Compactly Committing Authenticated Encryption Using Encryptment and Tweakable Block Cipher

Shoichi Hirose[1] and Kazuhiko Minematsu[2,3]

[1] University of Fukui, Fukui, Japan
hrs_shch@u-fukui.ac.jp
[2] NEC, Kawasaki, Japan
k-minematsu@nec.com
[3] Yokohama National University, Kanagawa, Japan

Abstract. Message franking is a feature of end-to-end encrypted messaging introduced by Facebook that enables users to report abusive contents in a verifiable manner. Grubbs et al. (CRYPTO 2017) formalized a symmetric-key primitive usable for message franking, called compactly committing authenticated encryption with associated data (ccAEAD), and presented schemes with provable security. Dodis et al. (CRYPTO 2018) proposed a core building block for ccAEAD, called encryptment, and presented a generic construction of ccAEAD combining encryptment and conventional AEAD. We show that ccAEAD can be built on encryptment and a tweakable block cipher (TBC), leading to simpler and more efficient constructions of ccAEAD than Dodis et al.'s methods. Our construction, called EnCryptment-then-TBC (ECT), is secure under a new but feasible assumption on the ciphertext integrity of encryptment. We also formalize the notion of remotely keyed ccAEAD (RK ccAEAD) and show that our ECT works as RK ccAEAD. RK ccAEAD was first considered by Dodis et al. as a useful variant of ccAEAD when it is implemented on a platform consisting of a trusted module and an untrusted (leaking) module. However, its feasibility was left open. Our work is the first to show its feasibility with a concrete scheme.

Keywords: Authenticated encryption · Commitment · Tweakable block cipher · Remotely keyed encryption

1 Introduction

Background. End-to-end encrypted messaging systems are now widely deployed, such as Facebook Messenger [17], Signal [36], and Whatsapp Messenger [38]. Accordingly, new security issues arise in addition to those on the privacy and authenticity of messages. A significant problem is preventing malicious senders from sending harassing messages and harmful/abusive contents. To achieve this goal, Facebook introduced message franking [18]. It is a cryptographic protocol allowing users to report the receipt of abusive messages in a verifiable manner to Facebook.

At Crypto 2017, Grubbs et al. [20] initiated the formal study of message franking and presented a new variant of AEAD, called compactly committing AEAD (ccAEAD), as a symmetric-key primitive that is useful for message franking. For ccAEAD, a small part of the ciphertext works as a commitment to the message and the associated data. They also presented two generic constructions of ccAEAD. One is called CtE (Commit-then-Encrypt), which consists of commitment and AEAD. The other is called CEP (Committing Encrypt-and-PRF). It consists of a pseudorandom generator, a pseudorandom function (PRF), and a collision-resistant PRF.

At Crypto 2018, Dodis et al. [15] further studied ccAEAD and proposed a new primitive, called encryptment, as a core component of ccAEAD. They show that, given encryptment, ccAEAD can be built from an additional common cryptographic primitive. Concretely, they presented two transformations. One transformation needs a call to (randomized) AEAD in addition to encryptment, and the other needs two calls to a related-key-secure PRF. The former is a randomized scheme, and the latter is nonce-based. In addition, they considered remotely keyed ccAEAD (RK ccAEAD) in the full version [16] of [15]. Here, RK ccAEAD is an extension of ccAEAD inheriting the property of remotely keyed encryption, which was proposed by Blaze [8] and extensively studied in the late 90's [9,25,31,32]. Its goal was to enable secure encryption under a setting where one could use a resource-limited personal device storing secret keys and computing cryptographic functions. The problem was how to do bulk encryption and decryption by utilizing the power of a host and the security of the personal device. Dodis et al. [16] suggested RK ccAEAD as a useful variant of ccAEAD under such environments. However, they left open its feasibility and concrete constructions.

Our Contributions. Focusing on the work of Dodis et al. [15,16], this paper makes two contributions. First, we present a new construction of ccAEAD based on encryptment, dubbed ECT (EnCryptment-then-TBC). While Dodis et al. [15,16] used AEAD as an additional component, we show that an additional single call of a tweakable block cipher (TBC) [29,30] is sufficient. Since the integrity mechanism provided by AEAD is not needed, our proposal allows simpler and more efficient ccAEAD compared with Dodis et al.'s proposals. In more detail, when encryption, Dodis et al.'s method needs AEAD taking two elements, B (for associated data) and L (for plaintext) as an input in addition to a secret key, while ECT simply encrypt L with tweak B by a TBC. The latter is arguably much simpler. See Fig. 1 for their illustrations. Note that the encryption output C_1 of AEAD in Dodis et al.'s method contains a random nonce and a tag in addition to the "raw" ciphertext of $|L|$ bits as otherwise decryption is not possible. Hence, ECT is more efficient in terms of bandwidth[4]. The security requirements of ECT are reduced to those of the underlying encryptment and a TBC. In particular, the ciphertext integrity of ECT requires a new but feasible

[4] The second method of Dodis et al. has also larger bandwidth than ours for the existence of tag. A concrete comparison is not possible as it is nonce-based.

type of ciphertext unforgeability for the encryptment. Actually, we show that HFC [15] – a hash-based efficient encryptment scheme proposed by Dodis et al. – satisfies this new ciphertext unforgeability in the random oracle model. We note that HFC originally assumed the random oracle, so we do not introduce any new assumption.

Second, we provide the first formalization of remotely keyed (RK) ccAEAD, and show that ECT is secure RK ccAEAD. This answers the aforementioned open question posed by Dodis et al. positively. Our formalization is based on that of RK authenticated encryption by Dodis and An [14]. The confidentiality of ECT as RK ccAEAD requires a new variant of confidentiality for encryptment. It is also shown that HFC satisfies the new variant of confidentiality in the random oracle model. ECT has a similar structure to the AEAD scheme named CONCRETE [7], which offers ciphertext integrity in the presence of nonce misuse and leakage. As mentioned above, remotely keyed encryption [8] is practically relevant when composing a trusted (small) module with an untrusted/leaking module. We think this similarity exhibits an interesting relationship with RK ccAEAD and leakage-resilient AEAD, where the latter has been actively studied in recent years, e.g., [5,6,13,34,35].

Related Work. Authenticated encryption is one of the central topics in symmetric cryptography. Its formal treatments were initiated by Katz and Yung [26] and by Bellare and Namprempre [3].

A variation of message franking scheme that enables a receiver to report an abusive message by revealing only the abusive parts was investigated independently by Leontiadis and Vaudenay [28] and by Chen and Tang [11]. Huguenin-Dumittan and Leontiadis formalized and instantiated a secure bidirectional channel with message franking [23]. Yamamuro et al. [39] proposed forward secure message franking and presented a scheme based on ccAEAD, a forward secure pseudorandom generator, and a forward secure MAC. Tyagi et al. [37] formalized asymmetric message franking and constructed a scheme from signatures of knowledge [22] for designated verifier signatures [24].

Hirose [21] proposed a generic construction of nonce-based ccAEAD. The proposal is similar to the second method of Dodis et al. Since it simply replaces a PRF with a TBC, it needs two additional TBC calls, while ECT needs only one TBC call. In addition, his scheme is nonce-based while ours is randomized as originally proposed. Thus, ECT is less restrictive and more efficient in computation.

Dodis and An [14] proposed and investigated a cryptographic primitive called concealment. They formalized RK authenticated encryption as an application and provided a generic construction with concealment and authenticated encryption.

Farshim et al. [19], Albertini et al. [1], Len et al. [27], Bellare and Hoang [2], and Chan and Rogaway [10] discussed so-called committing authenticated encryption. While their definitions and security goals are not identical, their primary goal was basically to decrease the risk of error or misuse by application

