR: Competition for Authenticated Encryption: Security, Applicability, and Robustness*. Accessed: Feb. 17, 2021. [Online]. Available: https://competitions.cr.yp.to/caesar.html

[47] NIST. *Lightweight Cryptography*. NIST. Accessed: Dec. 4, 2020. [Online]. Available: https://www.nist.gov/programs-projects/lightweight-cryptography

[48] M. R. Z'aba, N. Jamil, M. S. Rohmad, H. A. Rani, and S. Shamsuddin. *The CiliPadi Family of Lightweight Authenticated Encryption Version 1.0*. NIST. Accessed: Sep. 22, 2020. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/cilipadi-spec.pdf

[49] D. Gligoroski, H. Mihajloska, and D. Otte. *GAGE and InGAGE v1.0*. NIST. Accessed: Mar. 19, 2020. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/GAGEandInGAGE-spec.pdf

[50] R. Avanzi, S. Banik, A. Bogdanov, O. Dunkelman, S. Huang, and F. Regazzoni. *Qameleon V. 1.0*. NIST. Accessed: Mar. 19, 2020. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/qameleon-spec.pdf

[51] C. Dobraunig, M. Eichlseder, F. Mendel, and M. Schläffer, *Ascon v1.2*. Gaithersburg, MD, USA: NIST, Mar. 2021.

[52] T. Beyne, Y. L. Chen, C. Dobraunig, and B. Mennink. *Elephant v1.1*. NIST. Accessed: Mar. 10, 2021. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/elephant-spec-round2.pdf
[53] S. Banik, *GIFT-COFB v1.0*. Gaithersburg, MD, USA: NIST, Mar. 2021.
[54] M. Hell, T. Johansson, W. Meier, J. Sönnerup, and H. Yoshida. *Grain-128AEAD—A Lightweight AEAD Stream Cipher*. NIST. Accessed: Mar. 10, 2021. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/grain-128aead-spec-round2.pdf
[55] C. Dobraunig. *ISAP v2.0*. NIST. Accessed: Mar. 10, 2021. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/isap-spec-round2.pdf
[56] Z. Bao. *PHOTON-Beetle Authenticated Encryption and Hash Family*. NIST. Accessed: Mar. 10, 2021. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/photon-beetle-spec-round2.pdf
[57] T. Iwata, M. Khairallah, K. Minematsu, and T. Peyrin. *Romulus v1.2*. NIST. Accessed: Mar. 10, 2021. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/Romulus-spec-round2.pdf
[58] C. Beierle. *Schwaemm and Esch: Lightweight Authenticated Encryption and Hashing Using The Sparkle Permutation Family*. NIST. Accessed: Mar. 10, 2021. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/sparkle-spec-round2.pdf
[59] H. Wu and T. Huang. *TinyJAMBU: A Family of Lightweight Authenticated Encryption Algorithms*. NIST. Accessed: Mar. 10, 2021. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/TinyJAMBU-spec-round2.pdf
[60] J. Daemen, S. Hoffert, M. Peeters, G. V. Assche, and R. V. Keer. *Xoodyak, a Lightweight Cryptographic Scheme*. NIST. Accessed: Mar. 10, 2021. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/Xoodyak-spec-round2.pdf
[61] J. Daemen and V. Rijmen, *The Design of Rijndael AES—The Advanced Encryption Standard*. Cham, Switzerland: Springer, 2002.
[62] C. Beierle, J. Jean, S. Kölbl, G. Leander, A. Moradi, T. Peyrin, Y. Sasaki, P. Sasdrich, and S. M. Sim, "The SKINNY family of block ciphers and its low-latency variant MANTIS," in *Advances in Cryptology—CRYPTO*. Berlin, Germany: Springer, 2016, pp. 123–153.
[63] S. Banik, S. K. Pandey, T. Peyrin, Y. Sasaki, S. M. Sim, and Y. Todo, "GIFT: A small present," in *Cryptographic Hardware and Embedded Systems (CHES)*. Cham, Switzerland: Springer, 2017, pp. 321–345.
[64] R. Tahir, M. Y. Javed, and A. R. Cheema, "Rabbit-MAC: Lightweight authenticated encryption in wireless sensor networks," in *Proc. Int. Conf. Inf. Autom.*, Jun. 2008, pp. 573–577, doi: 10.1109/ICINFA.2008.4608065. [Online]. Available: https://ieeexplore.ieee.org/document/4608065/https://ieeexplore.ieee.org/ielx5/4599584/4607950/04608065.pdf?tp=&arnumber=4608065&isnumber=4607950&ref=
[65] J. Alizadeh, M. R. Aref, and N. Bagheri. (2014). *JHAE: A Novel Permutation-Based Authenticated Encryption Mode Based on the Hash Mode JH*. Cryptology ePrint Archive. [Online]. Available: https://eprint.iacr.org/2014/193.pdf
[66] J. Alizadeh, M. R. Aref, and N. Bagheri. *Artemia v1*. Accessed: May 11, 2020. [Online]. Available: http://competitions.cr.yp.to/round1/artemiav1.pdf
[67] S. Harris, "The Enchilada authenticated ciphers, v1," CAESAR, NIST, Gaithersburg, MD, USA, Tech. Rep., May 2020.
[68] D. Engels, M.-J. O. Saarinen, P. Schweitzer, and E. M. Smith. (2011). *The Hummingbird-2 Lightweight Authenticated Encryption Algorithm*. Cryptology ePrint Archive. [Online]. Available: https://eprint.iacr.org/2011/126.pdf
[69] P. I. S. Pena and R. E. G. Torres, "Authenticated encryption based on finite automata cryptosystems," in *Proc. 13th Int. Conf. Electr. Eng., Comput. Sci. Autom. Control (CCE)*, Sep. 2016, pp. 1–6, doi: 10.1109/ICEEE.2016.7751254.
[70] X. Lu, Z. Ma, and D.-G. Feng, "A quantum authenticated encryption scheme," in *Proc. 7th Int. Conf. Signal Process.*, Sep. 2004, pp. 2306–2309, doi: 10.1109/ICOSP.2004.1442241.
[71] M. Bellare, A. Boldyreva, L. Knudsen, and C. Namprempre, "Online ciphers and the hash-CBC construction," in *Advances in Cryptology—CRYPTO*. Berlin, Germany: Springer, 2001, pp. 292–309.
[72] M. Bellare and P. Rogaway, "Introduction to modern cryptography," in *Introduction to Modern Cryptography: Department of Computer Science*. Davis, CA, USA: Kemper Hall of Engineering, University of California at Davis, 2005, ch. 4.
[73] J. Black. (2004). *The Ideal-Cipher Model, Revisited: An Uninstantiable Blockcipher-Based Hash Function*. Cryptology Eprint. [Online]. Available: https://eprint.iacr.org/2005/210.pdf
[74] S. Kamara. *Lectures 2+3: Provable Security*. Accessed: Nov. 11, 2021. [Online]. Available: https://cs.brown.edu/~seny/2950-v/
[75] M. Aagaard, R. AlTawy, G. Gong, K. Mandal, and R. Rohit. *ACE: An Authenticated Encryption and Hash Algorithm*. NIST. Accessed: Jan. 17, 2021. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/ace-spec-round2.pdf
[76] T. Shrimpton. (2004). *A Characterization of Authenticated-Encryption as a Form of Chosen-Ciphertext Security*. Cryptology ePrint Archive. [Online]. Available: https://eprint.iacr.org/2004/272.pdf
[77] C. Dobraunig. *ISAP v2.0*. NIST. Accessed: Mar. 10, 2021. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/isap-spec-round2.pdf
[78] B. Mennink. (2020). *Beyond Birthday Bound Secure Fresh Rekeying: Application to Authenticated Encryption*. Cryptology ePrint. [Online]. Available: https://eprint.iacr.org/2020/1082.pdf
[79] S. Mangard, E. Oswald, and T. Popp, *Power Analysis Attacks: Revealing the Secrets of Smart Cards (Power Analysis Attacks: Revealing the Secrets of Smart Cards)*. Boston, MA, USA: Springer, 2007.
[80] A. Duc, S. Faust, and F.-X. Standaert, "Making masking security proofs concrete," in *Advances in Cryptology—EUROCRYPT*. Berlin, Germany: Springer, 2015, pp. 401–429.
[81] Y. Ishai, A. Sahai, and D. Wagner, "Private circuits: Securing hardware against probing attacks," in *Advances in Cryptology—CRYPTO*. Berlin, Germany: Springer, 2003, pp. 463–481.
[82] M. Medwed, F.-X. Standaert, J. Großschädl, and F. Regazzoni, "Fresh re-keying: Security against side-channel and fault attacks for low-cost devices," in *Progress in Cryptology—AFRICACRYPT?*. Berlin, Germany: Springer, 2010, pp. 279–296.
[83] M. Abdalla and M. Bellare, "Increasing the lifetime of a key: A comparative analysis of the security of re-keying techniques," in *Advances in Cryptology—ASIACRYPT*. Berlin, Germany: Springer, 2000, pp. 546–559.
[84] S. Gueron and Y. Lindell. (2015). *GCM-SIV: Full Nonce Misuse-Resistant Authenticated Encryption at Under One Cycle per Byte*. Cryptology ePrint Archive [Online]. Available: https://eprint.iacr.org/2015/102.pdf
[85] N. Borisov, I. Goldberg, and D. Wagner, "Intercepting mobile communications: The insecurity of 802.11," in *Proc. 7th Annu. Int. Conf. Mobile Comput. Netw. (MobiCom)*, 2001, pp. 180–189, doi: 10.1145/381677.381695.
[86] T. Kohno, "Attacking and repairing the WinZip encryption scheme," in *Proc. 11th ACM Conf. Comput. Commun. Secur. (CCS)*, 2004, pp. 72–81, doi: 10.1145/1030083.1030095.
[87] H. Wu. (2005). *The Misuse of RC4 in Microsoft Word and Excel*. Cryptology ePrint. [Online]. Available: https://eprint.iacr.org/2005/007
[88] M. Vanhoef and F. Piessens, "Key reinstallation attacks: Forcing nonce reuse in WPA2," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2017, pp. 1313–1328, doi: 10.1145/3133956.3134027.
[89] E. Andreeva, A. Bogdanov, A. Luykx, B. Mennink, N. Mouha, and K. Yasuda. (2014). *How to Securely Release Unverified Plaintext in Authenticated Encryption*. Cryptology ePrint Archive 2014. [Online]. Available: https://eprint.iacr.org/2014/144.pdf
[90] D. Chang, N. Datta, A. Dutta, B. Mennink, M. Nandi, S. Sanadhya, and F. Sibleyras, "Release of unverified plaintext: Tight unified model and application to ANYDAE," *IACR Trans. Symmetric Cryptol.*, vol. 2019, no. 4, pp. 119–146, 2020, doi: 10.13154/tosc.v2019.i4.119-146.
[91] M. Agrawal, D. Chang, and S. Sanadhya. (2015). *A New Authenticated Encryption Technique for Handling Long Ciphertexts in Memory Constrained Devices*. Cryptology ePrint Archive. [Online]. Available: https://eprint.iacr.org/2015/331.pdf
[92] T. Iwata, "Authenticated encryption mode for beyond the birthday bound security," in *Cryptology—AFRICACRYPT*. Berlin, Germany: Springer, 2008, pp. 125–142.

