Counter-in-Tweak: Authenticated Encryption Modes for Tweakable Block Ciphers

Thomas Peyrin[1] and Yannick Seurin[2(✉)]

[1] SPMS, NTU, Singapore, Singapore
thomas.peyrin@ntu.edu.sg
[2] ANSSI, Paris, France
yannick.seurin@m4x.org

Abstract. We propose the Synthetic Counter-in-Tweak (SCT) mode, which turns a tweakable block cipher into a nonce-based authenticated encryption scheme (with associated data). The SCT mode combines in a SIV-like manner a Wegman-Carter MAC inspired from PMAC for the authentication part and a new counter-like mode for the encryption part, with the unusual property that the counter is applied on the tweak input of the underlying tweakable block cipher rather than on the plaintext input. Unlike many previous authenticated encryption modes, SCT enjoys provable security beyond the birthday bound (and even up to roughly 2^n tweakable block cipher calls, where n is the block length, when the tweak length is sufficiently large) in the nonce-respecting scenario where nonces are never repeated. In addition, SCT ensures security up to the birthday bound even when nonces are reused, in the strong nonce-misuse resistance sense (MRAE) of Rogaway and Shrimpton (EUROCRYPT 2006). To the best of our knowledge, this is the first authenticated encryption mode that provides at the same time close-to-optimal security in the nonce-respecting scenario and birthday-bound security for the nonce-misuse scenario. While two passes are necessary to achieve MRAE-security, our mode enjoys a number of desirable features: it is simple, parallelizable, it requires the encryption direction only, it is particularly efficient for small messages compared to other nonce-misuse resistant schemes (no precomputation is required) and it allows incremental update of associated data.

Keywords: Authenticated encryption · Tweakable block cipher · Nonce-misuse resistance · Beyond-birthday-bound security · CAESAR competition

1 Introduction

BACKGROUND ON AUTHENTICATED ENCRYPTION. Confidentiality and authenticity of data are the two main security properties that one must ensure when communicating over an insecure channel. In the symmetric key setting, it has long been known how to ensure both of them independently, e.g., starting from

a secure block cipher, by using a suitable encryption mode for confidentiality [7] and a block cipher-based MAC for authenticity [9]. However, how exactly to combine both tools has long been left to the practitioners, leading to major security breaches [3,18,37]. Sometimes, protocol designers even overlooked that authenticity was a necessary requirement besides confidentiality, as exemplified by padding oracle attacks [59]. Even when the combination of the encryption and the MAC schemes is properly done, it might not be the most efficient solution, especially when the two parts rely on two different primitives. For these reasons, interest has shifted towards designing "integrated" Authenticated Encryption (AE) schemes ensuring jointly authenticity and confidentiality of data, which are more efficient and less likely to be incorrectly used. Besides, it has become standard for an AE scheme to have the ability to handle so-called associated data (AD), which are authenticated but not encrypted [51] (such a scheme was for a time called an AEAD scheme, but since this feature is so important in practice, virtually all modern AE schemes provide it; we will only talk of AE in this paper, implicitly meaning AEAD). Even though ad-hoc AE schemes were already used since a long time, the formal treatment of these constructions only started around 2000 [10,11,36]. At about the same time, provably secure AE designs started to appear, such as IAPM [34,35], XCBC [22], CCM [61], OCB [52,54], or GCM [43]. The CAESAR competition [1] for authenticated encryption, started in 2014, recently put this research topic in the limelight. Various AE schemes were proposed, from purely ad-hoc designs to (tweakable) block cipher operating modes.

NONCE-MISUSE RESISTANCE. Since most symmetric-key primitives (in particular block ciphers) from which AE schemes are built are deterministic, a random IV or a nonce (i.e., a value which must never be repeated for the same secret key) is a necessary ingredient for achieving strong security goals. Failing to ensure the corresponding requirement (high entropy for an IV, non-repetition for a nonce) can have dramatic consequences for security. For example, reusing a nonce just a single time for encrypting two messages in OCB completely breaks confidentiality: an attacker can immediately detect repeated message blocks since the corresponding ciphertext blocks will be equal. The non-repeating requirement on the nonce can be challenging to fulfill in some contexts, for example when encryption is implemented in a stateless device.[1] It is likely (and it has happened before) that some implementations will, e.g., simply generate nonces at random, "hoping" that no collision will occur. For that reason, a recent trend in AE has been to design schemes achieving *nonce-misuse resistance*, which informally means that the impact on security of a nonce repetition should be as limited as possible. This goal was first put forward by Rogaway and Shrimpton [55], who formalized the notion of *misuse-resistant AE* (MRAE). For a scheme enjoying this property, authenticity is not harmed by nonce repetitions, while confidentiality is only damaged insofar as the adversary can detect whether the same triple of nonce, AD and message values is repeated. Example of schemes achieving this

---

[1] Similarly, the high-entropy requirement on the IV is hard to meet when no good randomness source is available.

security notion are EAX [12], SIV [55], AEZ [26], or GCM-SIV [25]. Because the MRAE notion cannot be achieved for an online scheme (since each bit of the ciphertext must depend on every bit of the plaintext), Fleischmann *et al.* [21] proposed a relaxation of the MRAE notion called *online AE* (OAE), which can be achieved with a single pass on the input. Examples of schemes ensuring this security property are McOE [21], COPA [5], or POET [2]. However, the interest in the OAE notion has been recently reduced by some serious security concerns, notably the so-called chosen-prefix/secret-suffix (CPSS) generic attack [27], that shares some similarities with the BEAST attack [18].

BIRTHDAY AND BEYOND-BIRTHDAY SECURITY. Another important shortcoming of most AE operating modes is that they provide only birthday-bound security with respect to the block length of the underlying primitive. Since virtually all existing block ciphers have block length at most 128 bits (in particular the current block cipher standard AES), this means that security is lost at 2^{64} block cipher calls at best, which is low given modern security requirements (for 64-bit block ciphers, the situation is even more problematic). Moreover, this is rarely a problem with the tightness of the security proof: attacks matching the bound are often known. For example, Ferguson [19] described a simple collision-based attack on OCB that breaks authenticity with 2^{64} blocks of messages. Recently, some AE schemes providing security beyond the birthday bound (BBB) were proposed [28,29], but they usually come at an expensive performance price. One could argue that using a double-block-length block cipher would provide the expected security, but this solution comes with an important efficiency penalty (as can be seen in generic double-block-length block cipher constructions) and would be highly problematic for hardware implementations where internal state size is a major contribution to the total area cost.

AE FROM TWEAKABLE BLOCK CIPHERS. Compared with a conventional block cipher, a tweakable block cipher (TBC) $\widetilde{E}$ takes an additional input called a *tweak* bringing inherent variability to the primitive (equivalently, a TBC can be seen as a family of block ciphers indexed by the tweak). In the same paper that formalized the corresponding security notion [41], it was pointed out that a TBC was a very convenient starting point for building various schemes. In particular, for AE schemes, two prominent examples are the sibling modes TAE [41] and ΘCB [38] (the TBC-based generalization of OCB). They have "perfect" security in the sense that, when used with an ideal TBC, the advantage of any adversary is zero against confidentiality and close to $2^{-\tau}$ against authenticity, where τ is the tag length. However, as already pointed out, a weakness of both TAE and ΘCB (even when used with an ideal TBC) is that their security completely collapses as soon as a nonce is repeated. As a matter of fact, existing AE schemes built from an ideal TBC either ensure perfect security in the nonce-respecting scenario only (like TAE or ΘCB), or fulfill the weak OAE notion only (e.g. COPA, once recast to use an ideal TBC), or ensure MRAE-security but only up to the birthday bound, even if nonces are not repeated (like AEZ). The PIV construction by Shrimpton and Terashima [58] allows to construct a variable-input-length TBC

with BBB-security, which in turn allows to construct (via the Encode-then-Encipher method) an AEAD scheme with BBB-security against nonce-respecting adversaries and birthday-bound security against nonce-misusing ones. However, PIV requires as a building block a fixed-input-length TBC with *variable* tweak length (comparable to the maximal input length of the PIV construction), which in turn requires to appeal to universal hash functions with key length comparable to the maximal tweak length. Hence, the resulting AEAD scheme must use very large keys to ensure BBB-security for large messages. As of today, there is no AEAD scheme based on a fixed-tweak-length TBC that ensures both BBB-security in the nonce-respecting scenario and (at least) birthday-bound security in the nonce-misuse scenario. Yet this seems a very desirable goal since such a scheme would at the same time yield very high (BBB) security guarantees in the nominal, nonce-respecting use case and retain acceptable (birthday-bound) security when inadvertently misused.

OUR CONTRIBUTIONS. In this paper, we propose the SCT (Synthetic Counter-in-Tweak) nonce-based AE mode for tweakable block ciphers and prove that it ensures BBB-security in the nonce-respecting scenario, and birthday-bound security in the nonce-misuse scenario (in the strong MRAE sense [55]). More precisely, for the nonce-respecting case, when using a ideal TBC with block length n and "effective" tweak length[2] w, SCT is secure up to roughly 2^n TBC calls when $w \geq n$, and up to roughly $2^{(n+w)/2}$ TBC calls when $w \leq n$, which is always larger than $2^{n/2}$. The SCT mode requires two passes (as is inevitable for MRAE-security), but it is simple, parallelizable, it requires the encryption direction only, it is particularly efficient for small messages compared to other nonce-misuse resistant schemes (no precomputation is required) and it allows incremental update of associated data.

With respect to how authentication and encryption are combined, our design draws inspiration from the SIV generic composition method [55]: the nonce N, the associated data A, and the message M are first input to a keyed function F_K, yielding an pseudorandom initial value IV, which will serve as authentication tag. The message is then encrypted, using the generated IV *and the nonce N* (see Fig. 4). This "recycling" of the nonce in the encryption part of the mode is what makes our high-level construction (called NSIV) crucially different from SIV and allows to reach BBB-security in the nonce-respecting case.[3]

It remains to instantiate the two components of the NSIV construction, the keyed function F_K and the encryption scheme. Since we aim at BBB-security in the nonce-respecting case, a natural starting point for F_K is the Wegman-Carter paradigm [14,56,60]. Hence, we propose a nonce-based MAC mode called PWC (*Parallel Wegman-Carter*) which combines a xor-universal hash function inspired from PMAC [13,52] applied to the AD and the message, and a simple

---

[2] The SCT mode uses 5 tweak prefixes to separate the different usages of the TBC. The "effective" tweak length is what remains once 3 bits have been used to encode the prefix.

[3] While SIV corresponds to generic composition method A4 in the nomenclature of Namprempre *et al.* [46], NSIV does not fit any of the NRS schemes.

pseudorandom function applied to the nonce. In order to achieve nonce-misuse resistance (which in general Wegman-Carter MACs do not provide), we add an additional encryption layer, which results in the EPWC (*Encrypted PWC*) mode.

The real challenge lies in designing an encryption scheme which is BBB-secure in the nonce-respecting case. Since on one hand it seems hard to leverage on the non-repeating property of the nonce without actually giving the nonce as input to the encryption mode, and on the other hand we need to make use in some way of the pseudorandom IV computed from F_K,[4] it appears that what we need to design is actually a *combined nonce- and IV-based encryption scheme* (*nivE scheme* for short). To the best of our knowledge, this notion has never appeared before, and we introduce it in this paper. The encryption mode that we propose, called CTRT (*CounTeR in Tweak*), is a counter-like mode with the unusual property that the counter is applied on the tweak input of the underlying TBC rather than on the plaintext input, where the nonce comes in. The combination of EPWC and CTRT through the NSIV construction (the IV generated by EPWC being used as initial counter in CTRT) yields the SCT mode, illustrated in Fig. 1.

For completeness, we also describe in the full version of this paper [50] the CTPWC (CTRT-*then*-PWC) mode, an *online* nonce-based AE scheme which combines in an "encrypt-then-MAC" manner a slight variant of the CTRT encryption mode and the PWC authentication mode. The security guarantees provided by CTPWC are similar to those of ΘCB, but it is roughly twice less efficient, so that we do not claim that it is of particularly high interest. One small advantage that we see for this mode compared with ΘCB is that the nonce length can be as large as the block length of the underlying TBC, whereas for ΘCB the sum of the nonce length and of the maximal length of encrypted messages must be less than the tweak length of the underlying tweakable block cipher, which might be restrictive in some settings (e.g., for KIASU-BC [32]). It might also escape the patent issues which hindered the adoption of OCB.

INSTANTIATING THE TBC. As just discussed, our new AE modes offer BBB-security (in the nonce-respecting case) when used with an ideal TBC. If one aims at leveraging this security level in the real world, one must instantiate the TBC with care. Most existing TBCs are built from conventional block ciphers in a generic way, the prominent example being the XE/XEX construction [52] which only ensures security up to the birthday bound. Hence, using XE/XEX in our schemes would in a sense waste their nice security promises.[5] To remedy this problem, one can use either generic TBC constructions with BBB-security [39, 40, 44, 45] (but they are often inefficient or provably secure in the ideal cipher model only), or ad-hoc TBC designs without known weaknesses. The second option was chosen for a number of CAESAR candidates [24, 30–32]. In fact, the SCT mode was explicitly designed as a replacement to the COPA mode used in versions 1.1 and 1.2 of CAESAR candidates Deoxys [30] (128-bit

---

[4] This excludes for example a simple OCB-like encryption mode since it is only nonce-based, not IV-based.