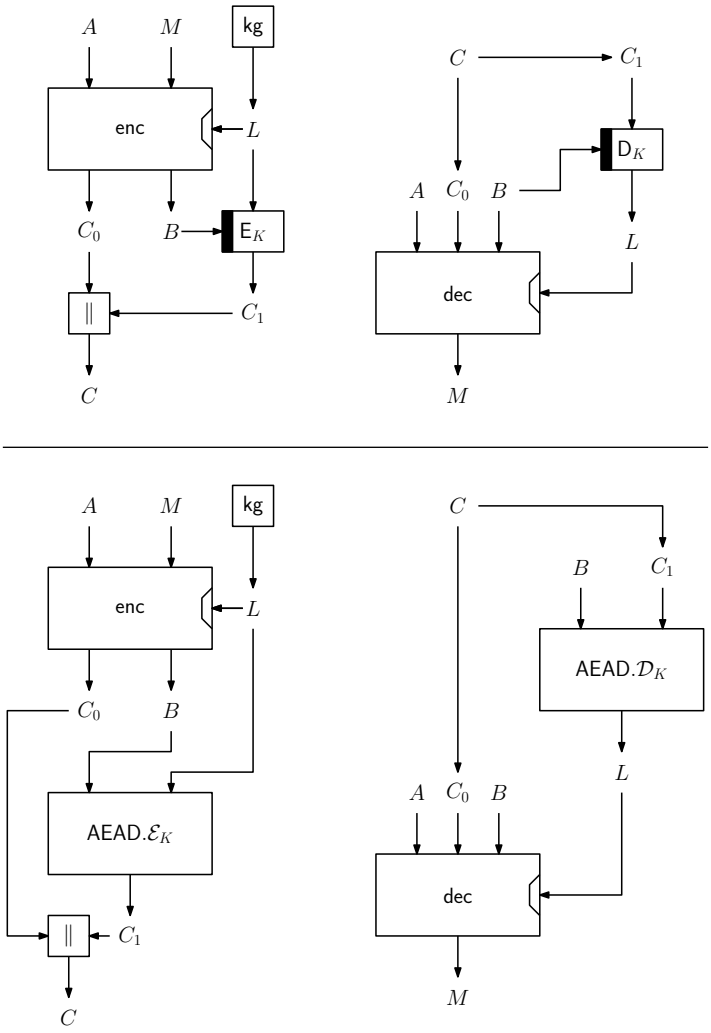


Fig. 1: Encryption and decryption algorithms of ccAEAD. (Top) our proposal, ECT, (Bottom) Dodis et al.'s method using AEAD [15]. For both cases, enc and dec are encryptment and decryptment algorithms of the encryptment scheme. The ccAEAD decryption algorithms omit the case of verification failures. In ECT, E_K and D_K denote the TBC's encryption and decryption, where the thick line is tweak input.

designers, and message franking was out of scope for the lack of opening key needed by ccAEAD.

Organization. Section 2 introduces notations and formalizes tweakable block ciphers, ccAEAD, and encryptment. Section 3 describes the generic construction of ccAEAD, called ECT, and confirms its security. Section 4 formalizes RK ccAEAD. Section 5 confirms the security of ECT as RK ccAEAD. Section 6 concludes the paper. Due to the page limit, some proofs of theorems are given in appendices.

2 Preliminaries

Let $\Sigma := \{0,1\}$. For any integer $l \geq 0$, let Σ^l be the set of all Σ-sequences of length l. Let $\Sigma^* := \bigcup_{i \geq 0} \Sigma^i$. The length of $x \in \Sigma^*$ is denoted by $|x|$. Concatenation of $x_1, x_2 \in \Sigma^*$ is denoted by $x_1 \| x_2$. A uniform random choice of an element s from a set $\mathcal{S}$ is denoted by $s \twoheadleftarrow \mathcal{S}$.

2.1 Tweakable Block Cipher

A TBC is formalized as a pair of encryption and decryption functions $\mathsf{TBC} := (\mathsf{E}, \mathsf{D})$ such that $\mathsf{E} : \Sigma^{n_\mathrm{k}} \times \Sigma^{n_\mathrm{t}} \times \Sigma^{n_\mathrm{b}} \to \Sigma^{n_\mathrm{b}}$ and $\mathsf{D} : \Sigma^{n_\mathrm{k}} \times \Sigma^{n_\mathrm{t}} \times \Sigma^{n_\mathrm{b}} \to \Sigma^{n_\mathrm{b}}$. Σ^{n_k} is a set of keys, Σ^{n_t} is a set of tweaks, and Σ^{n_b} is a set of plaintexts or ciphertexts. For every $(K, T) \in \Sigma^{n_\mathrm{k}} \times \Sigma^{n_\mathrm{t}}$, both $\mathsf{E}(K, T, \cdot)$ and $\mathsf{D}(K, T, \cdot)$ are permutations, and $\mathsf{D}(K, T, \mathsf{E}(K, T, \cdot))$ is the identity permutation over Σ^{n_b}.

Let $\mathcal{P}_{n_\mathrm{t}, n_\mathrm{b}}$ be the set of all tweakable permutations: For every $p \in \mathcal{P}_{n_\mathrm{t}, n_\mathrm{b}}$ and $T \in \Sigma^{n_\mathrm{t}}$, $p(T, \cdot)$ is a permutation over Σ^{n_b}. Let $p^{-1} \in \mathcal{P}_{n_\mathrm{t}, n_\mathrm{b}}$ be the inverse of $p \in \mathcal{P}_{n_\mathrm{t}, n_\mathrm{b}}$: $p^{-1}(T, p(T, \cdot))$ is the identity permutation for every $T \in \Sigma^{n_\mathrm{t}}$.

The security requirement of a TBC is formalized as indistinguishability from a uniform random tweakable permutation. Let $\mathbf{A}$ be an adversary with oracle access to a tweakable permutation (and its inverse) in $\mathcal{P}_{n_\mathrm{t}, n_\mathrm{b}}$. $\mathbf{A}$ can make adaptive queries to the oracle(s) and finally outputs 0 or 1. The advantage of $\mathbf{A}$ against TBC for a tweakable pseudorandom permutation (TPRP) is

$$\mathrm{Adv}^{\mathrm{tprp}}_{\mathsf{TBC}}(\mathbf{A}) := \big|\Pr[\mathbf{A}^{\mathsf{E}_K} = 1] - \Pr[\mathbf{A}^{\varpi} = 1]\big|,$$

where $K \twoheadleftarrow \Sigma^{n_\mathrm{k}}$ and $\varpi \twoheadleftarrow \mathcal{P}_{n_\mathrm{t}, n_\mathrm{b}}$. Similarly, the advantage of $\mathbf{A}$ against TBC for a strong tweakable pseudorandom permutation (STPRP) is

$$\mathrm{Adv}^{\mathrm{stprp}}_{\mathsf{TBC}}(\mathbf{A}) := \big|\Pr[\mathbf{A}^{\mathsf{E}_K, \mathsf{D}_K} = 1] - \Pr[\mathbf{A}^{\varpi, \varpi^{-1}} = 1]\big|.$$

2.2 ccAEAD

Syntax. ccAEAD [20] is formalized as a tuple of algorithms $\mathsf{CAE} := (\mathsf{Kg}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Ver})$. It is involved with a key space $\mathcal{K} := \Sigma^n$, an associated-data space $\mathcal{A} \subseteq \Sigma^*$, a message space $\mathcal{M} \subseteq \Sigma^*$, a ciphertext space $\mathcal{C} \subseteq \Sigma^*$, an opening-key space $\mathcal{L} \subseteq \Sigma^\ell$, and a binding-tag space $\mathcal{T} := \Sigma^\tau$. The "cc" (compactly committing) property requires that $\tau = O(n)$ is small.

– The key-generation algorithm Kg returns a secret key $K \in \mathcal{K}$ chosen uniformly at random.
– The encryption algorithm Enc takes as input $(K, A, M) \in \mathcal{K} \times \mathcal{A} \times \mathcal{M}$ and returns $(C, B) \in \mathcal{C} \times \mathcal{T}$.
– The decryption algorithm Dec takes as input $(K, A, C, B) \in \mathcal{K} \times \mathcal{A} \times \mathcal{C} \times \mathcal{T}$ and returns $(M, L) \in \mathcal{M} \times \mathcal{L}$ or $\perp \notin \mathcal{M} \times \mathcal{L}$.
– The verification algorithm Ver takes as input $(A, M, L, B) \in \mathcal{A} \times \mathcal{M} \times \mathcal{L} \times \mathcal{T}$ and returns $b \in \Sigma$.

Kg and Enc are randomized algorithms, and Dec and Ver are deterministic algorithms. For every $l \in \mathbb{N}$, $\Sigma^l \subseteq \mathcal{M}$ or $\Sigma^l \cap \mathcal{M} = \emptyset$. For $(C, B) \leftarrow \mathsf{Enc}(K, A, M)$, $|C|$ depends only on $|M|$, and there exists a function $\mathsf{clen} : \mathbb{N} \to \mathbb{N}$ such that $|C| = \mathsf{clen}(|M|)$.

CAE satisfies correctness. Namely, for any $(K, A, M) \in \mathcal{K} \times \mathcal{A} \times \mathcal{M}$, if $(C, B) \leftarrow \mathsf{Enc}(K, A, M)$, then there exists some $L \in \mathcal{L}$ such that $\mathsf{Dec}(K, A, C, B) = (M, L)$ and $\mathsf{Ver}(A, M, L, B) = 1$.

Security Requirements. The security requirements of ccAEAD are confidentiality, ciphertext integrity, and binding properties.

Confidentiality. The games MO-REAL and MO-RAND shown in Fig. 2 are introduced to formalize the confidentiality as real-or-random indistinguishability in the multi-opening setting. The advantage of an adversary $\mathbf{A}$ for confidentiality is

$$\mathrm{Adv}^{\text{mo-ror}}_{\mathsf{CAE}}(\mathbf{A}) := \left|\Pr[\text{MO-REAL}^{\mathbf{A}}_{\mathsf{CAE}} = 1] - \Pr[\text{MO-RAND}^{\mathbf{A}}_{\mathsf{CAE}} = 1]\right|.$$

$\mathbf{A}$ is allowed to make queries adaptively to the oracles **Enc**, **Dec**, and **ChalEnc**. In both of the games, **Enc** and **Dec** work in the same ways. For each query (A, C, B), **Dec** returns $(M, L) \leftarrow \mathsf{Dec}(K, A, C, B)$ only if the query is a previous reply from **Enc**.