[93] S. O'Neil and B. Gittins, "Authenticated encryption mode of VEST ciphers," *Cryptol. ePrint Arch.*, Nov. 2005. [Online]. Available: http://eprint.iacr.org/2005/414

[94] T. Iwata, K. Minematsu, J. Guo, and S. Morioka, "CLOC: Compact low-overhead CFB," Tech. Rep., 2017.

[95] P.-A. Fouque, A. Joux, G. Martinet, and F. Valette, "Authenticated on-line encryption," in *Selected Areas in Cryptography*. Berlin, Germany: Springer Berlin, 2004, pp. 145–159.

[96] A. Boldyreva and N. Taesombut, "Online encryption schemes: New security notions and constructions," in *Topics in Cryptology—CT-RSA*. Berlin, Germany: Springer, 2004, pp. 1–14.

[97] G. Bertoni, J. Daemen, M. Peeters, G. V. Assche, and R. V. Keer. Keyak v2. CAESAR, NIST, Gaithersburg, MD, USA. Accessed: Feb. 3, 2021. [Online]. Available: https://keccak.team/files/Keyakv2-doc2.2.pdf

[98] J.-P. Aumasson, P. Jovanovic, and S. Neves. *NORX v3*. NIST. Accessed: Feb. 3, 2021. [Online]. Available: http://competitions.cr.yp.to/round1/norxv1.pdf

[99] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche, "Duplexing the sponge: Single-pass authenticated encryption and other applications," in *Selected Areas in Cryptography*. Berlin, Germany: Springer, 2012, pp. 320–337.

[100] Y. Sasaki and K. Yasuda, "A new mode of operation for incremental authenticated encryption with associated data," in *Selected Areas in Cryptography—SAC*. Cham, Switzerland: Springer, 2015, pp. 397–416.

[101] M. Bellare, O. Goldreich, and S. Goldwasser, "Incremental cryptography and application to virus protection," in *Proc. 27th Annu. ACM Symp. Theory Comput. (STOC)*, 1995, pp. 45–56, doi: 10.1145/225058.225080.

[102] M. Bellare, O. Goldreich, and S. Goldwasser, "Incremental cryptography: The case of hashing and signing," in *Advances in Cryptology—CRYPTO*. Berlin, Germany: Springer, 1994, pp. 216–233.

[103] A. Boorghany, S. Bayat-Sarmadi, and R. Jalili. (2016). *Efficient Lattice-based Authenticated Encryption: A Practice-Oriented Provable Security Approach*. Cryptology ePrint Archive. [Online]. Available: https://eprint.iacr.org/2016/268.pdf

[104] R. Reyhanitabar, S. Vaudenay, and D. Vizár, "Authenticated encryption with variable stretch," in *Advances in Cryptology—ASIACRYPT*, J. H. Cheon and T. Takagi, Eds. Berlin, Germany: Springer, 2016, pp. 396–425.

[105] A. Chakraborti, A. Chattopadhyay, M. Hassan, and M. Nandi. (2015). *TriviA: A Fast and Secure Authenticated Encryption Scheme*. Cryptology ePrint Archive. [Online]. Available: https://eprint.iacr.org/2015/590.pdf

[106] E. Andreeva, B. Bilgin, A. Bogdanov, A. Luykx, B. Mennink, N. Mouha, and K. Yasuda. (2013). *APE: Authenticated Permutation-Based Encryption for Lightweight Cryptography*. Cryptology ePrint Archive. [Online]. Available: https://eprint.iacr.org/2013/791.pdf

[107] M. Agrawal, J. Zhou, and D. Chang, "A survey on lightweight authenticated encryption and challenges for securing industrial IoT," in *Security and Privacy Trends in the Industrial Internet of Things*, C. Alcaraz, Ed. Cham, Switzerland: Springer, 2019, pp. 71–94.

[108] F. Zhang, Z.-Y. Liang, B.-L. Yang, X.-J. Zhao, S.-Z. Guo, and K. Ren, "Survey of design and security evaluation of authenticated encryption algorithms in the CAESAR competition," *Frontiers Inf. Technol. Electron. Eng.*, vol. 19, no. 12, pp. 1475–1499, 2018, doi: 10.1631/FITEE.1800576.

[109] M. Bellare, P. Rogaway, and D. Wagner. (2003). *A Conventional Authenticated-Encryption Mode*. [Online]. Available: https://csrc.nist.gov/csrc/media/projects/block-cipher-techniques/documents/bcm/proposed-modes/eax/eax-spec.pdf

[110] N. Ferguson, D. Whiting, B. Schneier, J. Kelsey, S. Lucks, and T. Kohno, "Helix: Fast encryption and authentication in a single cryptographic primitive," in *Fast Software Encryption*. Berlin, Germany: Springer, 2003, pp. 330–346.