[5] Similarly, the only reason why OCB is secure up to the birthday bound whereas ΘCB is "perfectly" secure is because it relies on XE/XEX for instantiating the TBC.
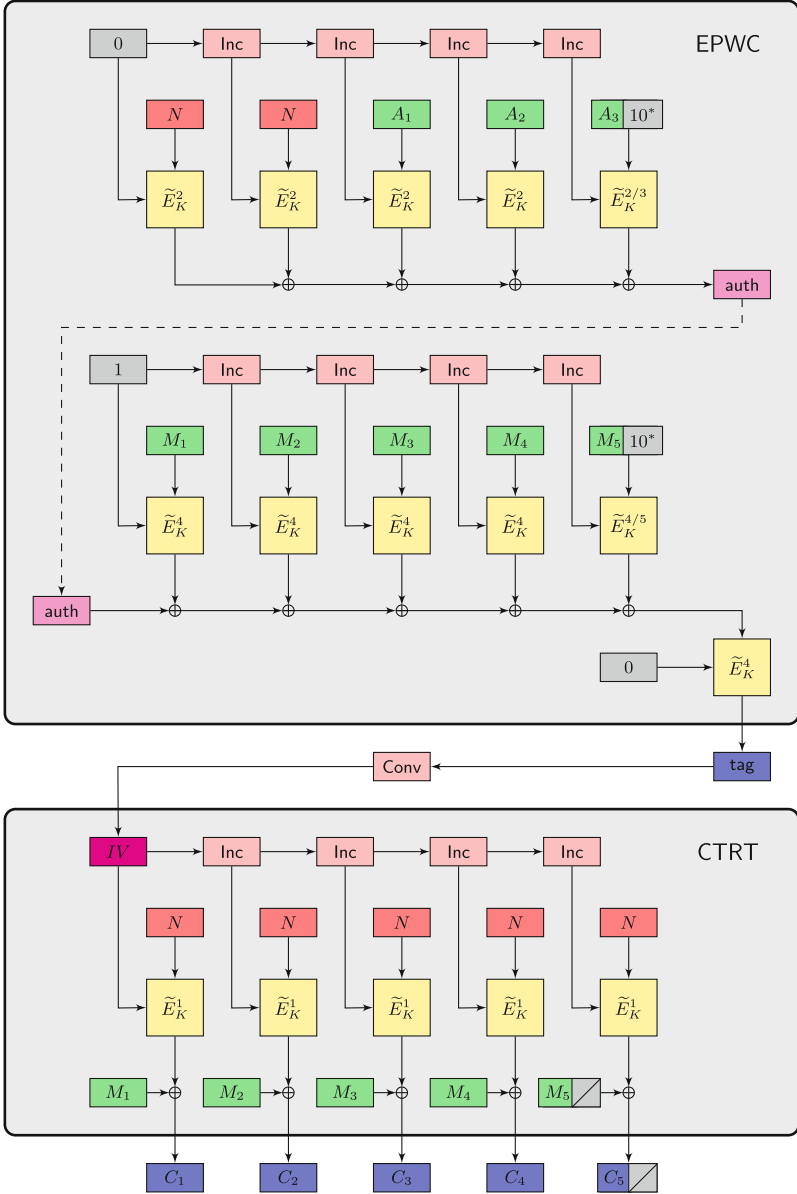
Fig. 1. The SCT mode, using a TBC $\widetilde{E}$ with tweak space $\{1,\ldots,5\} \times \mathcal{T}$ and domain $\mathcal{X} = \{0,1\}^n$. For each call to $\widetilde{E}_K$, the tweak enters left while the plaintext enters on top. We denote $\widetilde{E}_K^i(T, X)$ for $\widetilde{E}_K((i,T), X)$ and $\widetilde{E}_K^{i/j}$ means that prefix i is used when the input block is complete and unpadded, whereas j is used when the input block is incomplete and padded. Function Inc is a cyclic permutation of $\mathcal{T}$, and Conv is a regular function from $\mathcal{X}$ to $\mathcal{T}$ (e.g., truncation when $\mathcal{X} = \{0,1\}^n$ and $\mathcal{T} = \{0,1\}^w$, $w \leq n$).

blocks, 128-bit tweaks) and Joltik [31] (64-bit blocks, 64-bit tweaks).[6] We refer to the submission documents of these two candidates for a detailed report on implementation results, which are quite competitive. Other potential candidates for instantiating the SCT mode are Scream [24] and Threefish, the TBC on which the hash function Skein [20] is based. There is currently a shift towards designing dedicated TBCs achieving higher security and efficiency than generic BC-based constructions, and we hope to see more and more TBC proposals that could be used with SCT.

OPEN PROBLEMS AND FUTURE WORK. The CTRT encryption scheme has the notable feature that its security degrades gracefully with the maximal number of repetitions of nonces: when the nonce repetitions are limited, security remains close to the security bound in the nonce-respecting case. In contrast, the security of the EPWC authentication mode (and more generally of any encrypted Wegman-Carter MAC) falls back to birthday bound as soon as the adversary can repeat one single nonce twice (see Remark 2 in Sect. 5). It remains a pending question to modify EPWC so that it provides graceful security degradation with the maximal number of nonce repetitions as well. This would make the resulting AE scheme a good candidate for high security in both nonce-respecting and nonce-misuse models for most practical scenarios. Another challenging open problem would be to construct an AE scheme which remains BBB-secure even when nonces are arbitrarily repeated. The main difficulty is to build a deterministic, stateless, BBB-secure MAC, which is known to be notably hard [17,62]. Another possible direction for future work would be to design a mode similar to SCT using only one pass and achieving online nonce-misuse resistance in the OAE sense [21]. Such a feature would allow users to smoothly choose the best security achievable, depending on whether two passes can be tolerated or not by the application. Finally, it would be interesting to analyze how to strengthen SCT against other misuse scenarios such as release of unverified plaintext [4], and to study how its security is affected by tag truncation [26].

ORGANIZATION. In Sect. 2 we provide a high-level description of the various possibilities that we considered for constructing a BBB-secure nivE scheme. After introducing the notation and standard security notions in Sect. 3, we describe the CTRT encryption scheme and prove its security in Sect. 4, while we describe the PWC and EPWC nonce-based MAC schemes and prove their security in Sect. 5. Finally, we explain how to combine CTRT and EPWC using the NSIV construction to build the nonce-based AE mode SCT and prove its security in Sect. 6.

2   Counter-in-Tweak for Beyond-Birthday Security

As motivated in introduction, our goal is to design a simple TBC-based AE scheme that provides BBB-security in the nonce-respecting setting and (at least)

---

[6] The tweak prefixes used in this paper were chosen for ease of exposition and are slightly different from the ones used in Deoxys and Joltik v1.3, which were chosen mainly for efficiency reasons.

birthday-bound MRAE-security. As already mentioned, an encrypted Wegman-Carter MAC solves the problem for the authentication part, so that we focus here on encryption. Hence, our problem is as follows: given a nonce and a synthetic IV generated pseudorandomly from the nonce, the AD and the message, how do we use them to encrypt the message with BBB-security? We give a quick overview of the various constructions that we considered and why, except the CTRT encryption mode we propose, they fail or are unsatisfactory.

A natural direction to explore is to start from a scheme providing BBB-security for non-repeating nonces, such as TAE [41] or ΘCB [38], which are similar with regard to encryption: it simply consists in a "tweakable" codebook mode, the tweak holding the nonce and a message block counter. This is obviously not nonce-misuse resistant: repeating the nonce a single time will lead to a complete break of confidentiality since a constant message block leads to a constant ciphertext block. One could incorporate the IV by simply concatenating it to the nonce and the counter to form the tweak. However, this would require a TBC with larger tweak, which is usually very costly to achieve.[7] Rather than concatenating the nonce and the IV, one could try to combine them into a single shorter string S, but this would presumably result in birthday security even in the nonce-respecting scenario (since a collision on S would directly break confidentiality). Hence, a codebook encryption mode does not seem to be a very convenient starting point.

For this reason, we preferred to consider a counter mode (note that this was the encryption mode favored by Rogaway and Shrimpton to instantiate the SIV composition method [55]). The question now is: how do we feed the nonce, the IV, and the i-th counter to the TBC in order to create the mask that will be xored to the i-th message block? We considered several possibilities (we do not claim this to be exhaustive):

(a) One can put the nonce in the tweak input, and the sum of the IV and the counter in the plaintext input. The problem is that confidentiality caps at birthday bound even in the nonce-respecting scenario: the adversary can query the encryption of a single message with $2^{n/2}$ equal blocks, and observe that no collision occurs in the corresponding ciphertext blocks (since the nonce is fixed and all TBC calls use the same tweak), which will distinguish the ciphertext from a random string (for which a collision would be expected).

(b) One can concatenate the nonce and the counter in the tweak input, and use the IV for the plaintext input. Since the tweak is different for each message block position, this solves the issue of the previous solution. We conjecture that this mode meets our security objectives, but an important drawback is that a larger tweak length is required and, as mentioned before, this is very costly.

---

[7] For example, for TBCs following the TWEAKEY approach [30,31,33], there is a large gap in the number of rounds needed to make the TBC secure as the tweak length increases.

(c) One can put the sum of the nonce and the counter in the tweak input (instead of concatenating them) and the IV in the plaintext input. This mode might meet our security objectives, however the adversary can very easily provoke collisions on tweak inputs even in the nonce-respecting scenario, which might complicate the proof of BBB-security. Another drawback is that in the nonce-misuse scenario, a collision on the IV immediately breaks confidentiality, which dashes any hope for BBB nonce-misuse resistance. Note that one could imagine variants where the nonce and the IV are first encrypted before being used, but it is not clear if this would prevent the issues just mentioned and this would presumably make the security proof quite complex.

(d) Finally, one can put the sum of the IV and the counter in the tweak input and the nonce in the plaintext input, which is exactly the CTRT mode. We will prove in Sect. 4 that it meets our security goal. The first idea is that the counter in the tweak input ensures that all the calls to the internal TBC will use different tweaks for one single message query, so that the ciphertext looks uniformly random in that case. Thus, the adversary has to query several messages with different nonce values and hope that many collisions will occur between tweak inputs in order to observe a divergence from uniformity in the ciphertexts. However, these collisions are hard to control since they depend on the pseudorandom IV (in contrast with other modes discussed above, where the tweak input can be easily controlled by the adversary). We will show in Sect. 4, using a "balls-into-bins" analysis, that the number of tweak collisions remains small, so that the distribution of the ciphertexts remains close to uniform. Moreover, the nonce-misuse scenario helps the adversary only if it can repeat the same nonce a very high number of times until a collision happens on the tweaks, so that the security of the CTRT mode degrades gracefully with the maximal number of nonce repetitions.

3   Preliminaries

NOTATION. Given a string $X \in \{0,1\}^*$, $|X|$ denotes its length. If X and Y are respectively n-bit and m-bit strings, $n < m$, then $X \oplus Y$ denotes the n-bit string obtained by xoring X with the n leftmost bits of Y. Given some implicit length n and a bit-string X of length $1 \leq |X| < n$, we denote $X10^*$ the string obtained by appending a single 1 and $(n - |X| - 1)$ 0's to X. Given two sets $\mathcal{X}$ and $\mathcal{Y}$, the set of all functions from $\mathcal{X}$ to $\mathcal{Y}$ is denoted $\mathsf{Func}(\mathcal{X}, \mathcal{Y})$. A function $F \in \mathsf{Func}(\mathcal{X}, \mathcal{Y})$ is said *regular* if all $Y \in \mathcal{Y}$ have the same number of preimages by F (this obviously requires $|\mathcal{X}|$ to be a multiple of $|\mathcal{Y}|$).

TWEAKABLE BLOCK CIPHERS. A *tweakable block cipher* (TBC) with key space $\mathcal{K}$, tweak space $\mathcal{T}$, and domain $\mathcal{X}$ is a mapping $\widetilde{E} : \mathcal{K} \times \mathcal{T} \times \mathcal{X} \to \mathcal{X}$ such that for any key $K \in \mathcal{K}$ and any tweak $T \in \mathcal{T}$, $X \mapsto \widetilde{E}(K, T, X)$ is a permutation of $\mathcal{X}$. We often write $\widetilde{E}_K(T, X)$ or $\widetilde{E}_K^T(X)$ in place of $\widetilde{E}(K, T, X)$. We denote $\mathsf{TBC}(\mathcal{K}, \mathcal{T}, \mathcal{X})$ the set of all tweakable block ciphers with key space $\mathcal{K}$, tweak

space $\mathcal{T}$, and domain $\mathcal{X}$. A *tweakable permutation* with tweak space $\mathcal{T}$ and domain $\mathcal{X}$ is a mapping $\widetilde{P} : \mathcal{T} \times \mathcal{X} \to \mathcal{X}$ such that for any tweak $T \in \mathcal{T}$, $X \mapsto \widetilde{P}(T, X)$ is a permutation of $\mathcal{X}$. We often write $\widetilde{P}^T(X)$ in place of $\widetilde{P}(T, X)$. We denote $\mathsf{TP}(\mathcal{T}, \mathcal{X})$ the set of all tweakable permutations with tweak space $\mathcal{T}$ and domain $\mathcal{X}$. The security of a TBC is defined as follows.

Definition 1 (TPRP Security). *Let $\widetilde{E} \in \mathsf{TBC}(\mathcal{K}, \mathcal{T}, \mathcal{X})$ and A be an adversary with oracle access to a tweakable permutation with tweak space $\mathcal{T}$ and domain $\mathcal{X}$. The advantage of A in breaking the TPRP-security of $\widetilde{E}$ is defined as*

$$\mathbf{Adv}_{\widetilde{E}}^{\mathrm{TPRP}}(\mathsf{A}) = \left| \Pr\left[K \leftarrow_\$ \mathcal{K} : \mathsf{A}^{\widetilde{E}_K} = 1 \right] - \Pr\left[\widetilde{P} \leftarrow_\$ \mathsf{TP}(\mathcal{T}, \mathcal{X}) : \mathsf{A}^{\widetilde{P}} = 1 \right] \right|.$$

Note that we do not need the strongest "two-sided" version of TPRP-security (where the adversary also has access to a decryption oracle) since all constructions considered in this paper only use the forward (encryption) direction of the underlying TBC.