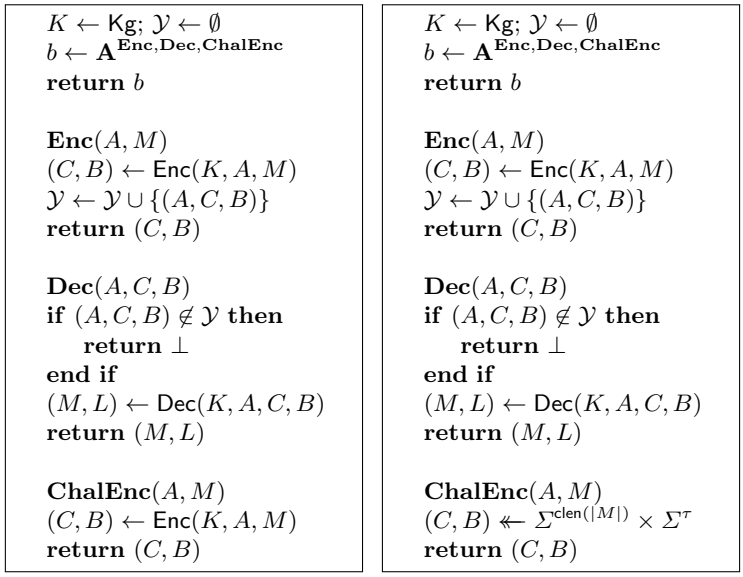
Ciphertext Integrity. The game MO-CTXT shown in Fig. 3 is introduced to formalize the ciphertext integrity as unforgeability in the multi-opening setting. The advantage of an adversary $\mathbf{A}$ for ciphertext integrity is

$$\mathrm{Adv}^{\text{mo-ctxt}}_{\mathsf{CAE}}(\mathbf{A}) := \Pr[\text{MO-CTXT}^{\mathbf{A}}_{\mathsf{CAE}} = \mathtt{true}].$$

$\mathbf{A}$ is allowed to make queries adaptively to the oracles **Enc**, **Dec**, and **ChalDec**. The game outputs $\mathtt{true}$ if $\mathbf{A}$ asks a query (A, C, B) to **ChalDec** such that $\mathsf{Dec}(K, A, C, B) \neq \perp$ without obtaining it from **Enc** by a previous query.

Binding Properties. Binding properties are defined for a sender and a receiver. Receiver binding describes that a malicious receiver cannot report a non-abusive sender for sending an abusive message. The advantage of an adversary $\mathbf{A}$ for receiver binding is

$$\begin{aligned}\mathrm{Adv}^{\text{r-bind}}_{\mathsf{CAE}}(\mathbf{A}) := \Pr[((A, M, L), (A', M', L'), B) \leftarrow \mathbf{A} : (A, M) \neq (A', M') \\ \wedge \mathsf{Ver}(A, M, L, B) = \mathsf{Ver}(A', M', L', B) = 1].\end{aligned}$$



(a) MO-REAL$^{\mathbf{A}}_{\mathsf{CAE}}$ (b) MO-RAND$^{\mathbf{A}}_{\mathsf{CAE}}$

Fig. 2: Games for confidentiality of ccAEAD

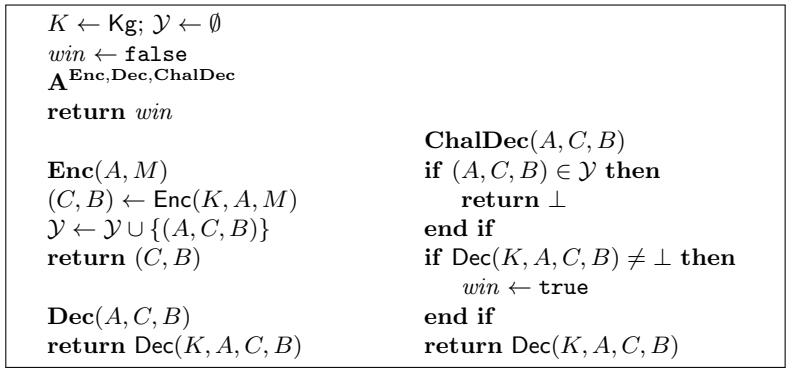


Fig. 3: Game MO-CTXT$^{\mathbf{A}}_{\mathsf{CAE}}$ for ciphertext integrity of ccAEAD

The advantage of $\mathbf{A}$ for strong receiver binding is

$$\mathrm{Adv}^{\text{sr-bind}}_{\mathsf{CAE}}(\mathbf{A}) := \Pr[((A,M,L),(A',M',L'),B) \leftarrow \mathbf{A} : (A,M,L) \neq (A',M',L') \\ \wedge \mathsf{Ver}(A,M,L,B) = \mathsf{Ver}(A',M',L',B) = 1].$$

It holds that $\mathrm{Adv}^{\text{r-bind}}_{\mathsf{CAE}}(\mathbf{A}) \leq \mathrm{Adv}^{\text{sr-bind}}_{\mathsf{CAE}}(\mathbf{A})$ for any CAE and $\mathbf{A}$.

Sender binding describes that a malicious sender of an abusive message cannot prevent the receiver from reporting it. The advantage of $\mathbf{A}$ for sender binding is

$$\mathrm{Adv}^{\text{s-bind}}_{\mathsf{CAE}}(\mathbf{A}) := \Pr[(K,A,C,B) \leftarrow \mathbf{A} : \mathsf{Dec}(K,A,C,B) \neq \bot \\ (M,L) \leftarrow \mathsf{Dec}(K,A,C,B) \ \wedge \ \mathsf{Ver}(A,M,L,B) = 0].$$

Message Franking Using ccAEAD. A service provider is assumed to relay all communication among users. Users encrypt their communication with ccAEAD. For a ciphertext from a sender, the service provider computes a tag with a MAC function for the binding tag in the ciphertext and transfers the ciphertext to the receiver together with the tag. Suppose that an abusive message is recovered from the ciphertext. Then, the receiver reports it to the service provider with the opening key, binding tag, and the tag attached by the service provider. The receiver binding prevents malicious receivers from blaming non-abusive senders. The sender binding prevents malicious senders from denying abusive reports by honest receivers.

2.3 Encryptment

Syntax. Encryptment [15] is roughly one-time ccAEAD. It is formalized as a tuple of algorithms $\mathsf{EC} = (\mathsf{kg}, \mathsf{enc}, \mathsf{dec}, \mathsf{ver})$. It is involved with a key space $\mathcal{K}_{\mathrm{ec}} := \Sigma^{\ell}$, an associated-data space $\mathcal{A} \subseteq \Sigma^*$, a message space $\mathcal{M} \subseteq \Sigma^*$, a ciphertext space $\mathcal{C} \subseteq \Sigma^*$, and a binding-tag space $\mathcal{T} := \Sigma^{\tau}$.

- The key-generation algorithm kg returns a secret key $K_{\mathrm{ec}} \in \mathcal{K}_{\mathrm{ec}}$ chosen uniformly at random.
- The encryptment algorithm enc takes as input $(K_{\mathrm{ec}}, A, M) \in \mathcal{K}_{\mathrm{ec}} \times \mathcal{A} \times \mathcal{M}$ and returns $(C, B) \in \mathcal{C} \times \mathcal{T}$.
- The decryptment algorithm dec takes as input $(K_{\mathrm{ec}}, A, C, B) \in \mathcal{K}_{\mathrm{ec}} \times \mathcal{A} \times \mathcal{C} \times \mathcal{T}$ and returns $M \in \mathcal{M}$ or $\bot \notin \mathcal{M}$.
- The verification algorithm ver takes as input $(A, M, K_{\mathrm{ec}}, B) \in \mathcal{A} \times \mathcal{M} \times \mathcal{K}_{\mathrm{ec}} \times \mathcal{T}$ and returns $b \in \Sigma$.

kg is a randomized algorithm, and enc, dec and ver are deterministic algorithms. For $(C, B) \leftarrow \mathsf{enc}(K_{\mathrm{ec}}, A, M)$, it is assumed that $|C|$ depends only on $|M|$.

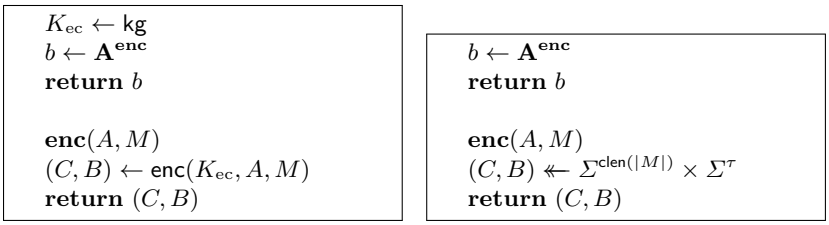
EC satisfies correctness: For any $(K_{\mathrm{ec}}, A, M) \in \mathcal{K}_{\mathrm{ec}} \times \mathcal{A} \times \mathcal{M}$, if $(C, B) \leftarrow \mathsf{enc}(K_{\mathrm{ec}}, A, M)$, then $\mathsf{dec}(K_{\mathrm{ec}}, A, C, B) = M$ and $\mathsf{ver}(A, M, K_{\mathrm{ec}}, B) = 1$. A stronger notion of correctness called strong correctness is also introduced: For any $(K_{\mathrm{ec}}, A, C, B) \in \mathcal{K}_{\mathrm{ec}} \times \mathcal{A} \times \mathcal{C} \times \mathcal{T}$, if $M \leftarrow \mathsf{dec}(K_{\mathrm{ec}}, A, C, B)$, then $\mathsf{enc}(K_{\mathrm{ec}}, A, M) = (C, B)$.