[111] S. Furuya and K. Sakurai, "Single-path authenticated-encryption scheme based on universal hashing," in *Selected Areas in Cryptography*. Berlin, Germany: Springer, 2003, pp. 94–109.

[112] T. Kohno, J. Viega, and D. Whiting. (2003). *CWC: A High-Performance Conventional Authenticated Encryption Mode*. Cryptology ePrint Archive. [Online]. Available: https://eprint.iacr.org/2003/106.pdf

[113] S. Lucks, "Two-pass authenticated encryption faster than generic composition," in *Fast Software Encryption*. Berlin, Germany: Springer, 2005, pp. 284–298.

[114] C. Castelluccia. (2006). *Authenticated Interleaved Encryption*. Cryptology ePrint Archive. [Online]. Available: https://eprint.iacr.org/2006/416.pdf

[115] Y. M. Y. Hasan, "Key-joined block ciphers with input-output pseudo-random shuffling applied to remotely keyed authenticated encryption," in *Proc. IEEE Int. Symp. Signal Process. Inf. Technol.*, Dec. 2007, pp. 74–79, doi: 10.1109/ISSPIT.2007.4458045. [Online]. Available: https://ieeexplore.ieee.org/document/4458045/https://ieeexplore.ieee.org/ielx5/4455349/4457988/04458045.pdf?tp=&arnumber=4458045&isnumber=4457988&ref=

[116] T. Krovetz, "Patent-free authenticated-encryption as fast As OCB," in *Innovative Algorithms and Techniques in Automation, Industrial Electronics and Telecommunications*. Dordrecht, The Netherlands: Springer, 2007, pp. 459–461.

[117] S. Y. Lim, C. C. Pu, H. T. Lim, and H. J. Lee. (2007). *Dragon-MAC: Securing Wireless Sensor Networks With Authenticated Encryption*. Cryptology ePrint Archive. [Online]. Available: https://eprint.iacr.org/2007/204.pdf

[118] T. Iwata and K. Yasuda, "BTM: A single-key, inverse-cipher-free mode for deterministic authenticated encryption," in *Selected Areas in Cryptography*. Berlin, Germany: Springer, 2009, pp. 313–330.

[119] T. Iwata and K. Yasuda, "HBS: A single-key mode of operation for deterministic authenticated encryption," in *Fast Software Encryption*. Berlin, Germany: Springer, 2009, pp. 394–415.

[120] P. Kumar, S. Cho, and H. J. Lee, "PingPong-MAC: Secure ubiquitous sensor network with authenticated encryption," in *Proc. 2nd Int. Conf. Interact. Sci. Inf. Technol., Culture Hum. (ICIS)*, 2009, pp. 256–260, doi: 10.1145/1655925.1655970.

[121] M. A. Simplicio, P. D. F. F. S. Barbuda, P. S. L. M. Barreto, T. C. M. B. Carvalho, and C. B. Margi, "The MARVIN message authentication code and the LETTERSOUP authenticated encryption scheme," *Secur. Commun. Netw.*, vol. 2, no. 2, pp. 165–180, Mar. 2009, doi: 10.1002/sec.66.

[122] A. A. Adekunle and S. R. Woodhead, "An efficient authenticated-encryption with associated-data block cipher mode for wireless sensor networks," in *Wired/Wireless Internet Communications*. Berlin, Germany: Springer, 2010, pp. 375–385.

[123] P. Sarkar, "A simple and generic construction of authenticated encryption with associated data," *ACM Trans. Inf. Syst. Secur.*, vol. 13, no. 4, pp. 1–16, Dec. 2010, doi: 10.1145/1880022.1880027.

[124] S. Zhang, G. Xing, and Y. Yang, "An efficient scheme of authenticated encryption with associated data," in *Proc. Chin. Control Decis. Conf.*, May 2010, pp. 4217–4221, doi: 10.1109/CCDC.2010.5498386.

[125] E. Fleischmann, C. Forler, S. Lucks, and J. Wenzel. (2011). *McOE: A Family of Almost Foolproof on-Line Authenticated Encryption Schemes*. Cryptology ePrint Archive. [Online]. Available: https://eprint.iacr.org/2011/644.pdf

[126] S. Trimberger, J. Moore, and W. Lu, "Authenticated encryption for FPGA bitstreams," in *Proc. 19th ACM/SIGDA Int. Symp. Field Program. Gate Arrays (FPGA)*, 2011, pp. 83–86, doi: 10.1145/1950413.1950432.

[127] A. A. Adekunle and S. R. Woodhead, "An AEAD cryptographic framework and TinyAEAD construct for secure WSN communication," in *Proc. Wireless Adv. (WiAd)*, Jun. 2012, pp. 1–5, doi: 10.1109/WiAd.2012.6296560. [Online]. Available: https://ieeexplore.ieee.org/document/6296560/https://ieeexplore.ieee.org/ielx5/6287113/6296540/06296560.pdf?tp=&arnumber=6296560&isnumber=6296540&ref=

[128] M. Bond, G. French, N. P. Smart, and G. J. Watson. (2012). *The Low-Call Diet: Authenticated Encryption for Call Counting HSM Users*. Cryptology ePrint Archive. [Online]. Available: https://eprint.iacr.org/2012/497.pdf

[129] G. Jakimoski and S. Khajuria, "ASC-1: An authenticated encryption stream cipher," in *Selected Areas in Cryptography*. Berlin, Germany: Springer, 2012, pp. 356–372.

[130] T.-C. Chen, "An authenticated encryption scheme for automatic dependent surveillance-broadcast data link," in *Proc. CSQRWC*, Jul. 2012, pp. 127–131, doi: 10.1109/CSQRWC.2012.6294960.

[131] E. Andreeva, A. Bogdanov, A. Luykx, B. Mennink, E. Tischhauser, and K. Yasuda. (2013). *Parallelizable and Authenticated Online Ciphers*. Cryptology ePrint Archive. [Online]. Available: https://eprint.iacr.org/2013/790.pdf

[132] Z. Jeddi, E. Amini, and M. Bayoumi, "A novel authenticated encryption algorithm for RFID systems," in *Proc. Euromicro Conf. Digit. Syst. Design*, Sep. 2013, pp. 658–661, doi: 10.1109/DSD.2013.117.

[133] K. Minematsu. (2013). *Parallelizable Rate-1 Authenticated Encryption From Pseudorandom Functions*. Cryptology ePrint Archive. [Online]. Available: https://eprint.iacr.org/2013/628.pdf

[134] P. Morawiecki and J. Pieprzyk. (2013). *Parallel Authenticated Encryption With the Duplex Construction*. Cryptology ePrint Archive. [Online]. Available: https://eprint.iacr.org/2013/658.pdf

[135] M.-J. O. Saarinen. (2013). *CBEAM: Efficient Authenticated Encryption From Feebly One-Way ϕ Functions*. Cryptology ePrint Archive. [Online]. Available: https://eprint.iacr.org/2013/773.pdf.

[136] J. Trostle. (2013). *CMCC: Misuse Resistant Authenticated Encryption With Minimal Ciphertext Expansion*. Cryptology ePrint Archive. [Online]. Available: https://eprint.iacr.org/2013/269.pdf

[137] A. Biryukov and D. Khovratovich, *PAEQ: Parallelizable Permutation-Based Authenticated Encryption*. Cham, Switzerland: Springer, 2014, pp. 72–89.

[138] D. Gligoroski, H. Mihajloska, S. Samardjiska, H. Jacobsen, R. E. Jensen, and M. El-Hadedy, "π-cipher: Authenticated encryption for big data," in *Secure IT Systems*. K. Bernsmed and S. Fischer-Hübner, Eds. Cham, Switzerland: Springer, 2014, pp. 110–128.