TWEAK SEPARATION. Let $\widetilde{E}$ be a TBC with tweak space of the form $\mathcal{T}' = \mathcal{I} \times \mathcal{T}$ for some subset $\mathcal{I} \subset \mathbb{N}$ and some set $\mathcal{T}$. We call $\mathcal{T}$ the *effective* tweak space of $\widetilde{E}$. Then, for $i \in \mathcal{I}$, we denote $\widetilde{E}^i$ the tweakable block cipher with the same key and message spaces as $\widetilde{E}$ and tweak space $\mathcal{T}$ defined by

$$\widetilde{E}^i(K, T, X) = \widetilde{E}(K, (i, T), X).$$

By the same convention as before, we write $\widetilde{E}_K^i(T, X)$ or $\widetilde{E}_K^{i,T}(X)$ for $\widetilde{E}^i(K, T, X)$. Clearly, when $\widetilde{E}$ is an ideal TBC drawn uniformly at random from $\mathsf{TBC}(\mathcal{K}, \mathcal{T}', \mathcal{M})$, then each $\widetilde{E}^i$ is an independent ideal TBC drawn uniformly at random from $\mathsf{TBC}(\mathcal{K}, \mathcal{T}, \mathcal{M})$. Given a bit-string X of length $1 \leq |X| \leq n$, we compactly write

$$\widetilde{E}^{i/j}(K, T, X(10^*)), \quad \widetilde{E}_K^{i/j}(T, X(10^*)), \quad \text{or} \quad \widetilde{E}_K^{i/j,T}(X(10^*))$$

to mean $\widetilde{E}^i(K, T, X)$ when $|X| = n$ and $\widetilde{E}^j(K, T, X10^*)$ when $|X| < n$.

STANDARD SECURITY NOTIONS. We give the security definitions of a nonce-based PRF, a nonce-based MAC, and a nonce-based Authenticated Encryption scheme. All these are standard, except maybe the nonce-based PRF notion which is a straightforward adaptation of the classical definition of a PRF to the nonce-based setting. Our definition of the security of a MAC is indistinguishability-based (which will be more convenient later), but it is easy to see that it is equivalent to the more conventional unforgeability-based definition. In the following, a nonce-based keyed function is a function $F : \mathcal{K} \times \mathcal{N} \times \mathcal{D} \to \mathcal{Y}$, where $\mathcal{K}$ is the key space, $\mathcal{N}$ the nonce space, $\mathcal{D}$ the domain and $\mathcal{Y}$ the range.

Definition 2 (Nonce-Based PRF). *Let $F : \mathcal{K} \times \mathcal{N} \times \mathcal{D} \to \mathcal{Y}$ be a nonce-based keyed function, and let us write $F_K(N, D)$ for $F(K, N, D)$. Let A be an adversary*

with oracle access to a function from $\mathcal{N} \times \mathcal{D}$ to $\mathcal{Y}$. The advantage of A *against the PRF-security of F is defined as*

$$\mathbf{Adv}_F^{\mathrm{PRF}}(\mathsf{A}) = \Big| \Pr\left[K \leftarrow_\$ \mathcal{K} : \mathsf{A}^{F_K} = 1\right]$$
$$- \Pr\left[R \leftarrow_\$ \mathsf{Func}(\mathcal{N} \times \mathcal{D}, \mathcal{Y}) : \mathsf{A}^R = 1\right] \Big|.$$

The adversary is said nonce-respecting if it never repeats a nonce $N \in \mathcal{N}$ in its oracle queries. In that case, we denote its advantage $\mathbf{Adv}_F^{\mathrm{nPRF}}(\mathsf{A})$.

Definition 3 (Nonce-Based MAC). *Let F be as in Definition 2. Let* B *be an adversary with oracle access to two oracles, the first oracle being a function from $\mathcal{N} \times \mathcal{D}$ to $\mathcal{Y}$, the second oracle with inputs in $\mathcal{N} \times \mathcal{D} \times \mathcal{Y}$ and outputs in $\{1, \perp\}$. The advantage of* B *against the MAC-security of F is defined as*

$$\mathbf{Adv}_F^{\mathrm{MAC}}(\mathsf{B}) = \Big| \Pr\left[K \leftarrow_\$ \mathcal{K} : \mathsf{B}^{F_K, \mathsf{Ver}_K} = 1\right] - \Pr\left[K \leftarrow_\$ \mathcal{K} : \mathsf{B}^{F_K, \mathsf{Rej}} = 1\right] \Big|,$$

where Ver_K is an oracle which takes as input a triple $(N, D, \mathsf{tag}) \in \mathcal{N} \times \mathcal{D} \times \mathcal{Y}$ and returns 1 if $F_K(N, D) = \mathsf{tag}$, and $\perp$ otherwise, and Rej is an oracle which always returns $\perp$. The adversary is not allowed to ask a verification query (N, D, tag) if a previous query (N, D) to F_K returned tag. The adversary is said nonce-respecting if it never repeats a nonce $N \in \mathcal{N}$ in its queries to the first oracle F_K. In that case, we denote its advantage $\mathbf{Adv}_F^{\mathrm{nMAC}}(\mathsf{B})$.

Note that in the general case where the adversary is allowed to repeat nonces, F can be seen as a standard (i.e., not nonce-based) keyed function with domain $\mathcal{N} \times \mathcal{D}$, in which case one recovers the standard definitions of a PRF and a MAC (hence our notation of the advantage when the adversary is unrestricted w.r.t. nonces). While it is a well-known fact that if F is a secure PRF, then it is a secure MAC [9,23], we stress that this is not true for the nonce-based variants of the two notions, which are in fact incomparable.[8]

We then give the definition of a nonce-based Authenticated Encryption (nAE) scheme (with associated data), for which we first recall the syntax. Let $\mathcal{K}$, $\mathcal{N}$, $\mathcal{A}$, and $\mathcal{M}$ be non-empty sets. A nAE scheme is a tuple $\Pi = (\mathcal{K}, \mathcal{N}, \mathcal{A}, \mathcal{M}, \mathsf{Enc}, \mathsf{Dec})$, where Enc and Dec are deterministic algorithms. The encryption algorithm Enc takes as input a key $K \in \mathcal{K}$, a nonce $N \in \mathcal{N}$, associated data $A \in \mathcal{A}$, and a message $M \in \mathcal{M}$, and outputs a binary string $C \in \{0,1\}^*$ (we assume that Enc returns $\perp$ if one of the inputs is not in the intended set). The decryption algorithm Dec takes as input a key $K \in \mathcal{K}$, a nonce $N \in \mathcal{N}$, associated data $A \in \mathcal{A}$, and a binary string $C \in \{0,1\}^*$, and outputs either a message $M \in \mathcal{M}$, or a special symbol $\perp$. We require that $\mathsf{Dec}(K, N, A, \mathsf{Enc}(K, N, A, M)) = M$ for all tuples $(K, N, A, M) \in \mathcal{K} \times \mathcal{N} \times \mathcal{A} \times \mathcal{M}$. We write $\mathsf{Enc}_K(N, A, M)$ for $\mathsf{Enc}(K, N, A, M)$ and $\mathsf{Dec}_K(N, A, C)$ for $\mathsf{Dec}(K, N, A, C)$.

---

[8] E.g., an nPRF-secure function F might depend only on the nonce, in which case it is trivial to forge and break nMAC-security, while an nMAC-secure function F might have all its outputs starting with a 0 bit, which allows to trivially break nPRF-security.

Definition 4 (Nonce-Based AE). *Let $\Pi = (\mathcal{K}, \mathcal{N}, \mathcal{A}, \mathcal{M}, \mathsf{Enc}, \mathsf{Dec})$ be a nAE scheme. The advantage of an adversary A in breaking Π is defined as*

$$\mathbf{Adv}_{\Pi}^{\mathrm{AE}}(\mathsf{A}) = \left| \Pr\left[K \leftarrow_{\$} \mathcal{K} : \mathsf{A}^{\Pi.\mathsf{Enc}_K(\cdot,\cdot,\cdot),\, \Pi.\mathsf{Dec}_K(\cdot,\cdot,\cdot)} = 1 \right] \right.$$
$$\left. - \Pr\left[\mathsf{A}^{\mathsf{Rand}(\cdot,\cdot,\cdot),\, \mathsf{Rej}(\cdot,\cdot,\cdot)} = 1 \right] \right|,$$

where Rand is an oracle which on input $(N, A, M) \in \mathcal{N} \times \mathcal{A} \times \mathcal{M}$ outputs a random[9] string of length $|\Pi.\mathsf{Enc}_K(N, A, M)|$ and Rej is an oracle which always outputs $\perp$. The adversary is not allowed to make a decryption query (N, A, C) if a previous encryption query (N, A, M) returned C. The adversary is said nonce-respecting if it never repeats a nonce $N \in \mathcal{N}$ in its encryption queries, in which case we denote its advantage $\mathbf{Adv}_{\Pi}^{\mathrm{nAE}}(\mathsf{A})$.

Note that in the general case where the adversary is allowed to repeat nonces, Π can be seen as a deterministic AE scheme [55] with header space (in the terms of [55]) $\mathcal{N} \times \mathcal{A}$, so that one exactly recovers the definition of the MRAE notion of Rogaway and Shrimpton [55] (which we simply abbreviate to AE here).

ADVERSARY CHARACTERISTICS. In all the paper, given some implicit parameter n, a (q, m, ℓ, σ, t)-adversary against a nonce-based scheme is an adversary:

- which makes at most q oracle queries; when the adversary has access to two oracles (i.e., when attacking the MAC-security of a keyed function or a nAE scheme), this means q queries in total to both oracles;
- which uses any nonce at most m times throughout its queries ($m = 1$ for a nonce-respecting adversary); when the adversary has access to two oracles, this only applies to queries to its first oracle (MAC or encryption oracle);
- such that the length of any of its queries (nonce excluded) is at most ℓ blocks of n bits; for a keyed function with domain $\mathcal{D} = \mathcal{A} \times \mathcal{M}$ or a nAE scheme, this means that *both* the AD length and the message length of any query is at most ℓ blocks of n bits;
- such that the total length of all its queries (nonce excluded) is at most σ blocks of n bits; for a keyed function with domain $\mathcal{D} = \mathcal{A} \times \mathcal{M}$ or a nAE scheme, this means the sum of the AD and the message length over all queries;
- which runs in time at most t.

4   The CTRT Encryption Mode

4.1   Syntax and Security of nivE Schemes

Most existing encryption schemes are either nonce-based [53] or IV-based [7], i.e., they employ an externally provided value which either should not repeat (nonce), or should be selected uniformly at random (IV). (See also [46]).

---

[9] We assume that Rand returns the same output if a query is repeated.

Here, we introduce the notion of combined nonce- and IV-based encryption scheme (*nivE* for short).

Syntactically, a nivE scheme is a tuple $\Pi = (\mathcal{K}, \mathcal{N}, \mathcal{IV}, \mathcal{M}, \mathsf{Enc}, \mathsf{Dec})$ where $\mathcal{K}$, $\mathcal{N}$, $\mathcal{IV}$ and $\mathcal{M}$ are non-empty sets and Enc and Dec are deterministic algorithms. The encryption algorithm Enc takes as input a key $K \in \mathcal{K}$, a nonce $N \in \mathcal{N}$, an initial value $IV \in \mathcal{IV}$, and a message $M \in \mathcal{M}$, and outputs a binary string $C \in \{0,1\}^*$ (we assume that Enc returns $\perp$ if one of the inputs is not in the intended set). The decryption algorithm Dec takes as input a key $K \in \mathcal{K}$, a nonce $N \in \mathcal{N}$, an initial value $IV \in \mathcal{IV}$, and a binary string $C \in \{0,1\}^*$, and outputs either a message $M \in \mathcal{M}$, or a special symbol $\perp$. We require that

$$\mathsf{Dec}(K, N, IV, \mathsf{Enc}(K, N, IV, M)) = M$$

for all tuples $(K, N, IV, M) \in \mathcal{K} \times \mathcal{N} \times \mathcal{IV} \times \mathcal{M}$.

We denote $\mathsf{Enc}^{\$}$ the probabilistic algorithm which takes as input $(K, N, M) \in \mathcal{K} \times \mathcal{N} \times \mathcal{M}$, internally generates a uniformly random $IV \leftarrow_{\$} \mathcal{IV}$, computes $C = \mathsf{Enc}(K, N, IV, M)$, and outputs $(IV, C) \in \mathcal{IV} \times \{0,1\}^*$. We write $\mathsf{Enc}_K(N, IV, M)$ for $\mathsf{Enc}(K, N, IV, M)$ and $\mathsf{Enc}_K^{\$}(N, M)$ for $\mathsf{Enc}^{\$}(K, N, M)$. The security of a nivE scheme is defined as follows.

Definition 5 (Security of a nivE Scheme). *Let $\Pi = (\mathcal{K}, \mathcal{N}, \mathcal{IV}, \mathcal{M}, \mathsf{Enc}, \mathsf{Dec})$ be a nivE scheme. The advantage of an adversary A in breaking Π is defined as*

$$\mathbf{Adv}_{\Pi}^{\mathrm{ivE}}(\mathsf{A}) = \left| \Pr \left[K \leftarrow_{\$} \mathcal{K} : \mathsf{A}^{\Pi.\mathsf{Enc}_K^{\$}(\cdot,\cdot)} = 1 \right] - \Pr \left[\mathsf{A}^{\mathsf{Rand}(\cdot,\cdot)} = 1 \right] \right|,$$

where Rand is an oracle which on input $(N, M) \in \mathcal{N} \times \mathcal{M}$ outputs a random string of length $|\Pi.\mathsf{Enc}_K^{\$}(N, M)|$. The adversary is said nonce-respecting *if it never repeats a nonce $N \in \mathcal{N}$ in its oracle queries, in which case we denote its advantage $\mathbf{Adv}_{\Pi}^{\mathrm{nivE}}(\mathsf{A})$.*

Note that when the adversary is allowed to repeat nonces, Π can be seen as a family of purely IV-based encryption (ivE) schemes [46] indexed by the nonce space $\mathcal{N}$, hence our notation of the advantage in that case.