Security Requirements. The security requirements of encryptment are confidentiality, second-ciphertext unforgeability, and binding properties.

Confidentiality. Two games otREAL and otRAND shown in Fig. 4 are introduced to formalize the confidentiality. In both of the games, an adversary $\mathbf{A}$ asks only a single query to the oracle **enc**. The advantage of $\mathbf{A}$ for confidentiality is

$$\mathrm{Adv}^{\text{ot-ror}}_{\mathsf{EC}}(\mathbf{A}) := \left|\Pr[\mathrm{otREAL}^{\mathbf{A}}_{\mathsf{EC}} = 1] - \Pr[\mathrm{otRAND}^{\mathbf{A}}_{\mathsf{EC}} = 1]\right|,$$

where "ot-ror" stands for "one-time real-or-random."



(a) $\mathrm{otREAL}^{\mathbf{A}}_{\mathsf{EC}}$ (b) $\mathrm{otRAND}^{\mathbf{A}}_{\mathsf{EC}}$

Fig. 4: Games for confidentiality of encryptment

Second-Ciphertext Unforgeability. An adversary $\mathbf{A}$ asks only a single query $(A, M) \in \mathcal{A} \times \mathcal{M}$ to $\mathsf{enc}_{K_{\mathrm{ec}}}$ and gets (C, B) and K_{ec}, where $K_{\mathrm{ec}} \leftarrow \mathsf{kg}$ and $(C, B) \leftarrow \mathsf{enc}_{K_{\mathrm{ec}}}(A, M)$. Then, $\mathbf{A}$ outputs $(A', C') \in \mathcal{A} \times \mathcal{C}$. The advantage of $\mathbf{A}$ for second-ciphertext unforgeability is

$$\mathrm{Adv}^{\mathrm{scu}}_{\mathsf{EC}}(\mathbf{A}) := \Pr[(A, C) \neq (A', C') \wedge \mathsf{dec}_{K_{\mathrm{ec}}}(A', C', B) \neq \perp].$$

Binding properties. The advantage of $\mathbf{A}$ for receiver binding is

$$\begin{aligned}\mathrm{Adv}^{\text{r-bind}}_{\mathsf{EC}}(\mathbf{A}) := \Pr[((K_{\mathrm{ec}}, A, M), (K'_{\mathrm{ec}}, A', M'), B) \leftarrow \mathbf{A} : (A, M) \neq (A', M') \\ \wedge\, \mathsf{ver}(A, M, K_{\mathrm{ec}}, B) = \mathsf{ver}(A', M', K'_{\mathrm{ec}}, B) = 1].\end{aligned}$$

The advantage of $\mathbf{A}$ for strong receiver binding is

$$\begin{aligned}&\mathrm{Adv}^{\text{sr-bind}}_{\mathsf{EC}}(\mathbf{A}) := \Pr[((K_{\mathrm{ec}}, A, M), (K'_{\mathrm{ec}}, A', M'), B) \leftarrow \mathbf{A} : \\ &\quad (K_{\mathrm{ec}}, A, M) \neq (K'_{\mathrm{ec}}, A', M') \wedge \mathsf{ver}(A, M, K_{\mathrm{ec}}, B) = \mathsf{ver}(A', M', K'_{\mathrm{ec}}, B) = 1].\end{aligned}$$

The advantage of an adversary $\mathbf{A}$ for sender binding is

$$\begin{aligned}\mathrm{Adv}^{\text{s-bind}}_{\mathsf{EC}}(\mathbf{A}) := \Pr[(K_{\mathrm{ec}}, A, C, B) \leftarrow \mathbf{A}, M \leftarrow \mathsf{dec}(K_{\mathrm{ec}}, A, C, B) : \\ M \neq \perp \ \wedge\ \mathsf{ver}(A, M, K_{\mathrm{ec}}, B) = 0].\end{aligned}$$

For strongly correct encryptment, Dodis et al. [15] reduced second-ciphertext unforgeability to sender binding and receiver binding. The following proposition shows that it can be reduced only to receiver binding. On the other hand, receiver binding cannot be reduced to second-ciphertext unforgeability. Suppose that EC is secure except that it has a weak key such that receiver binding is broken using the weak key. For second-ciphertext unforgeability, the probability that the weak key is chosen is negligible for a query made by an adversary.

Proposition 1. *Let* EC *be a strongly correct encryptment scheme. Then, for any adversary* $\mathbf{A}$ *against* EC *for second-ciphertext unforgeability, there exists an adversary* $\dot{\mathbf{A}}$ *such that* $\mathrm{Adv}^{\mathrm{scu}}_{\mathsf{EC}}(\mathbf{A}) \leq \mathrm{Adv}^{\text{r-bind}}_{\mathsf{EC}}(\dot{\mathbf{A}})$ *and the run time of* $\dot{\mathbf{A}}$ *is at most about that of* $\mathbf{A}$*.*

Proof. Shown in Appendix D.

3 ccAEAD Using Encryptment and TBC

3.1 Scheme

New ccAEAD construction ECT (EnCryptment-then-TBC) $\mathsf{ECT} = (\mathsf{KG}, \mathsf{ENC}, \mathsf{DEC}, \mathsf{VER})$ is proposed. It uses an encryptment scheme $\mathsf{EC} = (\mathsf{kg}, \mathsf{enc}, \mathsf{dec}, \mathsf{ver})$ and a TBC $\mathsf{TBC} = (\mathsf{E}, \mathsf{D})$. For ECT, let $\mathcal{K} := \Sigma^n$ be its key space, $\mathcal{A}$ be its associated-data space, $\mathcal{M}$ be its message space, $\mathcal{C}$ be its ciphertext space, $\mathcal{L} := \Sigma^\ell$ be its opening-key space, and $\mathcal{T} := \Sigma^\tau$ be its binding-tag space. Then, for EC, $\mathcal{L}$ is its key space, $\mathcal{A}$ is its associated-data space, $\mathcal{M}$ is its message space, $\mathcal{C}$ is its ciphertext space, and $\mathcal{T}$ is its binding-tag space. For TBC, its set of keys is $\mathcal{K}$, its set of tweaks is $\mathcal{T}$, and its set of plaintexts or ciphertexts is $\mathcal{L}$.

ENC and DEC are shown in Fig. 5. Also refer to Fig. 1 for illustration. They are also depicted in Fig. 1. KG selects a secret key K for TBC from Σ^n. VER simply runs ver.

$\mathsf{ENC}(K, A, M)$	$\mathsf{DEC}(K, A, C, B)$
$L \leftarrow \mathsf{kg}$	$C_0 \| C_1 \leftarrow C$
$(C_0, B) \leftarrow \mathsf{enc}(L, A, M)$	$L \leftarrow \mathsf{D}_K(B, C_1)$
$C_1 \leftarrow \mathsf{E}_K(B, L)$	**if** $\mathsf{dec}(L, A, C_0, B) = \perp$ **then**
$C \leftarrow C_0 \| C_1$	**return** $\perp$
return (C, B)	**else**
	$M \leftarrow \mathsf{dec}(L, A, C_0, B)$
	return (M, L)
	end if

Fig. 5: The encryption and decryption algorithms of ECT

3.2 Security

ECT replaces AEAD of the Dodis et al. scheme with TBC. This change does not impact the confidentiality or binding properties. However, it does affect the ciphertext integrity. With ECT, a candidate for the opening key can always be obtained for a ciphertext. Thus, to ensure the ciphertext integrity, it must be intractable to create a new valid ciphertext for the binding tag of the original ciphertext and the opening key candidate.