[139] P. L. Morawiecki, K. Gaj, E. Homsirikamol, K. Matusiewicz, J. Pieprzyk, M. Rogawski, M. Srebrny, and M. Wójcik. (2014). *ICEPOLE: High-Speed, Hardware-Oriented Authenticated Encryption*. Cryptology ePrint Archive. [Online]. Available: https://eprint.iacr.org/2014/266.pdf

[140] V. T. Hoang, R. Reyhanitabar, P. Rogaway, and D. Vizár. (2015). *Online Authenticated-Encryption and its Nonce-Reuse Misuse-Resistance*. Cryptology ePrint Archive. [Online]. Available: https://eprint.iacr.org/2015/189.pdf

[141] M. Kelly, A. Kaminsky, M. Kurdziel, M. Lukowiak, and S. Radziszowski, "Customizable sponge-based authenticated encryption using 16-bit S-boxes," in *Proc. MILCOM IEEE Mil. Commun. Conf.*, Oct. 2015, pp. 43–48, doi: 10.1109/MILCOM.2015.7357416.

[142] K. Minematsu. (2015). *Authenticated Encryption With Small Stretch (or, How to Accelerate AERO)*. Cryptology ePrint Archive. [Online]. Available: https://eprint.iacr.org/2015/738.pdf

[143] T. Peyrin and Y. Seurin. (2015). *Counter-in-Tweak: Authenticated Encryption Modes for Tweakable Block Ciphers*. Cryptology ePrint Archive. [Online]. Available: https://eprint.iacr.org/2015/1049.pdf

[144] F. Abed, C. Forler, E. List, S. Lucks, and J. Wenzel, "RIV for robust authenticated encryption," in *Fast Software Encryption*, T. Peyrin, Ed. Berlin, Germany: Springer, 2016, pp. 23–42.

[145] M. Bellare and B. Tackmann. (2016). *The Multi-User Security of Authenticated Encryption: AES-GCM in TLS 1.3*. Cryptology ePrint Archive. [Online]. Available: https://eprint.iacr.org/2016/564.pdf

[146] F. Berti, F. C. Koeune, O. Pereira, T. Peters, and F. C.-X. Standaert. (2016). *Leakage-Resilient and Misuse-Resistant Authenticated Encryption*. Cryptology ePrint Archive. [Online]. Available: https://eprint.iacr.org/2016/996.pdf

[147] L. Bossuet, N. Datta, C. Mancillas-López, and M. Nandi, "ELmD: A pipelineable authenticated encryption and its hardware implementation," *IEEE Trans. Comput.*, vol. 65, no. 11, pp. 3318–3331, Nov. 2016, doi: 10.1109/TC.2016.2529618.

[148] C. Dobraunig, M. Eichlseder, S. Mangard, F. Mendel, and T. Unterluggauer. (2016). *ISAP—Towards Side-Channel Secure Authenticated Encryption*. Cryptology ePrint Archive. [Online]. Available: https://eprint.iacr.org/2016/952.pdf

[149] C. Forler, E. List, S. Lucks, and J. Wenzel. (2016). *Efficient Beyond-Birthday-Bound-Secure Deterministic Authenticated Encryption With Minimal Stretch*. Cryptology ePrint Archive. [Online]. Available: https://eprint.iacr.org/2016/395.pdf

[150] E. List and M. Nandi. (2016). *Revisiting Full-PRF-Secure PMAC and Using it for Beyond-Birthday Authenticated Encryption*. Cryptology ePrint Archive. [Online]. Available: https://eprint.iacr.org/2016/1174.pdf

[151] A. S. Bhandari and D. R. Chowdhury. (2017). *ZETA: Towards Tagless Authenticated Encryption*. Cryptology ePrint Archive. [Online]. Available: https://eprint.iacr.org/2017/205.pdf

[152] P. Grubbs, J. Lu, and T. Ristenpart. (2017). *Message Franking Via Committing Authenticated Encryption*. Cryptology ePrint Archive. [Online]. Available: https://eprint.iacr.org/2017/664.pdf

[153] M. N. Hussein, M. H. Megahed, and M. H. A. Azeem, "Design and simulation of authenticated encryption AENOTP stream cipher algorithm," in *Proc. 13th Int. Comput. Eng. Conf. (ICENCO)*, Dec. 2017, pp. 393–398, doi: 10.1109/ICENCO.2017.8289821.

[154] Y. Naito. (2017). *Tweakable Blockciphers for Efficient Authenticated Encryptions With Beyond the Birthday-Bound Security*. Cryptology ePrint Archive. [Online]. Available: https://eprint.iacr.org/2017/466.pdf

[155] M. Barbosa and P. Farshim. (2018). *Indifferentiable Authenticated Encryption*. Cryptology ePrint Archive. [Online]. Available: https://eprint.iacr.org/2018/547.pdf

[156] A. Chakraborti, N. Datta, M. Nandi, and K. Yasuda. (2018). *Beetle Family of Lightweight and Secure Authenticated Encryption Ciphers*. Cryptology ePrint Archive 2018. [Online]. Available: https://eprint.iacr.org/2018/805.pdf

[157] J. H. Cheon, K. Han, S. M. Hong, H. J. Kim, J. Kim, S. Kim, H. Seo, H. Shim, and Y. Song, "Toward a secure drone system: Flying with real-time homomorphic authenticated encryption," *IEEE Access*, vol. 6, pp. 24325–24339, 2018, doi: 10.1109/ACCESS.2018.2819189.

[158] C. Jutla. (2018). *Authenticated Encryption Mode IAPM using SHA-3's Public Random Permutation*. Cryptology ePrint Archive. [Online]. Available: https://eprint.iacr.org/2018/128.pdf

[159] S. Kandele and S. Paul. (2018). *Key Assignment Scheme With Authenticated Encryption*. Cryptology ePrint Archive. [Online]. Available: https://eprint.iacr.org/2018/1233.pdf

[160] Y. Naito, M. Matsui, T. Sugawara, and D. Suzuki, "SAEB: A lightweight blockcipher-based AEAD mode of operation," *IACR Trans. Cryptograph. Hardw. Embedded Syst.*, vol. 2018, no. 2, pp. 192–217, May 2018, doi: 10.13154/tches.v2018.i2.192-217.

[161] R. Neethu, M. Sindhu, and C. Srinivasan, "XUBA: An authenticated encryption scheme," in *Data Engineering and Intelligent Computing*, S. C. Satapathy, V. Bhateja, K. S. Raju, and B. Janakiramaiah, Eds. Singapore: Springer, 2018, pp. 647–655.

[162] P. Zhang, H. Hu, and P. Wang, "Efficient beyond-birthday-bound secure authenticated encryption modes," *Sci. China Inf. Sci.*, vol. 61, no. 9, Sep. 2018, Art. no. 098104, doi: 10.1007/s11432-017-9253-9.

[163] Q. Zheng, X. Wang, M. K. Khan, W. Zhang, B. B. Gupta, and W. Guo, "A lightweight authenticated encryption scheme based on chaotic SCML for railway cloud service," *IEEE Access*, vol. 6, pp. 711–722, 2018, doi: 10.1109/ACCESS.2017.2775038.

[164] E. Andreeva, V. Lallemand, A. Purnal, R. Reyhanitabar, A. Roy, and D. Vizar, "Forkcipher: A new primitive for authenticated encryption of very short messages," Cryptol. ePrint Arch., Tech. Rep. 2019/1004, Sep. 2019. [Online]. Available: https://eprint.iacr.org/2019/1004

[165] Z. Bao, J. Guo, T. Iwata, and K. Minematsu. (2019). *ZOCB and ZOTR: Tweakable Blockcipher Modes for Authenticated Encryption With Full Absorption*. Cryptology ePrint Archive. [Online]. Available: https://eprint.iacr.org/2019/600.pdf

[166] F. Berti, C. Guo, O. Pereira, T. Peters, and F.-X. Standaert. (2019). *TEDT, a Leakage-Resilient AEAD Mode for High (Physical) Security Applications*. Cryptology ePrint Archive. [Online]. Available: https://eprint.iacr.org/2019/137.pdf

[167] G. Cassiers, C. Guo, O. Pereira, T. Peters, and F.-X. Standaert. (2019). *SpookChain: Chaining a Sponge-Based AEAD With Beyond-Birthday Security*. Cham, Switzerland: Springer, 2019, pp. 67–85.