4.2   Definition and Analysis of the CTRT Mode

We now define the CTRT (*CounTeR in Tweak*) mode, turning a tweakable block cipher into a nivE scheme. Let $\mathcal{K}$ and $\mathcal{T}$ be non-empty sets, and let $\widetilde{E} \in \mathsf{TBC}(\mathcal{K}, \mathcal{T}', \mathcal{X})$ be a tweakable block cipher with key space $\mathcal{K}$, tweak space[10] $\mathcal{T}' = \{1\} \times \mathcal{T}$, and domain $\mathcal{X} = \{0,1\}^n$. Let Inc be a cyclic permutation of $\mathcal{T}$. We construct from $\widetilde{E}$ a nivE scheme $\mathsf{CTRT}[\widetilde{E}]$ with key space $\mathcal{K}$, nonce space $\mathcal{N} = \mathcal{X} = \{0,1\}^n$, IV space $\mathcal{IV} = \mathcal{T}$, and message space $\mathcal{M} = \{0,1\}^*$ as defined in Fig. 2 and illustrated on bottom of Fig. 1.

---

[10] The CTRT mode does not need tweak separation per se. We use a single 1 prefix in order to conveniently combine CTRT with EPWC later.

```
1  algorithm CTRT[Ẽ].Enc_K(N, IV, M)
2    ℓ := |M|/n
3    parse M as M_1‖···‖M_ℓ, with |M_1| = ... = |M_{ℓ-1}| = n and 1 ≤ |M_ℓ| ≤ n
4    for i = 1 to ℓ do
5      C_i := M_i ⊕ Ẽ_K^{1,IV}(N)
6      IV := Inc(IV)
7    return C_1‖C_2‖···‖C_ℓ
```

Fig. 2. Definition of the CTRT mode, using a TBC $\widetilde{E} \in \mathsf{TBC}(\mathcal{K}, \mathcal{T}', \mathcal{X})$ with $\mathcal{T}' = \{1\} \times \mathcal{T}$ and $\mathcal{X} = \{0,1\}^n$.

The security of CTRT is captured by Theorem 1 below. Logarithms are in base 2 and $t_{\mathsf{CTRT}}(\sigma)$ is an upper bound on the time needed for computing $\mathsf{CTRT}[\widetilde{E}].\mathsf{Enc}_K$ on inputs of total message length at most σ blocks of n bits when calls to $\widetilde{E}_K$ cost unit time.

Theorem 1 (Security of CTRT). *Let $\widetilde{E} \in \mathsf{TBC}(\mathcal{K}, \mathcal{T}', \mathcal{X})$ with $\mathcal{X} = \{0,1\}^n$, $\mathcal{T}' = \{1\} \times \mathcal{T}$, and $|\mathcal{T}| \geq 8$. Let A be a (q, m, ℓ, σ, t)-adversary against $\mathsf{CTRT}[\widetilde{E}]$ with $\ell \leq |\mathcal{T}|$. Then there exists an adversary A' against the TPRP-security of $\widetilde{E}$, making at most σ oracle queries and running in time at most $t + t_{\mathsf{CTRT}}(\sigma)$, such that*

$$\mathbf{Adv}^{\mathrm{ivE}}_{\mathsf{CTRT}[\widetilde{E}]}(\mathsf{A}) \leq \mathbf{Adv}^{\mathrm{TPRP}}_{\widetilde{E}}(\mathsf{A}') + \frac{2(m-1)\sigma + 1}{|\mathcal{T}|} + f(\sigma),$$

where

$$f(\sigma) = \frac{2\sigma \log^2 \sigma}{|\mathcal{X}|} \qquad \textit{when } 8 \leq \sigma \leq |\mathcal{T}|,$$
$$= \frac{2\sigma^2 \log^2 |\mathcal{T}|}{|\mathcal{X}||\mathcal{T}|} \qquad \textit{when } \sigma \geq |\mathcal{T}|.$$

In particular, if A is nonce-respecting ($m = 1$), one has

$$\mathbf{Adv}^{\mathrm{nivE}}_{\mathsf{CTRT}[\widetilde{E}]}(\mathsf{A}) \leq \mathbf{Adv}^{\mathrm{TPRP}}_{\widetilde{E}}(\mathsf{A}') + \frac{1}{|\mathcal{T}|} + f(\sigma).$$

Before proceeding to the proof, we comment the security bound of this theorem. Consider first the case of a nonce-respecting adversary A. Assuming $|\mathcal{T}| \geq |\mathcal{X}|$, then A must makes queries of total message length σ blocks of n bits with σ close to $|\mathcal{X}| = 2^n$ (neglecting logarithmic factors) before being able to distinguish the outputs of $\mathsf{CTRT}[\widetilde{E}]$ from random.[11] On the other hand, if

---

[11] Note that in that case the size of the tweak space $\mathcal{T}$ only impacts the maximal message length ℓ, not the security bound.

$|\mathcal{T}| = 2^w < |\mathcal{X}|$, then $\mathsf{CTRT}[\widetilde{E}]$ is secure up to roughly $2^{(n+w)/2}$ TBC calls (again, neglecting logarithmic factors), which is always larger than $2^{n/2}$. In particular, if $w = n/2$ (as e.g. for KIASU-BC [32]), then security is ensured up to roughly $2^{3n/4}$ TBC calls. In the nonce-misuse scenario, note that the additional term $2(m-1)\sigma/|\mathcal{T}|$ remains small as long as nonces are not repeated too many times (e.g. $m \leq 100$) and $\sigma \ll |\mathcal{T}|$, and turns into a birthday-like term only in the extreme case where a few nonces are repeated close to σ times. This means that a few nonce repetitions will not hurt and that nonces must be "seriously" mishandled before security goes down to birthday bound.

PROOF OF THEOREM 1. Fix a $(q', m, |\mathcal{T}|, \sigma, t)$-adversary A against $\mathsf{CTRT}[\widetilde{E}]$ (we denote q' the maximal number of adversarial queries and will later use q for the actual number of queries in a specific attack). The first part of the proof is standard, and consists in introducing an intermediate game where all calls to $\widetilde{E}_K$ in the CTRT construction are replaced by calls to a random tweakable permutation $\widetilde{P}$. Consider the following adversary A' against the TPRP-security of $\widetilde{E}$. Let $G \in \{\widetilde{E}_K, \widetilde{P}\}$ be the oracle to which A' has access. Adversary A' runs A, answers its encryption queries (N, M) by drawing a random IV and executing the code in Fig. 2 on input (N, IV, M), replacing calls to $\widetilde{E}_K$ by oracle calls to G, and finally outputs the same bit as A. Clearly, A' makes at most σ oracle queries and runs in time at most $t + t_{\mathsf{CTRT}}(\sigma)$. Moreover, it is easy to see that

$$\mathbf{Adv}_{\mathsf{CTRT}[\widetilde{E}]}^{\mathrm{ivE}}(\mathsf{A}) \leq \mathbf{Adv}_{\widetilde{E}}^{\mathrm{TPRP}}(\mathsf{A}') + \delta, \tag{1}$$

where

$$\delta = \left| \Pr\left[\widetilde{P} \leftarrow_{\$} \mathsf{TP}(\mathcal{T}, \mathcal{X}) : \mathsf{A}^{\mathsf{CTRT}[\widetilde{P}].\mathsf{Enc}^{\$}} = 1 \right] - \Pr\left[\mathsf{A}^{\mathsf{Rand}} = 1 \right] \right| \tag{2}$$

and $\mathsf{CTRT}[\widetilde{P}]$ is a slight abuse of notation for the CTRT construction based on an arbitrary tweakable permutation $\widetilde{P}$.

Upper bounding δ is now a purely information-theoretic problem, so that we allow A to be computationally unbounded, and hence, *wlog*, deterministic. The adversary is now trying to distinguish between $\mathsf{CTRT}[\widetilde{P}]$ for a random $\widetilde{P}$ (thereafter called the "real world") and Rand (thereafter called the "ideal world"). We assume *wlog* that A always makes queries of length a multiple of the block length n, and of total length σ blocks (if not, we pad all queries whose final block is incomplete with zeros for free, which can only increase the adversary's advantage).

Following the H-coefficients method [15,48], we summarize the interaction of A with its oracle in the so-called *transcript* of the attack

$$\tau = ((N_1, M_1, IV_1, C_1), \ldots, (N_q, M_q, IV_q, C_q)),$$

where (N_i, M_i) denotes the i-th query of the attacker and (IV_i, C_i) the corresponding answer of the oracle. Furthermore, we denote $M_i = M_{i,1} \| \cdots \| M_{i,\ell_i}$, $C_i = C_{i,1} \| \cdots \| C_{i,\ell_i}$, where ℓ_i is the number of blocks of the i-th message, and

$IV_{i,j} = \mathsf{Inc}^{j-1}(IV_i)$ the j-th counter for the i-th message, $j = 1, \ldots, \ell_i$. Let Θ_{re}, resp. Θ_{id}, denote the distribution of the transcript in the real world, resp. ideal world. We say that a transcript τ is A-attainable (or simply attainable) if the probability to obtain τ in the ideal world is non-zero. Note that the number of queries q and the lengths of the queries $\ell_1, \ldots, \ell_q$ are themselves random variables (they can vary for distinct A-attainable transcripts), yet by the assumption that the attacker always asks the maximal number of allowed blocks throughout its queries, one always has $\sum_{i=1}^{q} \ell_i = \sigma$.

From τ we define for each possible tweak $T \in \mathcal{T}$ the "load" of the tweak as

$$L(T) = |\{(i,j) : IV_{i,j} = T\}|.$$

In words, $L(T)$ is the number of times the tweak T appears as a counter when encrypting the queries of the adversary. Clearly, one has

$$\sum_{T \in \mathcal{T}} L(T) = \sigma. \tag{3}$$

The proof relies on the fundamental lemma of the H-coefficients technique (see e.g. [15] for the proof).

Lemma 1. *Assume that the set of A-attainable transcripts is partitioned into two disjoint sets* GoodT *and* BadT, *and that there exists ε_1 and ε_2 such that for any $\tau \in$ GoodT, one has*

$$\frac{\Pr\left[\Theta_{\mathrm{re}} = \tau\right]}{\Pr\left[\Theta_{\mathrm{id}} = \tau\right]} \geq 1 - \varepsilon_1,$$

and $\Pr\left[\Theta_{\mathrm{id}} \in \mathsf{BadT}\right] \leq \varepsilon_2$. *Then* $\delta \leq \varepsilon_1 + \varepsilon_2$, *with δ as defined by* (2).

We say that an attainable transcript τ is bad if one of the two following conditions are met:

(C-1) there exists $(i,j) \neq (i',j')$ such that $IV_{i,j} = IV_{i',j'}$ and $N_i = N_{i'}$;
(C-2) there exists $(i,j) \neq (i',j')$ such that $IV_{i,j} = IV_{i',j'}$, $N_i \neq N_{i'}$, and $M_{i,j} \oplus C_{i,j} = M_{i',j'} \oplus C_{i',j'}$.

Note that condition (C-1) can only be satisfied for a nonce-misuse adversary, since (by the assumption that the length of each query is at most $|\mathcal{T}|$ blocks of n bits so that counters do not loop) $IV_{i,j} = IV_{i',j'}$ requires $i \neq i'$, which implies that $N_i \neq N_{i'}$ for a nonce-respecting adversary. Note also that the condition (C-2) can only be satisfied in the ideal world. Indeed, in the real world, $M_{i,j} \oplus C_{i,j} = \widetilde{P}(IV_{i,j}, N_i)$ and $M_{i',j'} \oplus C_{i',j'} = \widetilde{P}(IV_{i',j'}, N_{i'})$, so that if $IV_{i,j} = IV_{i',j'}$ and $N_i \neq N_{i'}$ one necessarily has $M_{i,j} \oplus C_{i,j} \neq M_{i',j'} \oplus C_{i',j'}$.

We let BadT be the set of bad transcripts, and GoodT be the set of attainable transcripts which are not bad, henceforth called good transcripts. We first consider good transcripts.

Lemma 2. *Let $\tau \in \mathsf{GoodT}$ be a good transcript. Then*

$$\frac{\Pr[\Theta_{\mathrm{re}} = \tau]}{\Pr[\Theta_{\mathrm{id}} = \tau]} \geq 1.$$

Proof. Note that a good transcript has the property that for each $(i,j) \neq (i',j')$ such that $IV_{i,j} = IV_{i',j'}$, one has $N_i \neq N_i'$ and $M_{i,j} \oplus C_{i,j} \neq M_{i',j'} \oplus C_{i',j'}$. In other words, the transcript encodes a partial tweakable permutation, where for each tweak $T \in \mathcal{T}$ there are exactly $L(T)$ distinct values N_i mapped to some value $M_{i,j} \oplus C_{i,j}$. The probability to obtain a good transcript τ in the ideal and real worlds can now be easily computed. In the ideal world, since the IV_i's and the C_i's are uniformly random, one has

$$\Pr[\Theta_{\mathrm{id}} = \tau] = \frac{1}{|\mathcal{IV}|^q \cdot |\mathcal{X}|^\sigma}.$$

In the real world, the IV_i's are random as well, but now the probability to obtain the C_i's can easily be seen to be the probability that the random tweakable permutation $\widetilde{P}$ is compatible with the partial tweakable permutation encoded by τ [15]. Hence, one has

$$\Pr[\Theta_{\mathrm{re}} = \tau] = \frac{1}{|\mathcal{IV}|^q} \cdot \prod_{T \in \mathcal{T}} \frac{1}{(|\mathcal{X}|)_{L(T)}},$$

where $(a)_b$ denotes the falling factorial $a(a-1)\cdots(a-b+1)$, with $(a)_0 = 1$ by convention. From this, we deduce that

$$\frac{\Pr[\Theta_{\mathrm{re}} = \tau]}{\Pr[\Theta_{\mathrm{id}} = \tau]} = \frac{|\mathcal{X}|^\sigma}{\prod_{T \in \mathcal{T}}(|\mathcal{X}|)_{L(T)}} \overset{(3)}{=} \prod_{T \in \mathcal{T}} \frac{|\mathcal{X}|^{L(T)}}{(|\mathcal{X}|)_{L(T)}} \geq 1.$$

$\square$

It remains to upper bound the probability to obtain a bad transcript in the ideal world. For $i \in \{1, 2\}$, let BadT_i be the set of attainable transcripts satisfying condition (C-i). We first consider condition (C-1).