Confidentiality. The confidentiality of ECT is reduced to the confidentiality of EC and the TPRP property of TBC:

Theorem 1 (Confidentiality). *Let* $\mathbf{A}$ *be an adversary against* ECT *making at most* q_{e}*,* q_{d}*, and* q_{c} *queries to* **Enc**, **Dec**, *and* **ChalEnc**, *respectively. Then, there exist adversaries* $\dot{\mathbf{A}}$ *and* $\mathbf{D}$ *such that*

$$\mathrm{Adv}^{\text{mo-ror}}_{\mathsf{ECT}}(\mathbf{A}) \leq q_{\mathrm{c}} \cdot \mathrm{Adv}^{\text{ot-ror}}_{\mathsf{EC}}(\dot{\mathbf{A}}) + 2 \cdot \mathrm{Adv}^{\text{tprp}}_{\mathsf{TBC}}(\mathbf{D}) + (q_{\mathrm{e}}^2 + (q_{\mathrm{e}} + q_{\mathrm{c}})^2)/2^{\ell}.$$

The run time of $\dot{\mathbf{A}}$ *and* $\mathbf{D}$ *is at most about that of* $\text{MO-REAL}^{\mathbf{A}}_{\mathsf{ECT}}$. $\mathbf{D}$ *makes at most* $(q_{\mathrm{e}} + q_{\mathrm{c}})$ *queries to its oracle.*

Proof. Shown in Appendix A. □

Ciphertext Integrity. For the ciphertext integrity of ECT, a new notion is introduced to the ciphertext unforgeability of encryptment EC:

Definition 1 (Targeted Ciphertext Unforgeability). *Let* $\mathbf{A} := (\mathbf{A}_1, \mathbf{A}_2)$ *be an adversary acting in two phases. First,* $\mathbf{A}_1$ *takes no input and outputs* (B, state)*, where* $B \in \mathcal{T}$ *and state is some state information. Then,* $\mathbf{A}_2$ *takes* (B, state) *and* K_{ec} *as input, where* $K_{\mathrm{ec}} \leftarrow \mathsf{kg}$*, and outputs* $(A, C) \in \mathcal{A} \times \mathcal{C}$*. The advantage of* $\mathbf{A}$ *for targeted ciphertext unforgeability is*

$$\mathrm{Adv}^{\text{tcu}}_{\mathsf{EC}}(\mathbf{A}) := \Pr[\mathsf{dec}(K_{\mathrm{ec}}, A, C, B) \neq \perp].$$

It is not difficult to see that the HFC encryptment scheme [15] satisfies targeted ciphertext unforgeability in the random oracle model, which is shown in Appendix C.

The ciphertext integrity of ECT is reduced to the second-ciphertext unforgeability and the targeted ciphertext unforgeability of EC and the STPRP property of TBC:

Theorem 2 (Ciphertext Integrity). *Let* $\mathbf{A}$ *be an adversary against* ECT *making at most* q_{e}*,* q_{d}*, and* q_{c} *queries to* **Enc**, **Dec**, *and* **ChalDec**, *respectively. Then, there exist adversaries* $\dot{\mathbf{A}}$*,* $\ddot{\mathbf{A}}$*, and* $\mathbf{D}$ *such that*

$$\begin{aligned}\mathrm{Adv}^{\text{mo-ctxt}}_{\mathsf{ECT}}(\mathbf{A}) \leq q_{\mathrm{e}} \cdot \mathrm{Adv}^{\text{scu}}_{\mathsf{EC}}(\dot{\mathbf{A}}) + (q_{\mathrm{d}} + q_{\mathrm{c}}) \cdot \mathrm{Adv}^{\text{tcu}}_{\mathsf{EC}}(\ddot{\mathbf{A}}) + \mathrm{Adv}^{\text{stprp}}_{\mathsf{TBC}}(\mathbf{D}) \\ + (q_{\mathrm{e}} + q_{\mathrm{d}} + q_{\mathrm{c}})^2/2^{\ell+1}.\end{aligned}$$

The run time of $\dot{\mathbf{A}}$*,* $\ddot{\mathbf{A}}$*, and* $\mathbf{D}$ *is at most about that of* $\text{MO-CTXT}^{\mathbf{A}}_{\mathsf{ECT}}$. $\mathbf{D}$ *makes at most* $q_{\mathrm{e}} + q_{\mathrm{d}} + q_{\mathrm{c}}$ *queries to its oracle.*

Proof. The game MO-CTXT$^{\mathbf{A}}_{\mathsf{ECT}}$ is shown in Fig. 6. Without loss of generality, it is assumed that $\mathbf{A}$ terminates right after *win* gets `true`.

The game MO-CTXT-G$^{\mathbf{A}}_1$ in Fig. 7 is different from MO-CTXT$^{\mathbf{A}}_{\mathsf{ECT}}$ in that the former records all the histories of E_K and D_K by "P$[B, C_1] \leftarrow L$" and uses them to answer to queries to **Dec** and **ChalDec**. Thus,

$$\mathrm{Adv}^{\text{mo-ctxt}}_{\mathsf{ECT}}(\mathbf{A}) = \Pr[\text{MO-CTXT}^{\mathbf{A}}_{\mathsf{ECT}} = \mathtt{true}] = \Pr[\text{MO-CTXT-G}^{\mathbf{A}}_1 = \mathtt{true}].$$

The game MO-CTXT-G$^{\mathbf{A}}_2$ in Fig. 8 is different from MO-CTXT-G$^{\mathbf{A}}_1$ in that the former uses a random tweakable permutation ϖ instead of TBC. Let $\mathbf{D}$ be an adversary against TBC. $\mathbf{D}$ has either $(\mathsf{E}_K, \mathsf{D}_K)$ or (ϖ, ϖ^{-1}) as an oracle and simulates MO-CTXT-G$^{\mathbf{A}}_1$ or MO-CTXT-G$^{\mathbf{A}}_2$ with the use of its oracle. Thus,

$$\mathrm{Adv}^{\text{stprp}}_{\mathsf{TBC}}(\mathbf{D}) = \big|\Pr[\text{MO-CTXT-G}^{\mathbf{A}}_1 = \mathtt{true}] - \Pr[\text{MO-CTXT-G}^{\mathbf{A}}_2 = \mathtt{true}]\big|.$$

$\mathbf{D}$ makes at most $q_\mathrm{e} + q_\mathrm{d} + q_\mathrm{c}$ queries to its oracle, and its run time is at most about that of MO-CTXT$^{\mathbf{A}}_{\mathsf{ECT}}$.

In the game MO-CTXT-G$^{\mathbf{A}}_3$ shown in Fig. 8, **Dec** and **ChalDec** select L uniformly at random from Σ^ℓ, while they call ϖ^{-1} in MO-CTXT-G$^{\mathbf{A}}_2$. As long as no collision is found for L, the games are equivalent to each other. Thus,

$$\big|\Pr[\text{MO-CTXT-G}^{\mathbf{A}}_2 = \mathtt{true}] - \Pr[\text{MO-CTXT-G}^{\mathbf{A}}_3 = \mathtt{true}]\big| \le (q_\mathrm{e}+q_\mathrm{d}+q_\mathrm{c})^2/2^{\ell+1}.$$

Now, $\Pr[\text{MO-CTXT-G}^{\mathbf{A}}_3 = \mathtt{true}]$ is evaluated. Suppose that *win* is set `true` by a query (A^*, C^*, B^*) to **ChalDec**. Let Win_1, Win_2, and Win_3 be the cases that

1. P$[B^*, C^*_1] \neq \bot$ and P$[B^*, C^*_1]$ is already set by **Enc**,
2. P$[B^*, C^*_1] \neq \bot$ and P$[B^*, C^*_1]$ is already set by **Dec** or **ChalDec**, and
3. P$[B^*, C^*_1] = \bot$,

respectively, where C^*_1 is the least significant ℓ bits of C^*. Then,

$$\Pr[\text{MO-CTXT-G}^{\mathbf{A}}_3 = \mathtt{true}] = \Pr[\mathrm{Win}_1] + \Pr[\mathrm{Win}_2] + \Pr[\mathrm{Win}_3].$$

For Win_1, suppose that **Enc** sets P$[B^*, C^*_1]$ while computing a reply $(\dot{C}, B^*)$ to a query $(\dot{A}, \dot{M})$. Then, $(\dot{A}, \dot{C}) \neq (A^*, C^*)$ since $(\dot{A}, \dot{C}, B^*) \in \mathcal{Y}$ and $(A^*, C^*, B^*) \notin \mathcal{Y}$. Thus, the following adversary $\dot{\mathbf{A}}$ with the oracle $\mathsf{enc}_{\dot{L}}$ against second-ciphertext unforgeability is successful. $\dot{\mathbf{A}}$ runs MO-CTXT-G$^{\dot{\mathbf{A}}}_3$ except that $\dot{\mathbf{A}}$ guesses $(\dot{A}, \dot{M})$, asks it to $\mathsf{enc}_{\dot{L}}$ and gets $(\dot{C}, B^*)$ and $\dot{L}$. Finally, $\dot{\mathbf{A}}$ outputs (A^*, C^*) satisfying $\mathsf{dec}(\dot{L}, A^*, C^*, B^*) \neq \bot$. Thus, $\mathrm{Adv}^{\text{scu}}_{\mathsf{EC}}(\dot{\mathbf{A}}) = \Pr[\mathrm{Win}_1]/q_\mathrm{e}$.