[168] A. Chakraborti, T. Iwata, K. Minematsu, and M. Nandi, "Blockcipher-based authenticated encryption: How small can we go?" *J. Cryptol.*, vol. 33, no. 3, pp. 703–741, Jul. 2020, doi: 10.1007/s00145-019-09325-z.

[169] J. P. Degabriele, C. Janson, and P. Struck. (2019). *Sponges Resist Leakage: The Case of Authenticated Encryption*. Cryptology ePrint Archive. [Online]. Available: https://eprint.iacr.org/2019/1034.pdf

[170] S. Gueron and Y. Lindell. (2019). *SimpleENC and SimpleENCsmall—An Authenticated Encryption Mode for the Lightweight Setting*. Cryptology ePrint Archive. [Online]. Available: https://eprint.iacr.org/2019/712.pdf

[171] C. Guo, O. Pereira, T. Peters, and F. C.-X. Standaert. (2019). *Towards Low-Energy Leakage-Resistant Authenticated Encryption From the Duplex Sponge Construction*. Cryptology ePrint Archive. [Online]. Available: https://eprint.iacr.org/2019/193.pdf

[172] M. Hell, T. Johansson, W. Meier, J. Sönnerup, and H. Yoshida, "An AEAD variant of the grain stream cipher," in *Codes, Cryptology and Information Security*. Cham, Switzerland: Springer, 2019, pp. 55–71.

[173] P. Kresmer and A. Zeh. (2019). *CCM-SIV: Single-PRF Nonce-Misuse-Resistant Authenticated Encryption*. Cryptology ePrint Archive. [Online]. Available: https://eprint.iacr.org/2019/892.pdf

[174] Y. Naito, "Improved XKX-based AEAD scheme: Removing the birthday terms," in *Progress in Cryptology—LATINCRYPT*. Cham, Switzerland: Springer, 2017, pp. 228–246.

[175] Y. Naito, M. Matsui, T. Sugawara, and D. Suzuki. (2019). *SAEB: A Lightweight Blockcipher-Based AEAD Mode of Operation*. Cryptology ePrint Archive. [Online]. Available: https://eprint.iacr.org/2019/700.pdf

[176] Y. Naito and T. Sugawara. (2019). *Lightweight Authenticated Encryption Mode of Operation for Tweakable Block Ciphers*. Cryptology ePrint Archive. [Online]. Available: https://eprint.iacr.org/2019/339.pdf

[177] T. Iwata, M. Khairallah, K. Minematsu, and T. Peyrin. (2019). *Duel of the Titans: The Romulus and Remus Families of Lightweight AEAD Algorithms*. Cryptology ePrint Archive. [Online]. Available: https://eprint.iacr.org/2019/992.pdf

[178] R. AlTawy, G. Gong, K. Mandal, and R. Rohit. (2020). *WAGE: An Authenticated Encryption With a Twist*. Cryptology ePrint. [Online]. Available: https://eprint.iacr.org/2020/435.pdf

[179] R. Bhaumik. (2020). *QCB: Efficient Quantum-Secure Authenticated Encryption*. Cryptology ePrint. [Online]. Available: https://eprint.iacr.org/2020/1304.pdf

[180] T. R. Campbell. (2020). *Daence: Salsa20 and ChaCha in Deterministic Authenticated Encryption With, no noNCEnse*. Cryptology ePrint. [Online]. Available: https://eprint.iacr.org/2020/067.pdf.

[181] S. Hussain, S. Farooq, and T. S. Ustun, "A method for achieving confidentiality and integrity in IEC 61850 GOOSE messages," *IEEE Trans. Power Del.*, vol. 35, no. 5, pp. 2565–2567, Oct. 2020, doi: 10.1109/TPWRD.2020.2990760.

[182] J. Krämer and P. Struck. (2020). *Leakage-Resilient Authenticated Encryption From Leakage-Resilient Pseudorandom Functions*. Cryptology ePrint. [Online]. Available: https://eprint.iacr.org/2020/280.pdf.

[183] U. Naito, Y. Sasaki, and T. Sugawara. (2020). *Lightweight Authenticated Encryption Mode Suitable for Threshold Implementation*. Cryptology ePrint. [Online]. Available: https://eprint.iacr.org/2020/542.pdf

[184] N. D. Nguyen, D. H. Bui, and X. T. Tran, "A Lightweight AEAD encryption core to secure IoT applications," in *Proc. IEEE Asia Pacific Conf. Circuits Syst. (APCCAS)*, Dec. 2020, pp. 35–38, doi: 10.1109/APCCAS50809.2020.9301683. [Online]. Available: https://ieeexplore.ieee.org/document/9301683/

[185] T. Simon, L. Batina, J. Daemen, V. Grosso, P. M. Massolino, K. Papagiannopoulos, F. Regazzoni, and N. Samwel. (2020). *Friet: An Authenticated Encryption Scheme With Built-in Fault Detection*. Cryptology ePrint. [Online]. Available: https://eprint.iacr.org/2020/425.pdf

[186] G. Bertoni, J. Daemen, M. Peeters, G. V. Assche, and R. V. Keer. *KETJE v2*. Accessed: Feb. 3, 2021. [Online]. Available: http://competitions.cr.yp.to/round1/ketjev11.pdf

[187] T. Iwata, K. Minematsu, J. Guo, S. Morioka, and E. Kobayashi. *CLOC and SILC*. NIST. Accessed: Feb. 3, 2021. [Online]. Available: http://competitions.cr.yp.to/round3/clocsilcv3.pdf

[188] K. Minematsu. *AES-OTR v3.1*. Accessed: Jan. 14, 2021. [Online]. Available: http://competitions.cr.yp.to/round1/aesotrv1.pdf

[189] I. Nikolić. *Tiaoxin 346 v.2.1*. Accessed: Jan. 14, 2021. [Online]. Available: http://competitions.cr.yp.to/round1/tiaoxinv1.pdf

[190] H. Wu and T. Huang. *The JAMBU Lightweight Authentication Encryption Mode (v2.1)*. Accessed: Jan. 14, 2021. [Online]. Available: http://competitions.cr.yp.to/round1/aesjambuv1.pdf

[191] H. Wu and T. Huang. *The Authenticated Cipher MORUS (v2)*. Accessed: Jan. 14, 2021. [Online]. Available: http://competitions.cr.yp.to/round1/morusv1.pdf

[192] V. T. Hoang, T. Krovetz, and P. Rogaway. *AEZ v5: Authenticated Encryption by Enciphering*. Accessed: Jan. 14, 2021. [Online]. Available: https://web.cs.ucdavis.edu/~rogaway/aez/aez.pdf

[193] F. Abed. *The POET Family of on-Line Authenticated Encryption Schemes*. Accessed: Aug. 12, 2020. [Online]. Available: http://competitions.cr.yp.to/round1/poetv101.pdf

[194] E. Andreeva. *PRIMATEs v1*. Accessed: Aug. 12, 2020. [Online]. Available: http://competitions.cr.yp.to/round1/primatesv1.pdf

[195] A. Biryukov and D. Khovratovich. *PAEQ v1*. Accessed: Aug. 12, 2020. [Online]. Available: http://competitions.cr.yp.to/round1/paeqv1.pdf

[196] A. Chakraborti and M. Nandi. *TriviA-ck-v1*. Accessed: Aug. 12, 2020. [Online]. Available: http://competitions.cr.yp.to/round1/triviackv1.pdf

[197] S. Cogliani. *Offset Merkle-Damgård (OMD) Version 1.0*. NIST. Accessed: Aug. 12, 2020. [Online]. Available: http://competitions.cr.yp.to/round1/omdv10.pdf

[198] D. Gligoroski, H. Mihajloska, S. Samardjiska, H. Jacobsen, M. El-Hadedy, and R. E. Jensen. *π-Cipher v11*. NIST. Accessed: Aug. 12, 2020. [Online]. Available: http://competitions.cr.yp.to/round1/picipherv1.pdf