Lemma 3. *One has*

$$\Pr[\Theta_{\mathrm{id}} \in \mathsf{BadT}_1] \leq \frac{2(m-1)\sigma}{|\mathcal{T}|}.$$

Proof. Consider two distinct queries (N_i, M_i) and $(N_{i'}, M_{i'})$. If the nonces are the same ($N_i = N_{i'}$), then the probability, over the random draw of IV_i and $IV_{i'}$ in $\mathcal{T}$, that there exists j and j' such that $IV_{i,j} = IV_{i',j'}$, is $(\ell_i + \ell_{i'} - 1)/|\mathcal{T}|$. If the nonces are distinct, then clearly condition (C-1) cannot be satisfied for i and i'. Hence, summing over all possible nonces, we have

$$\Pr[\Theta_{\mathrm{id}} \in \mathsf{BadT}_1] \leq \sum_{N \in \mathcal{N}} \sum_{\substack{1 \leq i < i' \leq q \\ N_i = N_{i'} = N}} \frac{\ell_i + \ell_{i'} - 1}{|\mathcal{T}|}.$$

Fix some nonce N, and assume for notational simplicity that the first q' queries use nonce N, with $q' \leq m$ by assumption. Then the probability that condition (C-1) is met for nonce N is at most

$$\sum_{i=1}^{q'-1} \sum_{i'=i+1}^{q'} \frac{\ell_i + \ell_{i'} - 1}{|\mathcal{T}|} \leq \sum_{i=1}^{q'-1} \frac{(q'-1)\ell_i + \ell(N)}{|\mathcal{T}|}$$

$$\leq \frac{2(q'-1)\ell(N)}{|\mathcal{T}|}$$

$$\leq \frac{2(m-1)\ell(N)}{|\mathcal{T}|},$$

where $\ell(N)$ is the total length of queries using nonce N. The result follows by summing over all possible nonces, using $\sum_{N \in \mathcal{N}} \ell(N) = \sigma$. $\square$

We handle condition (C-2) in the following lemma.

Lemma 4. *One has*

$$\Pr\left[\Theta_{\mathrm{id}} \in \mathsf{BadT}_2\right] \leq \frac{1}{|\mathcal{T}|} + \min\{\sigma, |\mathcal{T}|\} \cdot \frac{(L_{\max})^2}{2|\mathcal{X}|},$$

where $L_{\max} = 2 \log \sigma$ when $8 \leq \sigma \leq |\mathcal{T}|$ and $L_{\max} = \frac{2\sigma \log |\mathcal{T}|}{|\mathcal{T}|}$ when $\sigma \geq |\mathcal{T}|$.

Proof. Let BadT_3 be the set of transcripts satisfying the following condition ($L_{\max}$ being defined as in the statement of the lemma):
(C-3) there exists $T \in \mathcal{T}$ such that $L(T) \geq L_{\max}$.
Then

$$\Pr[\Theta_{\mathrm{id}} \in \mathsf{BadT}_2] \leq \Pr\left[\Theta_{\mathrm{id}} \in \mathsf{BadT}_2 \mid \Theta_{\mathrm{id}} \notin \mathsf{BadT}_3\right] + \Pr\left[\Theta_{\mathrm{id}} \in \mathsf{BadT}_3\right].$$

Note that in the ideal world, the values $L(T)$ only depend on the random draw of the IV_i's, and that once the $L(T)$'s are fixed, condition (C-2) only depends on the random draw of the $C_{i,j}$'s. In particular, since in the ideal world the $C_{i,j}$'s are uniformly random, one has

$$\Pr\left[\Theta_{\mathrm{id}} \in \mathsf{BadT}_2 \mid \Theta_{\mathrm{id}} \notin \mathsf{BadT}_3\right]$$

$$\leq \sum_{T \in \mathcal{T}} \sum_{\substack{(i,j),(i',j') \\ IV_{i,j}=IV_{i',j'}=T}} \Pr\left[M_{i,j} \oplus C_{i,j} = M_{i',j'} \oplus C_{i',j'}\right]$$

$$\leq \sum_{T \in \mathcal{T}} \frac{L(T)(L(T) - 1)}{2|\mathcal{X}|}$$

$$\leq \min\{\sigma, |\mathcal{T}|\} \cdot \frac{(L_{\max})^2}{2|\mathcal{X}|},$$

where for the third inequality we used that there are at most $\min\{\sigma, |\mathcal{T}|\}$ tweaks T such that $L(T) \geq 1$.

It remains to upper bound the probability that condition (C-3) is satisfied, which can be recast as a "balls-into-bins" problem. Thinking of each tweak T as a bin, each random IV_i determines a sequence of ℓ_i consecutive[12] bins where a ball is thrown. If the attacker only made queries of length one block, then this would be a standard "balls-into-bins" problem, where each ball is thrown independently in a bin chosen uniformly at random, and we could use classical results about the maximal occupancy of any bin directly. However, the attacker can choose the length of each message at will and we need to take this into account.[13] Intuitively, for some fixed total number σ of balls, using messages of length $\ell_i > 1$ should *lower* the maximal occupancy since balls thrown in consecutive bins cannot end in the same bin. We formalize this intuition in a separate Lemma below, which implies that

$$\Pr\left[\Theta_{\mathrm{id}} \in \mathsf{BadT}_3\right] \leq \frac{1}{|\mathcal{T}|}.$$

The result follows.   □

The lemma below is a simple variant on the standard balls-into-bins problem. A similar result was proved in [6] (and potentially in many other papers).

Lemma 5. *Consider a set of $|\mathcal{T}| \geq 8$ bins and $\sigma \geq 8$ balls. Fix an integer $q \leq \sigma$ and a sequence of integers $(\ell_1, \ldots, \ell_q)$ with $1 \leq \ell_i \leq |\mathcal{T}|$ and $\sum_{i=1}^{q} \ell_i = \sigma$. Consider the following random process: for $i = 1, \ldots, q$, a chain of ℓ_i balls is thrown in consecutive bins, the initial bin being chosen independently and uniformly at random. Then the probability that, at the end of the process, any bin contains $L_{\max}$ balls or more, is less than $1/|\mathcal{T}|$, where*

(a) $L_{\max} = 2 \log \sigma$ when $\sigma \leq |\mathcal{T}|$;
(b) $L_{\max} = \frac{2\sigma \log |\mathcal{T}|}{|\mathcal{T}|}$ when $\sigma \geq |\mathcal{T}|$.

Proof. See the full version of the paper [50].

COMPLETING THE PROOF OF THEOREM 1. From Lemmas 3 and 4, we obtain by the union bound that

$$\Pr\left[\Theta_{\mathrm{id}} \in \mathsf{BadT}\right] \leq \frac{2(m-1)\sigma + 1}{|\mathcal{T}|} + f(\sigma), \tag{4}$$

with $f(\sigma)$ as in the statement of Theorem 1. Combining (4) with Lemmas 1 and 2 (taking $\varepsilon_1 = 0$), we obtain the same upper bound for δ (defined by (2)) as for $\Pr\left[\Theta_{\mathrm{id}} \in \mathsf{BadT}\right]$. Finally, Eq. (1) yields the result.

VARIANTS. In the full version of the paper [50], we describe two variants of CTRT, a purely nonce-based one and a purely IV-based one.

---

[12] The successor of the tweak T is $\mathsf{Inc}(T)$.

[13] Note that the adversary must commit to the length ℓ_i of the chain *before* knowing the initial bin IV_i since it first makes the query (N_i, M_i) and only then receives the answer (IV_i, C_i).

5   The PWC and EPWC Message Authentication Codes

In this section, we describe two related modes for message authentication, PWC (*Parallel Wegman-Carter*) and EPWC (*Encrypted PWC*). Let $\mathcal{K}$ and $\mathcal{T}$ be two sets, and let $\widetilde{E}$ be a tweakable block cipher with key space $\mathcal{K}$, tweak space[14] $\mathcal{T}' = \{2, \ldots, 5\} \times \mathcal{T}$, and domain $\mathcal{X} = \{0,1\}^n$. Let Inc be a cyclic permutation of $\mathcal{T}$. From $\widetilde{E}$, we construct two nonce-based keyed functions, PWC$[\widetilde{E}]$ and EPWC$[\widetilde{E}]$, both with key space $\mathcal{K}$, nonce-space $\mathcal{N} = \mathcal{X} = \{0,1\}^n$, domain $\mathcal{D} = \mathcal{A} \times \mathcal{M}$, where $\mathcal{A} = \mathcal{M} = \{0,1\}^*$,[15] and range $\mathcal{Y} = \mathcal{X} = \{0,1\}^n$, as defined in Fig. 3 and illustrated on top of Fig. 1 (for PWC, just omit the final call to $\widetilde{E}_K^{4,0}$). We will prove that both PWC$[\widetilde{E}]$ and EPWC$[\widetilde{E}]$ are 2^n-secure as nonce-based MAC and nonce-based PRF, and that EPWC$[\widetilde{E}]$ is moreover a birthday bound-secure PRF in the nonce-misuse scenario.

The PWC construction follows the Wegman-Carter paradigm [14,56,60] by combining a xor-universal hash function H inspired from PMAC [13,52] applied to (A, M), and a pseudorandom function F applied to the nonce N. This pseudorandom function is constructed from $\widetilde{E}$ by summing two independent pseudorandom permutations in order to obtain security beyond the birthday bound [42]. The EPWC construction is simply PWC with an additional layer of encryption to provide nonce-misuse resistance.

Before stating and proving the security results for (E)PWC, we focus on how to obtain the BBB-secure pseudorandom function F from $\widetilde{E}$. A straightforward way would be to "put the nonce in the tweak", e.g.,

$$F'_K(N) = \widetilde{E}_K^{6,N}(0).$$

This would result in a uniformly random value for each new nonce, but this is only possible when the intended nonce space is smaller than the effective tweak space $\mathcal{T}$ of $\widetilde{E}$. In order to allow the nonce length to be as large as the block length of $\widetilde{E}$, we use instead the "sum-of-PRPs" construction by defining (the exact tweak prefixes are unimportant)

$$F_K(N) = \widetilde{E}_K^{2,0}(N) \oplus \widetilde{E}_K^{2,1}(N). \tag{5}$$

The pseudorandomness of this construction has been well studied. Assuming that $\widetilde{E}_K^{2,0}$ and $\widetilde{E}_K^{2,1}$ are perfectly random and independent permutations, Lucks [42, Theorem 5] showed that an information-theoretic adversary trying to distinguish F_K from a random function $\rho : \{0,1\}^n \to \{0,1\}^n$ within q queries has an advantage upper bounded by $q^3/2^{2n-1}$ (see also [16]). Better bounds were proposed in three different papers: Bellare and Impagliazzo [8] proved that the advantage is upper bounded by $\mathcal{O}(n)(q/2^n)^{1.5}$, while Patarin proved in two different

---

[14] We use a set of prefixes which is disjoint from the set used for the CTRT mode in order to later combine the two modes smoothly.

[15] When constructing an AE scheme, it is more convenient to directly define a vector-input MAC, rather than a string-input MAC that must later be transformed to handle vectors of strings, as required for an AE scheme.

1 **algorithm** $\mathsf{PWC}[\widetilde{E}]_K(N, A, M)$ $\boxed{\mathsf{EPWC}[\widetilde{E}]_K(N, A, M)}$

2   $\ell_a := |A|/n$

3   $\ell_m := |M|/n$

4   parse A as $A_1\|\cdots\|A_{\ell_a}$, with $|A_1| = \ldots = |A_{\ell_a-1}| = n$, $1 \le |A_{\ell_a}| \le n$

5   parse M as $M_1\|\cdots\|M_{\ell_m}$, with $|M_1| = \ldots = |M_{\ell_m-1}| = n$, $1 \le |M_{\ell_m}| \le n$

6   $\mathsf{auth} := \widetilde{E}_K^{2,0}(N) \oplus \widetilde{E}_K^{2,1}(N)$

7   **if** $\ell_a > 0$ **then**

8   **for** $i = 1$ **to** $\ell_a - 1$ **do**

9       $\mathsf{auth} := \mathsf{auth} \oplus \widetilde{E}_K^{2,i+1}(A_i)$

10   **if** $|A_{\ell_a}| = n$ **then**

11      $\mathsf{auth} := \mathsf{auth} \oplus \widetilde{E}_K^{2,\ell_a+1}(A_{\ell_a})$

12   **else**

13      $\mathsf{auth} := \mathsf{auth} \oplus \widetilde{E}_K^{3,\ell_a+1}(A_{\ell_a}10^*)$

14   **if** $\ell_m > 0$ **then**

15   **for** $i = 1$ **to** $\ell_m - 1$ **do**

16      $\mathsf{auth} := \mathsf{auth} \oplus \widetilde{E}_K^{4,i}(M_i)$

17   **if** $|M_{\ell_m}| = n$ **then**

18      $\mathsf{auth} := \mathsf{auth} \oplus \widetilde{E}_K^{4,\ell_m}(M_{\ell_m})$

19   **else**

20      $\mathsf{auth} := \mathsf{auth} \oplus \widetilde{E}_K^{5,\ell_m}(M_{\ell_m}10^*)$

21   $\boxed{\mathsf{tag} := \widetilde{E}_K^{4,0}(\mathsf{auth})}$

22   **return** tag

Fig. 3. Definition of the PWC and EPWC modes, using a TBC $\widetilde{E} \in \mathsf{TBC}(\mathcal{K}, \mathcal{T}', \mathcal{X})$ with $\mathcal{T}' = \{2, \ldots, 5\} \times \mathcal{T}$ and $\mathcal{X} = \{0, 1\}^n$. The boxed statement only applies to EPWC. For notational simplicity, we identify $\mathcal{T}$ with $\{0, \ldots, |\mathcal{T}| - 1\}$ and $\mathsf{Inc}^i(0)$ with i.

ways [47,49] an upper bound $\mathcal{O}(q/2^n)$. However, in all three cases the exact $\mathcal{O}(\cdot)$ function was left unspecified and the upper bound was not explicitly worked out. For the sake of concreteness, we propose the following optimistic conjecture.