For Win_2 and Win_3, the following adversary $\ddot{\mathbf{A}} = (\ddot{\mathbf{A}}_1, \ddot{\mathbf{A}}_2)$ against targeted ciphertext unforgeability is successful. First, $\ddot{\mathbf{A}}_1$ runs MO-CTXT-G$^{\mathbf{A}}_3$ and guesses (B^*, C^*_1). It interrupts the execution of MO-CTXT-G$^{\mathbf{A}}_3$ right after it obtains (B^*, C^*_1) and outputs (B^*, state^*). Then, $\ddot{\mathbf{A}}_2$ takes (B^*, state^*) and $\ddot{L} \twoheadleftarrow \Sigma^\ell$ as input and resumes the execution of MO-CTXT-G$^{\mathbf{A}}_3$ by making use of state^*. Finally, $\ddot{\mathbf{A}}_2$ outputs (A^*, C^*_0) satisfying $\mathsf{dec}(\ddot{L}, A^*, C^*_0, B^*) \neq \bot$. Thus, $\mathrm{Adv}^{\text{tcu}}_{\mathsf{EC}}(\ddot{\mathbf{A}}) = (\Pr[\mathrm{Win}_2] + \Pr[\mathrm{Win}_3])/(q_\mathrm{d} + q_\mathrm{c})$. □

$K \xleftarrow{\$} \Sigma^n$; $\mathcal{Y} \leftarrow \emptyset$
$win \leftarrow \mathtt{false}$
$\mathbf{A}^{\mathbf{Enc},\mathbf{Dec},\mathbf{ChalDec}}$
return win

Enc(A, M)
$L \xleftarrow{\$} \Sigma^\ell$
$(C_0, B) \leftarrow \mathsf{enc}(L, A, M)$
$C_1 \leftarrow \mathsf{E}_K(B, L)$
$C \leftarrow C_0 \| C_1$
$\mathcal{Y} \leftarrow \mathcal{Y} \cup \{(A, C, B)\}$
return (C, B)

Dec(A, C, B)
$C_0 \| C_1 \leftarrow C$
$L \leftarrow \mathsf{D}_K(B, C_1)$
return $\mathsf{dec}(L, A, C_0, B)$

ChalDec(A, C, B)
if $(A, C, B) \in \mathcal{Y}$ **then**
  return $\perp$
end if
$C_0 \| C_1 \leftarrow C$
$L \leftarrow \mathsf{D}_K(B, C_1)$
if $\mathsf{dec}(L, A, C_0, B) = \perp$ **then**
  return $\perp$
else
  $win \leftarrow \mathtt{true}$
  $M \leftarrow \mathsf{dec}(L, A, C_0, B)$
  return (M, L)
end if

Fig. 6: Game MO-CTXT$^{\mathbf{A}}_{\mathsf{ECT}}$

$K \xleftarrow{\$} \Sigma^n$; $\mathcal{Y} \leftarrow \emptyset$
$win \leftarrow \mathtt{false}$
$\mathbf{A}^{\mathbf{Enc},\mathbf{Dec},\mathbf{ChalDec}}$
return win

Enc(A, M)
$L \xleftarrow{\$} \Sigma^\ell$
$(C_0, B) \leftarrow \mathsf{enc}(L, A, M)$
$C_1 \leftarrow \mathsf{E}_K(B, L)$
$C \leftarrow C_0 \| C_1$
$\mathcal{Y} \leftarrow \mathcal{Y} \cup \{(A, C, B)\}$
$\underline{\mathrm{P}[B, C_1] \leftarrow L}$
return (C, B)

Dec(A, C, B)
$C_0 \| C_1 \leftarrow C$
if $\mathrm{P}[B, C_1] \neq \perp$ **then**
  $\underline{L \leftarrow \mathrm{P}[B, C_1]}$
else
  $L \leftarrow \mathsf{D}_K(B, C_1)$
  $\underline{\mathrm{P}[B, C_1] \leftarrow L}$
end if
return $\mathsf{dec}(L, A, C_0, B)$

ChalDec(A, C, B)
if $(A, C, B) \in \mathcal{Y}$ **then**
  return $\perp$
end if
$C_0 \| C_1 \leftarrow C$
if $\mathrm{P}[B, C_1] \neq \perp$ **then**
  $\underline{L \leftarrow \mathrm{P}[B, C_1]}$
else
  $L \leftarrow \mathsf{D}_K(B, C_1)$
  $\underline{\mathrm{P}[B, C_1] \leftarrow L}$
end if
if $\mathsf{dec}(L, A, C_0, B) = \perp$ **then**
  return $\perp$
else
  $win \leftarrow \mathtt{true}$
  $M \leftarrow \mathsf{dec}(L, A, C_0, B)$
  return (M, L)
end if

Fig. 7: MO-CTXT-G$^{\mathbf{A}}_1$. All the entries of the table P are initialized by $\perp$.

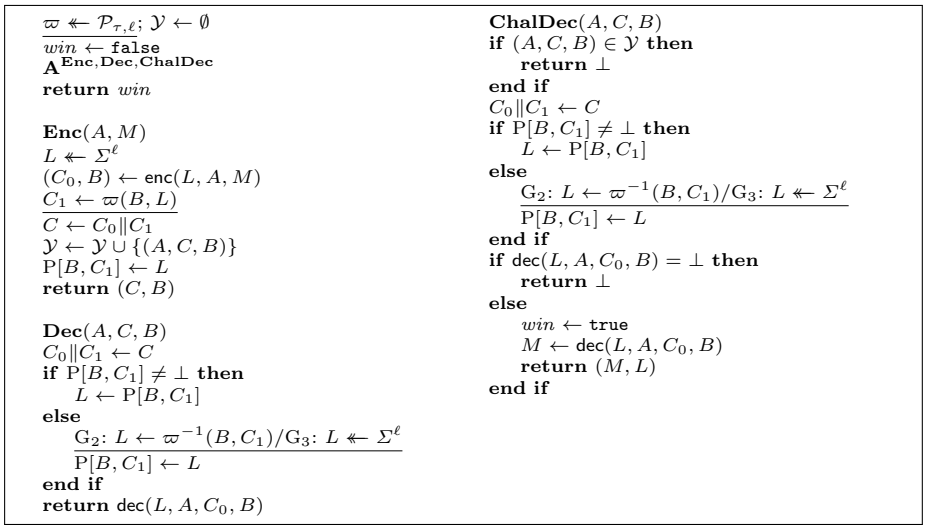


Fig. 8: MO-CTXT-$\mathrm{G}_2^{\mathbf{A}}$ and MO-CTXT-$\mathrm{G}_3^{\mathbf{A}}$

Binding Properties. ECT inherits (strong) receiver binding from EC.

ECT also inherits sender binding from EC. Suppose that (K, A, C, B) satisfies $\mathsf{DEC}(K, A, C, B) \neq \perp$ and $\mathsf{VER}(A, M, L, B) = 0$, where $(M, L) \leftarrow \mathsf{DEC}(K, A, C, B)$. Then, $L = \mathsf{D}_K(B, C_1)$, $\mathsf{dec}(L, A, C_0, B) = M$ and $M \neq \perp$, where $C = C_0 \| C_1$. In addition, $\mathsf{ver}(A, M, L, B) = 0$.

4 Remotely Keyed ccAEAD

RK ccAEAD is a particular type of ccAEAD. Their difference is that, for RK ccAEAD, some parts of encryption and decryption are done by a trusted device keeping the secret key. A user or a host performs encryption and/or decryption by making use of the trusted device. The amount of computation for the trusted device is required to be independent of the lengths of a message, associated data, and a ciphertext due to the common case that the computational power of the trusted device is limited.

Dodis et al. [16] left it as an open problem to formalize and construct RK ccAEAD schemes. An answer will be given to the problem in this section.

4.1 Syntax

RK ccAEAD is formalized as a tuple of algorithms $\mathsf{RKCAE} = (\mathsf{RKKg}, \mathsf{RKEnc}, \mathsf{RKDec}, \mathsf{RKVer})$. It is involved with a key space $\mathcal{K} := \Sigma^n$, an associated-data space $\mathcal{A} \subseteq \Sigma^*$, a message space $\mathcal{M} \subseteq \Sigma^*$, a ciphertext space $\mathcal{C} \subseteq \Sigma^*$, an opening-key space $\mathcal{L} := \Sigma^\ell$, and a binding-tag space $\mathcal{T} := \Sigma^\tau$.

In the formalization below, for simplicity, it is assumed that the trusted device is called only once during encryption and decryption:

– The key generation algorithm RKKg returns a secret key $K \in \mathcal{K}$ chosen uniformly at random.
– The encryption algorithm RKEnc takes as input $(K, A, M) \in \mathcal{K} \times \mathcal{A} \times \mathcal{M}$ and returns $(C, B) \in \mathcal{C} \times \mathcal{T}$. K is given to an algorithm TE, and it is run by a trusted device. The encryption proceeds in the following three steps:

$$(Q_{\mathrm{e}}, S_{\mathrm{e}}) \leftarrow \mathsf{Pre\text{-}TE}(A, M); R_{\mathrm{e}} \leftarrow \mathsf{TE}_K(Q_{\mathrm{e}}); (C, B) \leftarrow \mathsf{Post\text{-}TE}(R_{\mathrm{e}}, S_{\mathrm{e}}),$$

where S_{e} is some state information.
– The decryption algorithm RKDec takes as input $(K, A, C, B) \in \mathcal{K} \times \mathcal{A} \times \mathcal{C} \times \mathcal{T}$ and returns $(M, L) \in \mathcal{M} \times \mathcal{L}$ or $\perp \notin \mathcal{M} \times \mathcal{L}$. K is given to an algorithm TD, and it is run by a trusted device. The decryption proceeds in the following three steps:

$$(Q_{\mathrm{d}}, S_{\mathrm{d}}) \leftarrow \mathsf{Pre\text{-}TD}(A, C, B); R_{\mathrm{d}} \leftarrow \mathsf{TD}_K(Q_{\mathrm{d}}); (M, L)/\perp \leftarrow \mathsf{Post\text{-}TD}(R_{\mathrm{d}}, S_{\mathrm{d}}),$$

where S_{d} is some state information.
– The verification algorithm RKVer takes as input $(A, M, L, B) \in \mathcal{A} \times \mathcal{M} \times \mathcal{L} \times \mathcal{T}$ and returns $b \in \Sigma$.