[199] V. Grosso. *SCREAM & iSCREAM Side-Channel Resistant Authenticated Encryption With Masking*. Accessed: Aug. 12, 2020. [Online]. Available: http://competitions.cr.yp.to/round1/screamv1.pdf

[200] J. Jean, I. Nikolić, and T. Peyrin. *Joltik v1*. Accessed: Aug. 12, 2020. [Online]. Available: http://competitions.cr.yp.to/round1/joltikv1.pdf

[201] T. Krovetz. *HS1-SIV (Draft v2)*. Accessed: Jan. 17, 2021. [Online]. Available: http://competitions.cr.yp.to/round1/hs1siv-nh.pdf

[202] P. Morawiecki. *ICEPOLE v1*. Accessed: Jan. 17, 2021. [Online]. Available: http://competitions.cr.yp.to/round1/icepolev1.pdf

[203] M.-J. O. Saarinen. *The STRIBOBr1 Authenticated Encryption Algorithm*. Accessed: Jan. 17, 2021. [Online]. Available: http://competitions.cr.yp.to/round1/stribobr1.pdf

[204] U. Sasaki. *Minalpher v1*. Accessed: Jan. 17, 2021. [Online]. Available: http://competitions.cr.yp.to/round1/minalpherv1.pdf

[205] L. Wang. *SHELL v1.1*. Accessed: Jan. 17, 2021. [Online]. Available: http://competitions.cr.yp.to/round1/shell-corr.pdf

[206] B. Alomair. *AVALANCHEv1*. Accessed: May 11, 2020. [Online]. Available: http://competitions.cr.yp.to/round1/avalanchev1.pdf

[207] E. Andreeva. *AES-COBRA v1*. Accessed: May 11, 2020. [Online]. Available: http://competitions.cr.yp.to/round1/aescobrav1.pdf

[208] L. Bahack. *Julius: Secure Mode of Operation for Authenticated Encryption Based on ECB and Finite Field Multiplications*. Accessed: May 11, 2020. [Online]. Available: http://competitions.cr.yp.to/round1/julius-addendum.pdf

[209] A. Bosselaers and F. Vercauteren. *YAES v1*. Accessed: May 11, 2020. [Online]. Available: http://competitions.cr.yp.to/round1/yaesv1.pdf

[210] F. Chaza, C. McDonald, and R. Avanzi. *FASER v1 Authenticated Encryption in a Feedback Shift Register*. Accessed: May 11, 2020. [Online]. Available: http://competitions.cr.yp.to/round1/faserv1.pdf

[211] J. Guo. *Marble Specification Version 1.1*. Accessed: May 11, 2020. [Online]. Available: http://competitions.cr.yp.to/round1/marblev11.pdf

[212] M. Henricksen, S. Kiyomoto, and J. Lu. *The HKC Authenticated Stream Cipher (Ver.1)*. Accessed: May 20, 2020. [Online]. Available: http://competitions.cr.yp.to/round1/hkcv1.pdf

[213] H. Hosseini and S. Khazaei. *CBA Mode (v1)*. Accessed: May 20, 2020. [Online]. Available: http://competitions.cr.yp.to/round1/cbav1.pdf

[214] J. Jean, I. Nikolić, and T. Peyrin. *KIASU v1*. Accessed: May 20, 2020. [Online]. Available: http://competitions.cr.yp.to/round1/kiasuv1.pdf

[215] E. B. Kavun, M. M. Lauridsen, G. Leander, C. Rechberger, P. Schwabe, and T. Yalçın. *Prøst v1.1*. Accessed: May 20, 2020. [Online]. Available: http://proest.compute.dtu.dk/proestv11.pdf

[216] W. Ladd. *Mcmambo V1: A New Kind of Latin DanCE*. Accessed: May 20, 2020. [Online]. Available: http://competitions.cr.yp.to/round1/mcmambov1.pdf

[217] W. W. Lei Zhang, Y. Wang, S. Wu, and J. Zhang. *LAC: A Lightweight Authenticated Encryption Cipher*. Accessed: May 20, 2020. [Online]. Available: http://competitions.cr.yp.to/round1/lacv1.pdf

[218] P. Maxwell. *Wheesht: An AEAD Stream Cipher*. Accessed: May 20, 2020. [Online]. Available: http://competitions.cr.yp.to/round1/wheeshtv03.pdf

[219] M. Montes and D. Penazzi. *AES-CPFB v1*. Accessed: May 20, 2020. [Online]. Available: http://competitions.cr.yp.to/round1/aescpfbv1.pdf

[220] D. Penazzi and M. Montes. *Silver v.1*. Accessed: May 12, 2020. [Online]. Available: http://competitions.cr.yp.to/round1/silverv1.pdf

[221] F. Recacha. *++AE v1.0*. Accessed: May 12, 2020. [Online]. Available: http://competitions.cr.yp.to/round1/aev10.pdf

[222] M.-J. O. Saarinen. *The CBEAMr1 Authenticated Encryption Algorithm*. Accessed: May 12, 2020. [Online]. Available: http://competitions.cr.yp.to/round1/cbeamr1.pdf

[223] C. Taylor. *The Calico Family of Authenticated Ciphers Version 8*. Accessed: May 12, 2020. [Online]. Available: http://competitions.cr.yp.to/round1/calicov8.pdf

[224] J. Trostle. *AES-CMCC v1*. Accessed: May 12, 2020. [Online]. Available: http://competitions.cr.yp.to/round1/aescmccv1.pdf

[225] R. Vuckovac. *Raviyoyla v1*. Accessed: May 12, 2020. [Online]. Available: http://competitions.cr.yp.to/round1/raviyoylav1.pdf

[226] A. Wysokinski and I. Sikora. *POLAWIS*. Accessed: May 12, 2020. [Online]. Available: http://competitions.cr.yp.to/round1/polawisv1.pdf

[227] D. Ye. *PAES v1: Parallelizable Authenticated Encryption Schemes based on AES Round Function*. Accessed: May 12, 2020. [Online]. Available: http://competitions.cr.yp.to/round1/paesv1.pdf

[228] D. Ye. *PANDA v1*. Accessed: May 12, 2020. [Online]. Available: http://competitions.cr.yp.to/round1/pandav1.pdf

[229] B. Zhang, Z. Shi, C. Xu, Y. Yao, and Z. Li. *Sablier v1*. Accessed: May 12, 2020. [Online]. Available: http://competitions.cr.yp.to/round1/sablierv1.pdf