Conjecture 1. There is an absolute constant C such the advantage of any adversary trying to distinguish the sum of two independent random permutations of $\mathcal{X}$ from a random function from $\mathcal{X}$ to $\mathcal{X}$ within q queries is at most $Cq/|\mathcal{X}|$.

The security of PWC and EPWC is captured by Theorems 2 and 3 below. We denote by $t_{\mathsf{PWC}}(\sigma)$, resp. $t_{\mathsf{EPWC}}(\sigma)$, an upper bound on the time needed to compute $\mathsf{PWC}[\widetilde{E}]$, resp. $\mathsf{EPWC}[\widetilde{E}]$ on inputs of total (AD + message) length at most σ blocks of n bits when calls to $\widetilde{E}_K$ cost unit time.

Theorem 2 (PRF-Security of PWC and EPWC). *Let* $\widetilde{E} \in \mathsf{TBC}(\mathcal{K}, \mathcal{T}', \mathcal{X})$ *with* $\mathcal{X} = \{0, 1\}^n$ *and* $\mathcal{T}' = \{2, \ldots, 5\} \times \mathcal{T}$, *and assume Conjecture 1. Let* A *be a* (q, m, ℓ, σ, t)-*adversary against the PRF-security of* $\mathsf{PWC}[\widetilde{E}]$, *resp.* $\mathsf{EPWC}[\widetilde{E}]$,

with $\ell \leq |\mathcal{T}| - 2$. *Then there exists an absolute constant C and an adversary* A', *resp.* A'', *against the TPRP-security of* $\widetilde{E}$, *making at most* $\sigma + 2q$, *resp.* $\sigma + 3q$ *oracle queries and running it time at most* $t + t_{\mathsf{PWC}}(\sigma)$, *resp.* $t + t_{\mathsf{EPWC}}(\sigma)$, *such that*

(a) if A *is nonce-respecting* ($m = 1$), *then*

$$\mathbf{Adv}^{\mathrm{nPRF}}_{\mathsf{PWC}[\widetilde{E}]}(\mathsf{A}) \leq \mathbf{Adv}^{\mathrm{TPRP}}_{\widetilde{E}}(\mathsf{A}') + \frac{Cq}{|\mathcal{X}|};$$

$$\mathbf{Adv}^{\mathrm{nPRF}}_{\mathsf{EPWC}[\widetilde{E}]}(\mathsf{A}) \leq \mathbf{Adv}^{\mathrm{TPRP}}_{\widetilde{E}}(\mathsf{A}'') + \frac{Cq}{|\mathcal{X}|};$$

(b) if A *is allowed to repeat nonces* ($m > 1$), *then*

$$\mathbf{Adv}^{\mathrm{PRF}}_{\mathsf{EPWC}[\widetilde{E}]}(\mathsf{A}) \leq \mathbf{Adv}^{\mathrm{TPRP}}_{\widetilde{E}}(\mathsf{A}'') + \frac{q^2}{|\mathcal{X}|}.$$

Proof. Fix a $(q, m, |\mathcal{T}| - 2, \sigma, t)$-adversary A against the PRF-security of $\mathsf{PWC}[\widetilde{E}]$ or $\mathsf{EPWC}[\widetilde{E}]$, trying to distinguish the construction from a random function $R \leftarrow_{\$} \mathsf{Func}(\mathcal{N} \times \mathcal{D}, \mathcal{Y})$, where $\mathcal{D} = \mathcal{A} \times \mathcal{M}$. We start by proving (a), assuming A is nonce-respecting ($m = 1$). First, slightly abusing the notation, let us see $(\mathsf{E})\mathsf{PWC}$ as a construction based on an arbitrary tweakable permutation, identifying $(\mathsf{E})\mathsf{PWC}[\widetilde{E}]_K$ with $(\mathsf{E})\mathsf{PWC}[\widetilde{E}_K]$. We start by replacing $\widetilde{E}_K$ in the security experiment by a uniformly random tweakable permutation $\widetilde{P}$. One can see $\mathsf{A}^{\mathsf{PWC}[\cdot]}$, resp. $\mathsf{A}^{\mathsf{EPWC}[\cdot]}$, as an adversary A', resp. A'' against the TPRP-security of $\widetilde{E}$, making at most $\sigma + 2q$, resp. $\sigma + 3q$ queries to its oracle (since a query of ℓ_i blocks to PWC, resp. EPWC, costs $\ell_i + 2$, resp. $\ell_i + 3$ calls to $\widetilde{E}$) and running in time at most $t' = t + t_{\mathsf{PWC}}(\sigma)$, resp. $t' = t + t_{\mathsf{EPWC}}(\sigma)$, so that

$$\mathbf{Adv}^{\mathrm{nPRF}}_{\mathsf{PWC}[\widetilde{E}]}(\mathsf{A}) \leq \mathbf{Adv}^{\mathrm{TPRP}}_{\widetilde{E}}(\mathsf{A}') + \delta, \tag{6}$$

$$\mathbf{Adv}^{\mathrm{nPRF}}_{\mathsf{EPWC}[\widetilde{E}]}(\mathsf{A}) \leq \mathbf{Adv}^{\mathrm{TPRP}}_{\widetilde{E}}(\mathsf{A}'') + \delta, \tag{7}$$

where

$$\delta = \left| \Pr\left[\widetilde{P} \leftarrow_{\$} \mathsf{TP}(\mathcal{T}', \mathcal{X}) : \mathsf{A}^{(\mathsf{E})\mathsf{PWC}[\widetilde{P}]} = 1 \right] \right.$$

$$\left. - \Pr\left[R \leftarrow_{\$} \mathsf{Func}(\mathcal{N} \times \mathcal{D}, \mathcal{Y}) : \mathsf{A}^R = 1 \right] \right|. \tag{8}$$

In order to upper bound δ, we abstract the high-level structure of $(\mathsf{E})\mathsf{PWC}[\widetilde{P}]$ as follows. First, we see how A and M are handled as applying a keyed hash function (the key being $\widetilde{P}$) to the pair (A, M), viz.

$$H_{\widetilde{P}}(A, M) \stackrel{\mathrm{def}}{=} \left(\bigoplus_{i=1}^{\ell_a - 1} \widetilde{P}^{2, i+1}(A_i) \right) \oplus \widetilde{P}^{2/3, \ell_a + 1}(A_{\ell_a}(10^*))$$

$$\oplus \left(\bigoplus_{i=1}^{\ell_m - 1} \widetilde{P}^{4, i}(M_i) \right) \oplus \widetilde{P}^{4/5, \ell_m}(M_{\ell_m}(10^*)). \tag{9}$$

We also define a pseudorandom function (again with key $\widetilde{P}$) as

$$F_{\widetilde{P}}(N) \stackrel{\text{def}}{=} \widetilde{P}^{2,0}(N) \oplus \widetilde{P}^{2,1}(N). \tag{10}$$

Then, $(\mathsf{E})\mathsf{PWC}[\widetilde{P}]$ can be written

$$\mathsf{PWC}[\widetilde{P}](N, A, M) = F_{\widetilde{P}}(N) \oplus H_{\widetilde{P}}(A, M), \tag{11}$$

$$\mathsf{EPWC}[\widetilde{P}](N, A, M) = \widetilde{P}^{4,0}\Big(F_{\widetilde{P}}(N) \oplus H_{\widetilde{P}}(A, M)\Big), \tag{12}$$

which should make it clear that the PWC construction follows the Wegman-Carter paradigm [60] with an additional layer of encryption for EPWC (note that the three sets of tweaks used in F, H, and for the final encryption call are disjoint, so that these three building blocks are independent).

We start by showing that the hash function family $(H_{\widetilde{P}})$, with $\widetilde{P} \in \mathsf{TP}(\mathcal{T}', \mathcal{X})$, is xor-universal, i.e., for any two distinct inputs (A, M), (A', M'), and any $X \in \mathcal{X} = \{0,1\}^n$, the probability, over the random draw of $\widetilde{P} \leftarrow_\$ \mathsf{TP}(\mathcal{T}', \mathcal{X})$, that

$$H_{\widetilde{P}}(A, M) \oplus H_{\widetilde{P}}(A', M') = X, \tag{13}$$

is less than $1/|\mathcal{X}|$. Assume that $A \neq A'$ (the reasoning is similar if $A = A'$ and $M \neq M'$), let $\ell_a = |A|/n$ and $\ell'_a = |A'|/n$, and assume $wlog$ that $\ell_a \geq \ell'_a$. Denote $A = A_1 \| \cdots \| A_{\ell_a}$ and $A' = A'_1 \| \cdots \| A'_{\ell'_a}$. Assume first that $\ell_a > \ell'_a$. Then (13) is equivalent to

$$\widetilde{P}^{2/3, \ell_a+1}(A_{\ell_a}(10^*)) = Z,$$

where Z is independent of permutations $\widetilde{P}^{2, \ell_a+1}$ and $\widetilde{P}^{3, \ell_a+1}$, hence the probability is exactly $1/|\mathcal{X}|$. Assume now that $\ell_a = \ell'_a$. There is necessarily an index $i \leq \ell_a$ such that $A_i \neq A'_i$. If $i < \ell_a$, then (13) is equivalent to

$$\widetilde{P}^{2, i+1}(A_i) \oplus \widetilde{P}^{2, i+1}(A'_i) = Z,$$

where Z is a value potentially depending on $\widetilde{P}$ for tweaks different from $(2, i+1)$. Since the probability of this equality (over the random draw of $\widetilde{P}^{2, i+1}$) is either 0 when $Z = 0$ or exactly $1/|\mathcal{X}|$ when $Z \neq 0$, it follows that the condition is met with probability at most $1/|\mathcal{X}|$ in that case. Similarly, if $i = \ell_a$, then (13) is equivalent to

$$\widetilde{P}^{2/3, i+1}(A_i(10^*)) \oplus \widetilde{P}^{2/3, i+1}(A'_i(10^*)) = Z,$$

where Z is a value potentially depending on $\widetilde{P}$ for tweaks different from $(2, i+1)$ and $(3, i+1)$. Again, the condition is met with probability at most $1/|\mathcal{X}|$ in that case. This concludes the proof that H is xor-universal.

As a second step, we replace $F_{\widetilde{P}}$ by a uniformly random function ρ from $\mathcal{N} = \{0,1\}^n$ to $\mathcal{X} = \{0,1\}^n$. Let $\mathsf{PWC}'[\rho, \widetilde{P}]$, resp. $\mathsf{EPWC}'[\rho, \widetilde{P}]$ be defined as in (11), resp. (12), except that $F_{\widetilde{P}}$ is replaced by a call to ρ. Since A is nonce-respecting, then both $\mathsf{PWC}'[\rho, \widetilde{P}]$ and $\mathsf{EPWC}'[\rho, \widetilde{P}]$ are perfectly indistinguishable

from Rand (this is obvious for PWC$'$, while for EPWC$'$ this follows from the fact that applying any fixed permutation to uniformly random values yields uniformly random values). Hence, it remains to upper bound A's advantage in distinguishing (E)PWC$[\widetilde{P}]$ from (E)PWC$'[\rho, \widetilde{P}]$. By a straightforward hybrid argument, this is exactly the advantage of an adversary A$'''$ simulating H (and $\widetilde{P}^{4,0}$ for EPWC) in distinguishing $F_{\widetilde{P}}$ from ρ within at most q queries (since each query to the construction translates in exactly one query to the function applied to the nonce). Using Conjecture 1, this advantage is upper bounded by $Cq/|\mathcal{X}|$. Combining this with (6), resp. (7), we obtain the result.