As well as CAE, RKCAE satisfies correctness. For every $l \in \mathbb{N}$, $\Sigma^l \subseteq \mathcal{M}$ or $\Sigma^l \cap \mathcal{M} = \emptyset$. For any message M and the corresponding ciphertext C, $|C|$ depends only on $|M|$ and let $|C| = \mathsf{clen}(|M|)$.

4.2 Security Requirement

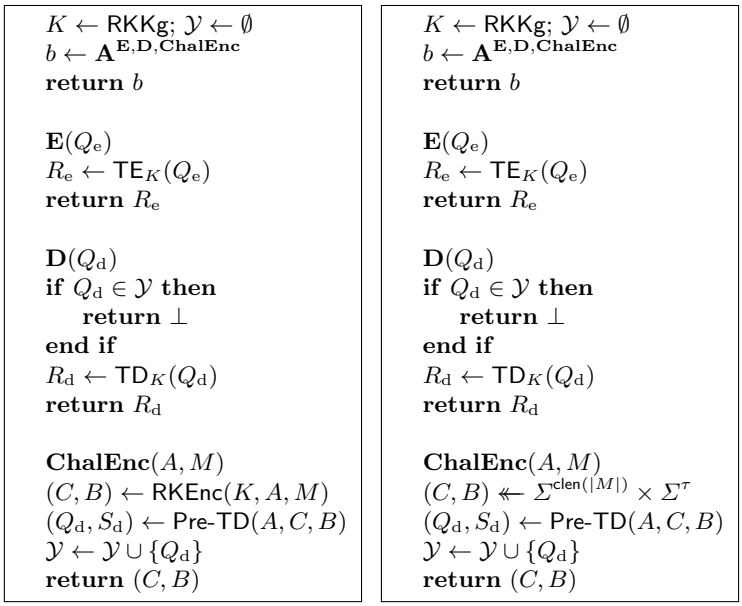
For RK ccAEAD, an adversary is allowed to have direct access to the trusted device. Thus, the adversary can run RKEnc and RKDec by using TE_K and TD_K as oracles, respectively.

Confidentiality. Confidentiality of RK ccAEAD is defined as real-or-random indistinguishability. The games RK-REAL and RK-RAND shown in Fig. 9 are introduced. An adversary $\mathbf{A}$ is given access to oracles $\mathbf{E}$, $\mathbf{D}$, and $\mathbf{ChalEnc}$. $\mathbf{A}$ is not allowed to decrypt (A, C, B) obtained by asking (A, M) to $\mathbf{ChalEnc}$. The advantage of $\mathbf{A}$ for confidentiality is

$$\mathrm{Adv}^{\text{rk-ror}}_{\mathsf{RKCAE}}(\mathbf{A}) := \left|\Pr[\text{RK-REAL}^{\mathbf{A}}_{\mathsf{RKCAE}} = 1] - \Pr[\text{RK-RAND}^{\mathbf{A}}_{\mathsf{RKCAE}} = 1]\right|.$$

Ciphertext Integrity. The game $\text{RK-CTXT}^{\mathbf{A}}_{\mathsf{RKCAE}}$, shown in Fig. 10, is introduced. An adversary $\mathbf{A}$ is given access to oracles $\mathbf{E}$, $\mathbf{D}$, and $\mathbf{ChalDec}$. $\mathbf{A}$ is not allowed to repeat the same queries to $\mathbf{ChalDec}$. The game outputs `true` if the number of valid ciphertexts produced by $\mathbf{A}$ is greater than the number of queries to $\mathbf{E}$ made by $\mathbf{A}$. The advantage of $\mathbf{A}$ for ciphertext integrity is

$$\mathrm{Adv}^{\text{rk-ctxt}}_{\mathsf{RKCAE}}(\mathbf{A}) := \Pr[\text{RK-CTXT}^{\mathbf{A}}_{\mathsf{RKCAE}} = \texttt{true}].$$



(a) $\text{RK-REAL}^{\mathbf{A}}_{\mathsf{RKCAE}}$ (b) $\text{RK-RAND}^{\mathbf{A}}_{\mathsf{RKCAE}}$

Fig. 9: Games for confidentiality of RK ccAEAD

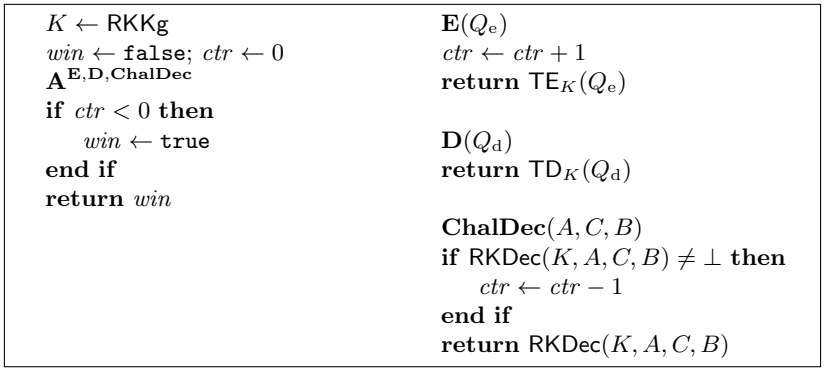


Fig. 10: Game $\text{RK-CTXT}^{\mathbf{A}}_{\mathsf{RKCAE}}$ for ciphertext integrity of RK ccAEAD

Binding Properties. $\mathrm{Adv}^{\text{r-bind}}_{\mathsf{RKCAE}}$, $\mathrm{Adv}^{\text{sr-bind}}_{\mathsf{RKCAE}}$, and $\mathrm{Adv}^{\text{s-bind}}_{\mathsf{RKCAE}}$ are defined as $\mathrm{Adv}^{\text{r-bind}}_{\mathsf{CAE}}$, $\mathrm{Adv}^{\text{sr-bind}}_{\mathsf{CAE}}$, and $\mathrm{Adv}^{\text{s-bind}}_{\mathsf{CAE}}$, respectively, simply by replacing Dec with RKDec and Ver with RKVer.

5 ECT as RK ccAEAD

5.1 Scheme

ECT functions as RK ccAEAD if E and D of TBC are used for TE and TD, respectively. For simplicity, ECT as RK ccAEAD is called RK ECT in the remaining parts.

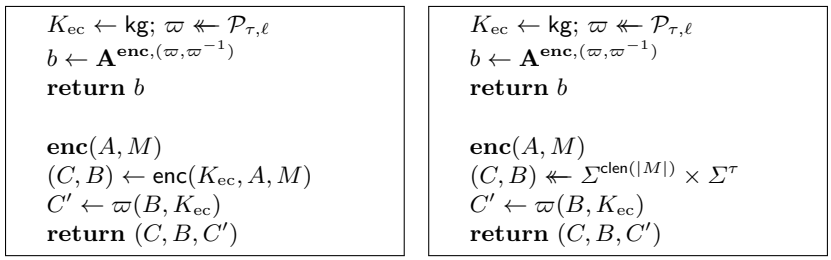
5.2 Security

Confidentiality. The crucial difference between RK ECT and ordinary ECT is that, for a ciphertext (C, B), the former allows adversaries to check whether $L' \in \mathcal{L}$ is the corresponding opening key or not only by asking (B, L') to E_K. It requires a new notion on the confidentiality of encryptment for the confidentiality of RK ECT:

Definition 2 (Confidentiality with Attachment). *Two games* $\widetilde{\mathrm{otREAL}}$ *and* $\widetilde{\mathrm{otRAND}}$ *shown in Fig. 11 are introduced to formalize confidentiality. In both of the games, an adversary* $\mathbf{A}$ *is allowed to ask only a single query to the oracle* **enc***, while* $\mathbf{A}$ *is allowed to ask multiple queries adaptively to the oracle* (ϖ, ϖ^{-1})*. The advantage of* $\mathbf{A}$ *for confidentiality is*

$$\widetilde{\mathrm{Adv}}^{\text{ot-ror}}_{\mathsf{EC}}(\mathbf{A}) := \left|\Pr[\widetilde{\mathrm{otREAL}}^{\mathbf{A}}_{\mathsf{EC}} = 1] - \Pr[\widetilde{\mathrm{otRAND}}^{\mathbf{A}}_{\mathsf{EC}} = 1]\right|,$$

It is shown that the HFC encryptment scheme [15] satisfies confidentiality with attachment in the random oracle model in Appendix C.