[230] L. Zhang, W. Wu, H. Sui, and P. Wang. *iFeed[AES] v1*. Accessed: May 12, 2020. [Online]. Available: http://competitions.cr.yp.to/round1/ifeedaesv1.pdf
[231] M. Aagaard, R. AlTawy, G. Gong, K. Mandal, and R. Rohit. *ACE: An Authenticated Encryption and Hash Algorithm*. NIST. Accessed: Jan. 17, 2021. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/ace-spec-round2.pdf
[232] M. Aagaard, R. AlTawy, G. Gong, K. Mandal, R. Rohit, and N. Zidaric. *WAGE: An Authenticated Cipher Submission to the NIST LWC Competition*. NIST. Accessed: Feb. 11, 2021. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/wage-spec-round2.pdf
[233] R. AlTawy. *SpoC: An Authenticated Cipher Submission to the NIST LWC Competition*. NIST. Accessed: Feb. 11, 2021. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/spoc-spec-round2.pdf
[234] R. AlTawy, G. Gong, M. He, K. Mandal, and R. Rohit. *Spix: An Authenticated Cipher Submission to the NIST LWC Competition*. NIST. Accessed: Feb. 11, 2021. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/spix-spec-round2.pdf
[235] E. Andreeva, V. Lallemand, A. Purnal, R. Reyhanitabar, A. Roy, and D. Vizár. *ForkAE v.1*. NIST. Accessed: Jan. 17, 2021. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/forkae-spec-round2.pdf
[236] A. Chakraborti, N. Datta, A. Jha, C. M. Lopez, M. Nandi, and Y. Sasaki. *LOTUS-AEAD and LOCUS-AEAD*. NIST. Accessed: Jan. 17, 2021. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/lotus-locus-spec-round2.pdf
[237] S. Banik. *SUNDAE-GIFT v1.0*. NIST. Accessed: Feb. 11, 2021. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/SUNDAE-GIFT-spec-round2.pdf
[238] S. Banik, *GIFT-COFB v1.0*. Gaithersburg, MD, USA: NIST, Jan. 2021.
[239] Z. Bao. *PHOTON-Beetle Authenticated Encryption and Hash Family*. NIST. Accessed: Jan. 17, 2021. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/photon-beetle-spec-round2.pdf
[240] C. Beierle, A. Biryukov, L. C. dos Santos, J. Großschaädl, L. Perrin, A. Udovenko, V. Velichkov, Q. Wang, and A. Biryukov. *Schwaemm and Esch: Lightweight Authenticated Encryption and Hashing Using the Sparkle Permutation Family*. NIST. Accessed: Feb. 11, 2021. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/sparkle-spec-round2.pdf
[241] C. Beierle. *SKINNY-AEAD and SKINNY-Hash v1.1*. NIST. Accessed: Feb. 11, 2021. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/SKINNY-spec-round2.pdf
[242] D. Bellizia. *Spook: Sponge-Based Leakage-Resistant Authenticated Encryption With a Masked Tweakable Block Cipher*. NIST. Accessed: Feb. 11, 2021. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/Spook-spec-round2.pdf
[243] D. J. Bernstein. *Gimli*. NIST. Accessed: Jan. 17, 2021. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/gimli-spec-round2.pdf
[244] T. Beyne, Y. L. Chen, C. Dobraunig, and B. Mennink. *Elephant v1.1*. NIST. Accessed: Jan. 17, 2021. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/elephant-spec-round2.pdf
[245] A. Bhattacharjee, E. List, C. M. López, and M. Nandi. *The Oribatida Family of Lightweight Authenticated Encryption Schemes*. NIST. Accessed: Jan. 17, 2021. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/oribatida-spec-round2.pdf
[246] A. Canteaut. *Saturnin—A Suite of Lightweight Symmetric Algorithms for Post-Quantum Security*. NIST. Accessed: Feb. 11, 2021. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/saturnin-spec-round2.pdf
[247] A. Chakraborti, N. Datta, A. Jha, C. M. Lopez, M. Nandi, and Y. Sasaki. *ESTATE*. Accessed: Jan. 17, 2021. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/estate-spec-round2.pdf
[248] A. Chakraborti, N. Datta, A. Jha, and M. Nandi. *HyENA*. NIST. Accessed: Jan. 17, 2021. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/hyena-spec-round2.pdf
[249] B. Chakraborty and M. Nandi. *mixFeed*. NIST. Accessed: Jan. 17, 2021. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/mixFeed-spec-round2.pdf
[250] B. Chakraborty and M. Nandi. *ORANGE*. Accessed: Jan. 17, 2021. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/orange-spec-round2.pdf
[251] J. Daemen, S. Hoffert, M. Peeters, G. V. Assche, and R. V. Keer. *Xoodyak, a Lightweight Cryptographic Scheme*. NIST. Accessed: Feb. 11, 2021. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/Xoodyak-spec-round2.pdf
[252] J. Daemen, P. M. C. Massolino, and Y. Rotella. *The Subterranean 2.0 Cipher Suite*. NIST. Accessed: Feb. 11, 2021. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/subterranean-spec-round2.pdf
[253] C. Dobraunig. *ISAP v2.0*. NIST. Accessed: Jan. 17, 2021. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/isap-spec-round2.pdf
[254] C. Dobraunig, M. Eichlseder, F. Mendel, and M. Schläffer, "Ascon v1.2," CAESAR, NIST, Gaithersburg, MD, USA, Tech. Rep., Jan. 2021.
[255] D. Goudarzi. *Pyjamask v1.0*. NIST. Accessed: Jan. 17, 2021. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/pyjamask-spec-round2.pdf
[256] S. Gueron, A. Jha, and M. Nandi. *COMET: COunter Mode Encryption With Authentication Tag*. Accessed: Jan. 17, 2021. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/comet-spec-round2.pdf
[257] M. Hell, T. Johansson, W. Meier, J. Sönnerup, and H. Yoshida. *Grain-128AEAD—A Lightweight AEAD Stream Cipher*. NIST. Accessed: Jan. 17, 2021. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/grain-128aead-spec-round2.pdf
[258] T. Iwata, M. Khairallah, K. Minematsu, and T. Peyrin. *Romulus v1.2*. NIST. Accessed: Jan. 17, 2021. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/Romulus-spec-round2.pdf
[259] Y. Naito, M. Matsui, Y. Sakai, D. Suzuki, K. Sakiyama, and T. Sugawara. *SAEAES*. NIST. Accessed: Feb. 3, 2021. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/SAEAES-spec-round2.pdf
[260] H. Wu and T. Huang. *TinyJAMBU: A Family of Lightweight Authenticated Encryption Algorithms*. NIST. Accessed: Feb. 11, 2021. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/TinyJAMBU-spec-round2.pdf
[261] W. Zhang. *KNOT-Algorithm Specifications and Supporting Document*. NIST. Accessed: Jan. 17, 2021. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/lightweight-cryptography/documents/round-2/spec-doc-rnd2/knot-spec-round.pdf
[262] A. Adomnicai. *Lilliput-AE: A New Lightweight Tweakable Block Cipher for Authenticated Encryption With Associated Data*. NIST. Accessed: Mar. 19, 2020. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/LILLIPUT-AE-spec.pdf
[263] S. Banik, T. Isobe, W. Meier, Y. Todo, and B. Zhang. *TRIAD v1—A Lightweight AEAD and Hash Function Based on Stream Cipher*. NIST. Accessed: Mar. 19, 2020. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/TRIAD-spec.pdf

[264] Z. Bao, J. Guo, T. Iwata, and L. Song. *SIV-Rijndael256 Authenticated Encryption and Hash Family*. NIST. Accessed: Mar. 19, 2020. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/SIV-Rijndael256-Spec.pdf

[265] Z. Bao, J. Guo, T. Iwata, and L. Song. *SIV-TEM-PHOTON Authenticated Encryption and Hash Family*. NIST. Accessed: Mar. 19, 2020. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/SIV-TEM-PHOTON-Spec.pdf

[266] N. Datta, A. Ghoshal, D. Mukhopadhyay, S. Patranabis, S. Picek, and R. Sadhukhan. *TRIFLE*. NIST. Accessed: Mar. 19, 2020. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/trifle-spec.pdf

[267] K. R. Driscoll. *Bleep64*. NIST. Accessed: Mar. 19, 2020. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/Bleep64-spec.pdf

[268] S. Gueron and Y. Lindell. *Simple: A Simple AEAD Scheme*. NIST. Accessed: Mar. 28, 2020. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/Simple-spec.pdf

[269] T. Iwata, M. Khairallah, K. Minematsu, and T. Peyrin. *Remus v1.0*. NIST. Accessed: Mar. 28, 2020. [Online]. Available: https://csrc.nist.gov/x CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/Remus-spec.pdf

[270] T. Iwata. *Thank Goodness it's Friday (TGIF) v1.0*. NIST. Accessed: Mar. 28, 2020. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/TGIF-spec.pdf

[271] D. Liu, S. Nepal, J. Pieprzyk, and W. Susilo. *CLAE*. NIST. Accessed: Mar. 28, 2020. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/clae-spec.pdf

[272] C. E. Mehner. *Limdolen A Lightweight Authenticated Encryption Algorithm*. NIST. Accessed: Mar. 28, 2020. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/Limdolen-Spec.pdf

[273] M. Montes and D. Penazzi. *Yarara and Coral v1*. NIST. Accessed: Sep. 22, 2020. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/yarara_and_coral-spec.pdf

[274] E. M. D. Nascimento and J. A. M. Xexéo. *FlexAEAD—A Lightweight Cipher With Integrated Authentication*. NIST. Accessed: Sep. 22, 2020. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/FlexAEAD-spec.pdf