We then prove (b), assuming A is allowed to repeat nonces ($m > 1$). Exactly as before, one has

$$\mathbf{Adv}^{\mathrm{PRF}}_{\mathsf{EPWC}[\widetilde{E}]}(\mathsf{A}) \leq \mathbf{Adv}^{\mathrm{TPRP}}_{\widetilde{E}}(\mathsf{A}'') + \delta,$$

with δ defined as in (8). We now see EPWC$[\widetilde{P}]$ as a construction based on a universal hash function applied to (N, A, M) followed by a PRF. More precisely, let

$$H'_{\widetilde{P}}(N, A, M) = F_{\widetilde{P}}(N) \oplus H_{\widetilde{P}}(A, M),$$

with H and F as defined in resp. (9) and (10). Then

$$\mathsf{EPWC}[\widetilde{P}](N, A, M) = \widetilde{P}^{4,0}(H'_{\widetilde{P}}(N, A, M)).$$

It is easy to adapt the proof that H is xor-universal to show that H' is also xor-universal (hence, in particular, universal, which is all we need here). The remaining of the proof is now standard [57], and we only sketch it. We first replace $\widetilde{P}^{4,0}$ in EPWC$[\widetilde{P}]$ by a uniformly random function $\rho : \mathcal{X} \to \mathcal{X}$, and denote EPWC$''[\rho, \widetilde{P}]$ the resulting construction. By the PRP-PRF switching lemma, A can distinguish EPWC$[\widetilde{P}]$ from EPWC$''[\rho, \widetilde{P}]$ with advantage at most $q^2/(2|\mathcal{X}|)$, and because H' is universal, it can distinguish EPWC$''[\rho, \widetilde{P}]$ from Rand with advantage at most $q^2/(2|\mathcal{X}|)$. The result follows.   □

Theorem 3 (MAC-Security of PWC and EPWC). *Let $\widetilde{E} \in \mathsf{TBC}(\mathcal{K}, \mathcal{T}', \mathcal{X})$ with $\mathcal{X} = \{0,1\}^n$ and $\mathcal{T}' = \{2, \ldots, 5\} \times \mathcal{T}$, and assume Conjecture 1. Let B be a nonce-respecting $(q, 1, \ell, \sigma, t)$-adversary against the MAC-security of PWC$[\widetilde{E}]$, resp. EPWC$[\widetilde{E}]$, with $\ell \leq |\mathcal{T}| - 2$. Then there exists an absolute constant C and an adversary B$'$, resp. B$''$, against the TPRP-security of $\widetilde{E}$, making at most $\sigma + 2q$, resp. $\sigma + 3q$ oracle queries and running it time at most $t + t_{\mathsf{PWC}}(\sigma)$, resp. $t + t_{\mathsf{EPWC}}(\sigma)$, such that*

$$\mathbf{Adv}^{\mathrm{nMAC}}_{\mathsf{PWC}[\widetilde{E}]}(\mathsf{B}) \leq \mathbf{Adv}^{\mathrm{TPRP}}_{\widetilde{E}}(\mathsf{B}') + \frac{(C+1)q}{|\mathcal{X}|};$$

$$\mathbf{Adv}^{\mathrm{nMAC}}_{\mathsf{EPWC}[\widetilde{E}]}(\mathsf{B}) \leq \mathbf{Adv}^{\mathrm{TPRP}}_{\widetilde{E}}(\mathsf{B}'') + \frac{(C+1)q}{|\mathcal{X}|}.$$

Proof. The proof is standard and deferred to the full version of the paper [50].
□

Remark 1. While it is in principle possible to save one encryption call in the EPWC construction by keeping the final AD or message block unencrypted as in the standard PMAC construction [13,52], we avoid this to ensure that static AD always gets treated the same, independently of the message. Indeed, applying this optimization would result in a construction where the final block of AD should be treated differently depending on whether the message is empty or not. Handling the AD independently of the message allows to precompute

$$\mathsf{auth}' = \bigoplus_{i=1}^{\ell_a - 1} \widetilde{P}^{2,i+1}(A_i) \oplus \widetilde{P}^{2/3,\ell_a+1}(A_{\ell_a}(10^*))$$

and to process the nonce and the message later (in particular, when the AD is static, auth' need not be recomputed each time).

Remark 2. In the nonce-misuse scenario, there is a simple birthday attack against $\mathsf{EPWC}[\widetilde{E}]$ as soon as the adversary can repeat a single nonce twice. The attack proceeds as follows: simply query $\mathsf{EPWC}[\widetilde{E}]_K$ for roughly $2^{n/2}$ pairs (N_i, A, M) with distinct nonces and the same AD and message until a collision occurs on the outputs for two nonces N_1 and N_2. Clearly, a collision on the MACs implies that $F_K(N_1) = F_K(N_2)$ (where F_K is given by (5)). Hence, the adversary can now query $Y = \mathsf{EPWC}[\widetilde{E}]_K(N_1, A', M')$ for a new pair $(A', M') \neq (A, M)$. Then Y is a valid forgery for (N_2, A', M'). It remains an open problem to design a nonce-based MAC scheme ensuring graceful degradation of security with the maximal number of nonce repetitions.

6   The SCT Mode

6.1   The NSIV Construction

In this section, we present the nAE mode SCT and analyze its security. We first describe a generic composition method named NSIV, which defines a nAE scheme from a nonce-based keyed function and an nivE scheme. The NSIV construction results from a small (but important from a security viewpoint) modification to the (generic) SIV construction [55]. While in SIV the encryption part is purely IV-based, NSIV relies on a combined nonce- and IV-based encryption (nivE) scheme, the nonce being used as input *both* to the keyed function and the nivE scheme. This is the only difference with SIV, where the nonce is only given as input to the keyed function.

More formally, let F be a nonce-based keyed function with key-space $\mathcal{K}_1$, nonce space $\mathcal{N}$, domain $\mathcal{D} = \mathcal{A} \times \mathcal{M}$, and range $\mathcal{Y}$, and $\Pi = (\mathcal{K}_2, \mathcal{N}, \mathcal{IV}, \mathcal{M}, \mathsf{Enc}, \mathsf{Dec})$ be a nivE scheme. Fix a regular function $\mathsf{Conv} : \mathcal{Y} \to \mathcal{IV}$. We define the nAE scheme[16] $\mathsf{NSIV}[F, \Pi] = (\mathcal{K}, \mathcal{N}, \mathcal{A}, \mathcal{M}, \mathsf{Enc}, \mathsf{Dec})$ with key-space $\mathcal{K} = \mathcal{K}_1 \times \mathcal{K}_2$ as specified on Fig. 4.

---

[16] Our formalization of an nAE scheme in Definition 4 assumes that the ciphertext is a binary string, whereas in our description, $\mathsf{NSIV}[F, \Pi].\mathsf{Enc}$ returns a pair (C, tag). We assume some implicit encoding of this pair into a single binary string.
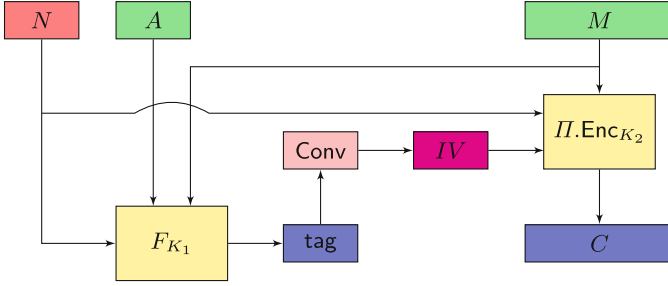
```
1  algorithm NSIV[F, Π].Enc_{K_1,K_2}(N, A, M)
2      tag := F_{K_1}(N, A, M)
3      IV := Conv(tag)
4      C := Π.Enc_{K_2}(N, IV, M)
5      return (C, tag)
6
7  algorithm NSIV[F, Π].Dec_{K_1,K_2}(N, A, C, tag)
8      IV := Conv(tag)
9      M := Π.Dec_{K_2}(N, IV, C)
10     tag' := F_{K_1}(N, A, M)
11     if tag' = tag then return M else return ⊥
```

Fig. 4. The NSIV construction, defining a nAE scheme from a nonce-based keyed function $F : \mathcal{K}_1 \times \mathcal{N} \times \mathcal{D} \to \mathcal{Y}$ where $\mathcal{D} = \mathcal{A} \times \mathcal{M}$ and a nivE scheme $\Pi = (\mathcal{K}_2, \mathcal{N}, \mathcal{IV}, \mathcal{M}, \mathsf{Enc}, \mathsf{Dec})$. Function Conv is a regular function from $\mathcal{Y}$ to $\mathcal{IV}$.

The security of $\mathsf{NSIV}[F, \Pi]$ is given by Theorem 4 below. We assume that $\mathcal{A} = \mathcal{M} = \{0,1\}^*$ for convenience, but this restriction can be lifted easily. We denote by $t_\Pi(\sigma)$ an upper bound on the time needed for computing $\Pi.\mathsf{Enc}$ or $\Pi.\mathsf{Dec}$ on inputs of total message length at most σ blocks of n bits, and we assume that computing $\mathsf{Conv}(\mathsf{tag})$ or sampling uniformly from $\mathsf{Conv}^{-1}(IV)$ takes negligible time for any $\mathsf{tag} \in \mathcal{Y}$ and $IV \in \mathcal{IV}$. The proof of this theorem is similar to the security proof of SIV, and deferred to the full version of the paper [50].

Theorem 4 (Security of NSIV). *Let $F : \mathcal{K}_1 \times \mathcal{N} \times \mathcal{D} \to \mathcal{Y}$, where $\mathcal{D} = \mathcal{A} \times \mathcal{M}$, be a nonce-based keyed function, $\Pi = (\mathcal{K}_2, \mathcal{N}, \mathcal{IV}, \mathcal{M}, \mathsf{Enc}, \mathsf{Dec})$ be a nivE scheme, and Conv $: \mathcal{Y} \to \mathcal{IV}$ be a regular function. Let A be a (q, m, ℓ, σ, t)-adversary against $\mathsf{NSIV}[F, \Pi]$. Then, letting $t' = t + t_\Pi(\sigma)$, the following holds:*

(a) if A is allowed to repeat nonces ($m > 1$), then there exists a (q, m, ℓ, σ, t')-adversary A' against Π and a (q, q, ℓ, σ, t')-adversary A'' against the PRF-security of F such that

$$\mathbf{Adv}^{\mathrm{AE}}_{\mathsf{NSIV}[F,\Pi]}(\mathsf{A}) \leq \mathbf{Adv}^{\mathrm{ivE}}_\Pi(\mathsf{A}') + \mathbf{Adv}^{\mathrm{PRF}}_F(\mathsf{A}'') + \frac{q}{|\mathcal{Y}|};$$

(b) if A *is nonce-respecting* ($m = 1$), *then there exists a* $(q, 1, \ell, \sigma, t')$-*adversary* A′ *against* Π *and* $(q, 1, \ell, \sigma, t')$-*adversaries* A″ *and* A‴ *against respectively the* PRF- *and the* MAC-*security of* F, *all nonce-respecting, such that*

$$\mathbf{Adv}^{\mathrm{nAE}}_{\mathsf{NSIV}[F,\Pi]}(\mathsf{A}) \le \mathbf{Adv}^{\mathrm{nivE}}_{\Pi}(\mathsf{A}') + \mathbf{Adv}^{\mathrm{nPRF}}_{F}(\mathsf{A}'') + \mathbf{Adv}^{\mathrm{nMAC}}_{F}(\mathsf{A}''').$$

6.2   From NSIV to SCT

The $\mathsf{SCT}[\widetilde{E}]$ mode is simply $\mathsf{NSIV}[F, \Pi]$ where F is instantiated with $\mathsf{EPWC}[\widetilde{E}]$ and Π is instantiated with $\mathsf{CTRT}[\widetilde{E}]$. Additionally, in order to be able to use the same key for calls to $\widetilde{E}$ both in EPWC and in CTRT, we use tweak separation to ensure that all calls to $\widetilde{E}$ in EPWC and in CTRT are independent. The resulting construction is illustrated in Fig. 1. Combining Theorem 4 with Theorems 1, 2 and 3, we finally obtain the following result for the security of SCT.[17] We denote by $t_{\mathsf{SCT}}(\sigma)$ an upper bound on the time needed for computing $\mathsf{SCT}[\widetilde{E}].\mathsf{Enc}_K$ or $\mathsf{SCT}[\widetilde{E}].\mathsf{Dec}_K$ on inputs of total (AD + message) length at most σ blocks of n bits when calls to $\widetilde{E}_K$ cost unit time.

Theorem 5 (Security of SCT). *Let* $\widetilde{E} \in \mathsf{TBC}(\mathcal{K}, \mathcal{T}', \mathcal{X})$ *with* $\mathcal{X} = \{0, 1\}^n$, $\mathcal{T} = \{1, \dots, 5\} \times \mathcal{T}$, *and* $|\mathcal{T}| \ge 8$. *Let* Conv *be a regular[18] function from* $\mathcal{X}$ *to* $\mathcal{T}$. *Assume Conjecture 1 and let* $f(\sigma)$ *be defined as in Theorem 1. Let* A *be a* (q, m, ℓ, σ, t)-*adversary against* $\mathsf{SCT}[\widetilde{E}]$ *with* $\ell \le |\mathcal{T}| - 2$. *Then there exists an absolute constant* C *and an adversary* A′ *against the TPRP-security of* $\widetilde{E}$, *making at most* $\sigma + 3q$ *oracle queries and running in time at most* $t + t_{\mathsf{SCT}}(\sigma)$, *such that*

(a) if A *is allowed to repeat nonces in encryption queries* ($m > 1$), *then*

$$\mathbf{Adv}^{\mathrm{AE}}_{\mathsf{SCT}[\widetilde{E}]}(\mathsf{A}) \le \mathbf{Adv}^{\mathrm{TPRP}}_{\widetilde{E}}(\mathsf{A}') + \frac{2(m-1)\sigma + 1}{|\mathcal{T}|} + f(\sigma) + \frac{q^2 + q}{|\mathcal{X}|};$$

(b) if A *is nonce-respecting* ($m = 1$), *then*

$$\mathbf{Adv}^{\mathrm{nAE}}_{\mathsf{SCT}[\widetilde{E}]}(\mathsf{A}) \le \mathbf{Adv}^{\mathrm{TPRP}}_{\widetilde{E}}(\mathsf{A}') + \frac{1}{|\mathcal{T}|} + f(\sigma) + \frac{(2C+1)q}{|\mathcal{X}|}.$$

---

[17] In more details, it is more convenient to prove Theorem 5 by first replacing $\widetilde{E}_K$ by a uniformly random tweakable permutation, and then applying Theorems 1, 2, and 3 for a perfect TBC.