[275] D. Penazzi and M. Montes. *Shamash (and Shamashash) (Version 1)*. NIST. Accessed: Sep. 22, 2020. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/ShamashAndShamashash-spec.pdf

[276] M.-J. O. Saarinen. *SNEIKEN and SNEIKHA Authenticated Encryption and Cryptographic Hashing*. NIST. Accessed: Sep. 22, 2020. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/sneik-spec.pdf

[277] S. Sarkar, K. Mandal, and D. Saha. *Sycon v1.0 Submission to Lightweight Cryptographic Standards*. NIST. Accessed: Sep. 22, 2020. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/sycon-spec.pdf

[278] H. Sui, W. Wu, L. Zhang, and D. Zhang. *LAEM (Lightweight Authentication Encryption Mode)*. NIST. Accessed: Sep. 22, 2020. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/LAEM-spec.pdf

[279] H. Wu and T. Huang. *CLX: A Family of Lightweight Authenticated Encryption Algorithms*. NIST. Accessed: Sep. 22, 2020. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/CLX-spec.pdf

[280] D. Ye, D. Shi, Y. Ma, and P. Wang. *HERN & HERON: Lightweight AEAD and Hash Constructions based on Thin Sponge (v1)*. NIST. Accessed: Sep. 22, 2020. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/HERN%26HERON-spec.pdf

[281] B. Zhang. *Fountain: A Lightweight Authenticated Cipher (v1)*. NIST. Accessed: Sep. 22, 2020. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/fountain-spec.pdf

[282] B. Zhang. *Quartet: A Lightweight Authenticated Cipher (v1)*. NIST. Accessed: Sep. 22, 2020. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/Quartet-spec.pdf

[283] L. R. Krishnan, M. Sindhu, and C. Srinivasan, "Analysis of sponge function based authenticated encryption schemes," in *Proc. 4th Int. Conf. Adv. Comput. Commun. Syst. (ICACCS)*, Jan. 2017, pp. 1–5, doi: 10.1109/ICACCS.2017.8014683. [Online]. Available: https://ieeexplore.ieee.org/ielx7/8010764/8014556/08014683.pdf?tp=&arnumber=8014683&isnumber=8014556&ref=

[284] T. Santoli and C. Schaffner, "Using Simon's algorithm to attack symmetric-key cryptographic primitives," *Quantum Inf. Comput.*, vol. 17, nos. 1–2, pp. 65–78, 2017.

[285] M. Kaplan, G. Leurent, A. Leverrier, and M. Naya-Plasencia, "Breaking symmetric cryptosystems using quantum period finding," *Cryptogr. Secur.*, Jun. 2016. [Online]. Available: https://arxiv.org/abs/1602.05973

[286] S. J. H. Pirzada, A. Murtaza, L. Jianwei, and T. Xu, "The parallel CMAC authenticated encryption algorithm for satellite communication," in *Proc. IEEE 9th Int. Conf. Electron. Inf. Emergency Commun. (ICEIEC)*, Jul. 2019, pp. 1–5, doi: 10.1109/ICEIEC.2019.8784593. [Online]. Available: https://ieeexplore.ieee.org/document/8784593/https://ieeexplore.ieee.org/ielx7/8771464/8784454/08784593.pdf?tp=&arnumber=8784593&isnumber=8784454&ref=

[287] E. Andreeva, A. Bogdanov, A. Luykx, B. Mennink, N. Mouha, and K. Yasuda, "How to securely release unverified plaintext in authenticated encryption," *Advances in Cryptology—ASIACRYPT*. Berlin, Germany: Springer, 2014, pp. 105–125.

[288] D. Ye, D. Shi, Y. Ma, and P. Wang. *HERN & HERON: Lightweight AEAD and Hash Constructions based on Thin Sponge (v1)*. NIST. Accessed: Feb. 15, 2021. [Online]. Available: https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/HERN%26HERON-spec.pdf

MOHAMUD AHMED JIMALE received the bachelor's degree in information technology from SIMAD University, Mogadishu, Somalia, and the master's degree in computer science from the University of Malaya, Malaysia, where he is currently pursuing the Ph.D. degree. He held different academic and administrative positions, including the Founding President of the Jamhuriya University of Science and Technology (JUST) and the Deputy Head of the Information Technology Department, Dahabshil International Company, Somalia. His research interests include cryptography, blockchain, cloud computing, and the Internet of Everything (IoE).

MUHAMMAD REZA Z'ABA received the Bachelor of Science degree (computer) from Universiti Teknologi Malaysia (UTM), in 2004, and the Ph.D. degree from the Queensland University of Technology, Australia, in 2010.

He is currently a Senior Lecturer at the Department of Computer System and Technology, Faculty of Computer Science and Information Technology, University of Malaya. He was previously a Researcher at MIMOS Berhad, from 2010 to February 2018, which is a research arm under the purview of the Ministry of Science, Technology and Innovation, Malaysia. His main research interests include symmetric cryptography, including block ciphers and hash functions. He is also looking into blockchain-related technologies, including digital currencies and other areas of information security.

MISS LAIHA BINTI MAT KIAH (Senior Member, IEEE) received the Ph.D. degree in information security from the Royal Holloway, University of London, U.K., in 2007. Since then, she has been an Active Researcher at the Faculty of Computer Science and Information Technology, UM, in her computer science field, particularly in security. She was promoted to a Professorship, in 2015. Her main research interest includes security aspect of computing and technology fields with variation of applications in multi and/or trans disciplinary projects. This is evidenced by her publications and research projects in which she is/was the principal investigator (PI) as well as a co-PI. As a Professional Technologist (Ts.), keeping up with the current trend and demand of ever evolving computing technology field is crucial to ensure the quality and the impact of her research work. Her current research interests include cyber security, blockchain technology, the IoT, and health information exchange. She is an Active Member of EC Council, Malaysian Society for Cryptology Research (MSCR), and Malaysia Board of Technologists (Ts.).

MOHD YAMANI IDNA IDRIS (Member, IEEE) received the B.E. degree in electrical engineering, the M.Sc. degree in computer science, and the Ph.D. degree in electrical engineering from Universiti Malaya, Kuala Lumpur, Malaysia. He is currently an Associate Professor with the Department of Computer System and Technology, Faculty of Computer Science and Information Technology, Universiti Malaya. He has published many articles in reputable journals. His research interests include the Internet of Things (IoT), information security, embedded systems, image processing and computer vision, and wireless sensor networks. He has received many awards for his inventions.

NORZIANA JAMIL received the Ph.D. degree in security in computing, in 2013. She is currently an Associate Professor at Universiti Tenaga Nasional, Malaysia. She is an Alumni of Leadership in Innovation Fellowship by U.K. Royal Academy of Engineering and the Project Leader of various cryptography and cyber security related research and consultancy projects. She has been actively involving in advisory for cryptography and cyber security projects and works with several international prominent researchers and professors. Her area of research specialization and interests include cryptography, security for cyber-physical systems, security analytics, and intelligent systems.

MOESFA SOEHEILA MOHAMAD received the Bachelor of Arts degree in mathematics and computation from Oxford University, in 1997, and the Master of Science degree in mathematics for cryptography and communications from the Royal Holloway College, University of London, in 2011. She is currently pursuing the Ph.D. degree in IT with Multimedia University, Cyberjaya, Malaysia. She has been a Researcher at MIMOS Berhad, since 1997.

MOHD SAUFY ROHMAD received the first degree in information technology from Universiti Teknologi PETRONAS and the Master of Science degree in computer science from UiTM, Shah Alam, where he is currently pursuing the Ph.D. degree in embedded cryptography. He is the Head of robotic, the IoT, and big data with the Smart Manufacturing Research Institute, UiTM. He is a full time Senior Lecturer with the College of Engineering, UiTM. He was previously a Researcher at Telekom Malaysia Research and Development and MIMOS Berhad. He was also a SoC Design Engineer at Intel Penang. He also involved in a few Industrial IoT projects for livestock and agriculture.