[18] Note that this regularity condition imposes $|\mathcal{T}| \le |\mathcal{X}|$. However, when $\mathcal{T} > |\mathcal{X}|$, the security bounds of CTRT and EPWC do not depend on the tweak length (only the maximal message length does). Hence, one can always use a subset of tweaks of size $|\mathcal{X}|$ in case $|\mathcal{T}| > |\mathcal{X}|$.

References

1. CAESAR: Competition for Authenticated Encryption: Security, Applicability, and Robustness. http://competitions.cr.yp.to/caesar.html

2. Abed, F., Fluhrer, S., Forler, C., List, E., Lucks, S., McGrew, D., Wenzel, J.: Pipelineable on-line encryption. In: Cid, C., Rechberger, C. (eds.) FSE 2014. LNCS, vol. 8540, pp. 205–223. Springer, Heidelberg (2015)

3. AlFardan, N.J., Paterson, K.G., Lucky thirteen: breaking the TLS and DTLS record protocols. In: Security and Privacy - SP 2013, pp. 526–540 (2013)

4. Andreeva, E., Bogdanov, A., Luykx, A., Mennink, B., Mouha, N., Yasuda, K.: How to securely release unverified plaintext in authenticated encryption. In: Sarkar, P., Iwata, T. (eds.) ASIACRYPT 2014. LNCS, vol. 8873, pp. 105–125. Springer, Heidelberg (2014)

5. Andreeva, E., Bogdanov, A., Luykx, A., Mennink, B., Tischhauser, E., Yasuda, K.: Parallelizable and authenticated online ciphers. In: Sako, K., Sarkar, P. (eds.) ASIACRYPT 2013, Part I. LNCS, vol. 8269, pp. 424–443. Springer, Heidelberg (2013)

6. Asharov, G., Naor, M., Segev, G., Shahaf, I., Encryption, S.S.: Optimal locality in linear space via two-dimensional balanced allocations. IACR Cryptology ePrint Archive, Report 2016/251 (2016). To appear at STOC 2016

7. Bellare, M., Desai, A., Jokipii, E., Rogaway, P.: A concrete security treatment of symmetric encryption. In: FOCS 1997, pp. 394–403 (1997)

8. Bellare, M., Impagliazzo, R.: A tool for obtaining tighter security analyses of pseudorandom function based constructions, with applications to PRP to PRF conversion. IACR Cryptology ePrint Archive, Report 1999/024 (1999)

9. Bellare, M., Kilian, J., Rogaway, P.: The security of the cipher block chaining message authentication code. J. Comput. Syst. Sci. **61**(3), 362–399 (2000)

10. Bellare, M., Namprempre, C.: Authenticated encryption: relations among notions and analysis of the generic composition paradigm. In: Okamoto, T. (ed.) ASIACRYPT 2000. LNCS, vol. 1976, pp. 531–545. Springer, Heidelberg (2000)

11. Bellare, M., Rogaway, P.: Encode-then-encipher encryption: how to exploit nonces or redundancy in plaintexts for efficient cryptography. In: Okamoto, T. (ed.) ASIACRYPT 2000. LNCS, vol. 1976, pp. 317–330. Springer, Heidelberg (2000)

12. Bellare, M., Rogaway, P., Wagner, D.: The EAX mode of operation. In: Roy, B., Meier, W. (eds.) FSE 2004. LNCS, vol. 3017, pp. 389–407. Springer, Heidelberg (2004)

13. Black, J.A., Rogaway, P.: A block-cipher mode of operation for parallelizable message authentication. In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 384–397. Springer, Heidelberg (2002)

14. Brassard, G.: On computationally secure authentication tags requiring short secret shared keys. In: CRYPTO 1982, pp. 79–86 (1982)

15. Chen, S., Steinberger, J.: Tight security bounds for key-alternating ciphers. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 327–350. Springer, Heidelberg (2014)

16. Cogliati, B., Lampe, R., Patarin, J.: The indistinguishability of the XOR of k permutations. In: Cid, C., Rechberger, C. (eds.) FSE 2014. LNCS, vol. 8540, pp. 285–302. Springer, Heidelberg (2014)

17. Dodis, Y., Steinberger, J.: Domain extension for MACs beyond the birthday barrier. In: Paterson, K.G. (ed.) EUROCRYPT 2011. LNCS, vol. 6632, pp. 323–342. Springer, Heidelberg (2011)

18. Duong, T., Rizzo, J.: Here come the ⊕ Ninjas. Unpublished manuscript (2011). https://bug665814.bugzilla.mozilla.org/attachment.cgi?id=540839
19. Ferguson, N.: Collision attacks on OCB. Unpublished manuscript (2002). http://www.cs.ucdavis.edu/~rogaway/ocb/fe02.pdf
20. Ferguson, N., Lucks, S., Schneier, B., Whiting, D., Bellare, M., Kohno, T., Callas, J., Walker, J.: The Skein hash function family. SHA3 Submission to NIST (Round 3) (2010)
21. Fleischmann, E., Forler, C., Lucks, S.: McOE: a family of almost foolproof on-line authenticated encryption schemes. In: Canteaut, A. (ed.) FSE 2012. LNCS, vol. 7549, pp. 196–215. Springer, Heidelberg (2012)
22. Gligor, V.D., Donescu, P.: Fast encryption and authentication: XCBC encryption and XECB authentication modes. In: Matsui, M. (ed.) FSE 2001. LNCS, vol. 2355, p. 92. Springer, Heidelberg (2002)
23. Goldreich, O., Goldwasser, S., Micali, S.: How to construct random functions. J. ACM **33**(4), 792–807 (1986)
24. Grosso, V., Leurent, G., Standaert, F.-X., Varici, K., Durvaux, F., Gaspar, L., Kerckhof, S.: SCREAM and iSCREAM. Submitted to CAESAR (2014)
25. Gueron, S., Lindell, Y.: GCM-SIV: full nonce misuse-resistant authenticated encryption atunder one cycle per byte. In: ACM CCS 2015, pp. 109–119 (2015)
26. Hoang, V.T., Krovetz, T., Rogaway, P.: Robust authenticated-encryption AEZ and the problem that it solves. In: Oswald, E., Fischlin, M. (eds.) EUROCRYPT 2015. LNCS, vol. 9056, pp. 15–44. Springer, Heidelberg (2015)
27. Hoang, V.T., Reyhanitabar, R., Rogaway, P., Vizár, D.: Online authenticated-encryption and its nonce-reuse misuse-resistance. In: Gennaro, R., Robshaw, M. (eds.) CRYPTO 2015. LNCS, vol. 9215, pp. 493–517. Springer, Heidelberg (2015)
28. Iwata, T.: New blockcipher modes of operation with beyond the birthday bound security. In: Robshaw, M. (ed.) FSE 2006. LNCS, vol. 4047, pp. 310–327. Springer, Heidelberg (2006)
29. Iwata, T.: Authenticated encryption mode for beyond the birthday bound security. In: Vaudenay, S. (ed.) AFRICACRYPT 2008. LNCS, vol. 5023, pp. 125–142. Springer, Heidelberg (2008)
30. Jean, J., Nikolic, I., Peyrin, T.: Deoxys v1. Submitted to the CAESAR competition (2014)
31. Jean, J., Nikolic, I., Peyrin, T.: Joltik v1. Submitted to the CAESAR competition (2014)
32. Jean, J., Nikolic, I., Peyrin, T.: KIASU v1. Submitted to the CAESAR competition (2014)
33. Jean, J., Nikolic, I., Peyrin, T.: Tweaks and keys for blockciphers: the TWEAKEY framework. In: Sarkar, P., Iwata, T. (eds.) ASIACRYPT 2014. LNCS, vol. 8874, pp. 274–288. Springer, Heidelberg (2014)
34. Jutla, C.S.: Encryption modes with almost free message integrity. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 529–544. Springer, Heidelberg (2001)
35. Jutla, C.S.: Encryption modes with almost free message integrity. J. Cryptol. **21**(4), 547–578 (2008). Earlier version at EUROCRYPT 2001
36. Katz, J., Yung, M.: Characterization of security notions for probabilistic private-key encryption. J. Cryptol. **19**(1), 67–95 (2006)
37. Krawczyk, H.: The order of encryption and authentication for protecting communications (or: how secure is SSL?). In: Kilian, J. (ed.) CRYPTO 2001. LNCS, vol. 2139, pp. 310–331. Springer, Heidelberg (2001)

38. Krovetz, T., Rogaway, P.: The software performance of authenticated-encryption modes. In: Joux, A. (ed.) FSE 2011. LNCS, vol. 6733, pp. 306–327. Springer, Heidelberg (2011)

39. Lampe, R., Seurin, Y.: Tweakable blockciphers with asymptotically optimal security. In: Moriai, S. (ed.) FSE 2013. LNCS, vol. 8424, pp. 133–152. Springer, Heidelberg (2014)

40. Landecker, W., Shrimpton, T., Terashima, R.S.: Tweakable blockciphers with beyond birthday-bound security. In: Safavi-Naini, R., Canetti, R. (eds.) CRYPTO 2012. LNCS, vol. 7417, pp. 14–30. Springer, Heidelberg (2012)

41. Liskov, M., Rivest, R.L., Wagner, D.: Tweakable block ciphers. In: Yung, M. (ed.) CRYPTO 2002. LNCS, vol. 2442, pp. 31–46. Springer, Heidelberg (2002)

42. Lucks, S.: The sum of PRPs is a secure PRF. In: Preneel, B. (ed.) EUROCRYPT 2000. LNCS, vol. 1807, pp. 470–484. Springer, Heidelberg (2000)

43. McGrew, D.A., Viega, J.: The security and performance of the Galois/counter mode (GCM) of operation. In: Canteaut, A., Viswanathan, K. (eds.) INDOCRYPT 2004. LNCS, vol. 3348, pp. 343–355. Springer, Heidelberg (2004)

44. Mennink, B.: Optimally secure tweakable blockciphers. In: Leander, G. (ed.) FSE 2015. LNCS, vol. 9054, pp. 428–448. Springer, Heidelberg (2015)

45. Minematsu, K.: Beyond-birthday-bound security based on tweakable block cipher. In: Dunkelman, O. (ed.) FSE 2009. LNCS, vol. 5665, pp. 308–326. Springer, Heidelberg (2009)

46. Namprempre, C., Rogaway, P., Shrimpton, T.: Reconsidering generic composition. In: Nguyen, P.Q., Oswald, E. (eds.) EUROCRYPT 2014. LNCS, vol. 8441, pp. 257–274. Springer, Heidelberg (2014)

47. Patarin, J.: A proof of security in $O(2^n)$ for the Xor of two random permutations. In: Safavi-Naini, R. (ed.) ICITS 2008. LNCS, vol. 5155, pp. 232–248. Springer, Heidelberg (2008)

48. Patarin, J.: The "Coefficients H" technique. In: Avanzi, R.M., Keliher, L., Sica, F. (eds.) SAC 2008. LNCS, vol. 5381, pp. 328–345. Springer, Heidelberg (2009)

49. Patarin, J.: Security in $O(2^n)$ for the Xor of two random permutations: proof with the standard H technique. IACR Cryptology ePrint Archive, Report 2013/368 (2013)

50. Peyrin, T., Seurin, Y.: Counter-in-Tweak: authenticated encryption modes for tweakable block ciphers. Full version of this paper. http://eprint.iacr.org/2015/1049

51. Rogaway, P.: Authenticated-encryption with associated-data. In: ACM CCS 2002, pp. 98–107 (2002)

52. Rogaway, P.: Efficient instantiations of tweakable blockciphers and refinements to modes OCB and PMAC. In: Lee, P.J. (ed.) ASIACRYPT 2004. LNCS, vol. 3329, pp. 16–31. Springer, Heidelberg (2004)

53. Rogaway, P.: Nonce-based symmetric encryption. In: Roy, B., Meier, W. (eds.) FSE 2004. LNCS, vol. 3017, pp. 348–359. Springer, Heidelberg (2004)

54. Rogaway, P., Bellare, M., Black, J.: OCB: a block-cipher mode of operation for efficient authenticated encryption. ACM Trans. Inf. Syst. Secur. **6**(3), 365–403 (2003)

55. Rogaway, P., Shrimpton, T.: A provable-security treatment of the key-wrap problem. In: Vaudenay, S. (ed.) EUROCRYPT 2006. LNCS, vol. 4004, pp. 373–390. Springer, Heidelberg (2006)

56. Shoup, V.: On fast and provably secure message authentication based on universal hashing. In: Koblitz, N. (ed.) CRYPTO 1996. LNCS, vol. 1109, pp. 313–328. Springer, Heidelberg (1996)

57. Shoup, V.: Sequences of games: a tool for taming complexity in security proofs. IACR Cryptology ePrint Archive, Report 2004/332 (2004)
58. Shrimpton, T., Terashima, R.S.: A modular framework for building variable-input-length tweakable ciphers. In: Sako, K., Sarkar, P. (eds.) ASIACRYPT 2013, Part I. LNCS, vol. 8269, pp. 405–423. Springer, Heidelberg (2013)
59. Vaudenay, S.: Security flaws induced by CBC padding - applications to SSL, IPSEC, WTLS ... In: Knudsen, L.R. (ed.) EUROCRYPT 2002. LNCS, vol. 2332, pp. 534–546. Springer, Heidelberg (2002)
60. Wegman, M.N., Carter, L.: New hash functions and their use in authentication and set equality. J. Comput. Syst. Sci. **22**(3), 265–279 (1981)
61. Whiting, D., Housley, R., Ferguson, N.: Counter with CBC-MAC (CCM). Submission to NIST (2002). http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/ccm/ccm.pdf
62. Yasuda, K.: A new variant of PMAC: beyond the birthday bound. In: Rogaway, P. (ed.) CRYPTO 2011. LNCS, vol. 6841, pp. 596–609. Springer, Heidelberg (2011)