(a) $\widetilde{\mathrm{otREAL}}^{\mathbf{A}}_{\mathsf{EC}}$ (b) $\widetilde{\mathrm{otRAND}}^{\mathbf{A}}_{\mathsf{EC}}$

Fig. 11: The games for confidentiality of encryptment

The confidentiality of RK ECT is reduced to the confidentiality of EC with attachment and the STPRP of TBC:

Theorem 3 (Confidentiality). *Let* $\mathbf{A}$ *be an adversary against RK* ECT *making at most* q_{e}, q_{d}, *and* q_{c} *queries to* $\mathbf{E}$, $\mathbf{D}$, *and* **ChalEnc**, *respectively. Then, there exist adversaries* $\dot{\mathbf{A}}$ *and* $\mathbf{D}$ *such that*

$$\mathrm{Adv}^{\text{rk-ror}}_{\mathsf{ECT}}(\mathbf{A}) \le q_{\mathrm{c}} \cdot \widetilde{\mathrm{Adv}}^{\text{ot-ror}}_{\mathsf{EC}}(\dot{\mathbf{A}}) + 2 \cdot \mathrm{Adv}^{\text{stprp}}_{\mathsf{TBC}}(\mathbf{D}) + q_{\mathrm{c}}(q_{\mathrm{e}} + q_{\mathrm{d}} + q_{\mathrm{c}})/2^{\ell-1}.$$

The run time of $\dot{\mathbf{A}}$ *and* $\mathbf{D}$ *is at most about that of* $\text{RK-REAL}^{\mathbf{A}}_{\mathsf{ECT}}$. $\dot{\mathbf{A}}$ *makes at most* $q_{\mathrm{e}}+q_{\mathrm{d}}+q_{\mathrm{c}}$ *queries to the uniform random tweakable permutation* (ϖ, ϖ^{-1}). $\mathbf{D}$ *makes at most* $q_{\mathrm{e}} + q_{\mathrm{d}} + q_{\mathrm{c}}$ *queries to its oracle.*

Proof. For the games $\text{RK-REAL}^{\mathbf{A}}_{\mathsf{ECT}}$ and $\text{RK-RAND}^{\mathbf{A}}_{\mathsf{ECT}}$ in Fig. 12,

$$\mathrm{Adv}^{\text{rk-ror}}_{\mathsf{ECT}}(\mathbf{A}) = \left|\Pr[\text{RK-REAL}^{\mathbf{A}}_{\mathsf{ECT}} = 1] - \Pr[\text{RK-RAND}^{\mathbf{A}}_{\mathsf{ECT}} = 1]\right|.$$

The game $\text{RK-ROR-G}^{\mathbf{A}}_{1}$ in Fig. 13 is different from $\text{RK-REAL}^{\mathbf{A}}_{\mathsf{ECT}}$ in that the former uses a random tweakable permutation ϖ instead of TBC. Let $\mathbf{D}_1$ be an adversary against TBC. $\mathbf{D}_1$ has either $(\mathsf{E}_K, \mathsf{D}_K)$ or (ϖ, ϖ^{-1}) as an oracle and simulates $\text{RK-REAL}^{\mathbf{A}}_{\mathsf{ECT}}$ or $\text{RK-ROR-G}^{\mathbf{A}}_{1}$, respectively. Then,

$$\mathrm{Adv}^{\text{stprp}}_{\mathsf{TBC}}(\mathbf{D}_1) = \left|\Pr[\text{RK-REAL}^{\mathbf{A}}_{\mathsf{ECT}} = 1] - \Pr[\text{RK-ROR-G}^{\mathbf{A}}_{1} = 1]\right|.$$

$\mathbf{D}_1$ makes at most $q_{\mathrm{e}} + q_{\mathrm{d}} + q_{\mathrm{c}}$ queries to its oracle, and its run time is at most about that of $\text{RK-REAL}^{\mathbf{A}}_{\mathsf{ECT}}$.

The game $\text{RK-ROR-G}^{\mathbf{A}}_{2}$ in Fig. 14 is different from $\text{RK-ROR-G}^{\mathbf{A}}_{1}$ in that the former selects (C_0, B) uniformly at random. Thus, from the hybrid argument, there exists some $\dot{\mathbf{A}}$ such that

$$\left|\Pr[\text{RK-ROR-G}^{\mathbf{A}}_{1} = 1] - \Pr[\text{RK-ROR-G}^{\mathbf{A}}_{2} = 1]\right| \le q_{\mathrm{c}} \cdot \widetilde{\mathrm{Adv}}^{\text{ot-ror}}_{\mathsf{EC}}(\dot{\mathbf{A}}).$$

$\dot{\mathbf{A}}$ makes at most $q_{\mathrm{e}} + q_{\mathrm{d}} + q_{\mathrm{c}}$ queries to (ϖ, ϖ^{-1}). The run time of $\dot{\mathbf{A}}$ is at most about that of $\text{RK-REAL}^{\mathbf{A}}_{\mathsf{ECT}}$.

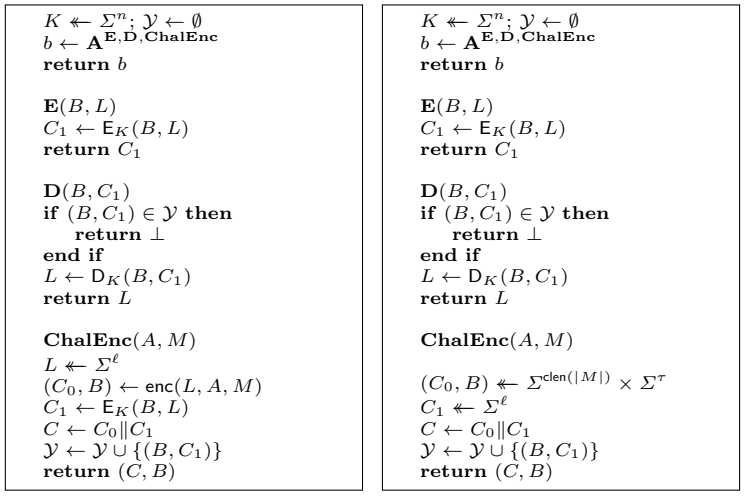
The game $\text{RK-ROR-G}^{\mathbf{A}}_{3}$ in Fig. 14 is different from $\text{RK-ROR-G}^{\mathbf{A}}_{2}$ in that **ChalEnc** selects C_1 uniformly at random from Σ^{ℓ} in the former game. As long as no collision is found for L and C_1, $\text{RK-ROR-G}^{\mathbf{A}}_{3}$ is equivalent to $\text{RK-ROR-G}^{\mathbf{A}}_{2}$. Thus,

$$\left|\Pr[\text{RK-ROR-G}^{\mathbf{A}}_{2} = 1] - \Pr[\text{RK-ROR-G}^{\mathbf{A}}_{3} = 1]\right| \le q_{\mathrm{c}}(q_{\mathrm{e}} + q_{\mathrm{d}} + q_{\mathrm{c}})/2^{\ell-1}.$$

For $\text{RK-ROR-G}^{\mathbf{A}}_{3}$ and $\text{RK-RAND}^{\mathbf{A}}_{\mathsf{ECT}}$, similar to the transformation from $\text{RK-REAL}^{\mathbf{A}}_{\mathsf{ECT}}$ to $\text{RK-ROR-G}^{\mathbf{A}}_{1}$, there exists some $\mathbf{D}_2$ such that

$$\left|\Pr[\text{RK-ROR-G}^{\mathbf{A}}_{3}] - \Pr[\text{RK-RAND}^{\mathbf{A}}_{\mathsf{ECT}} = 1]\right| \le \mathrm{Adv}^{\text{stprp}}_{\mathsf{TBC}}(\mathbf{D}_2).$$

$\mathbf{D}_2$ makes at most $q_{\mathrm{e}} + q_{\mathrm{d}}$ queries to its oracle, and its run time is at most about that of $\text{RK-RAND}^{\mathbf{A}}_{\mathsf{ECT}}$. □



(a) RK-REAL$^{\mathbf{A}}_{\mathsf{ECT}}$ (b) RK-RAND$^{\mathbf{A}}_{\mathsf{ECT}}$

Fig. 12: Games for confidentiality of RK ECT

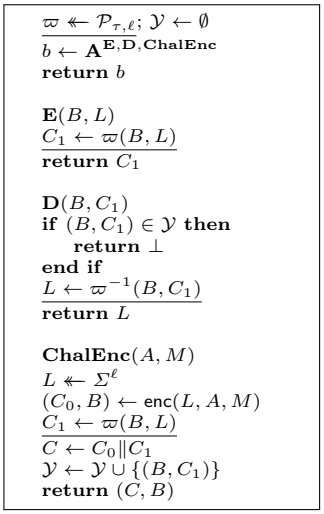


Fig. 13: RK-ROR-G$^{\mathbf{A}}_1$

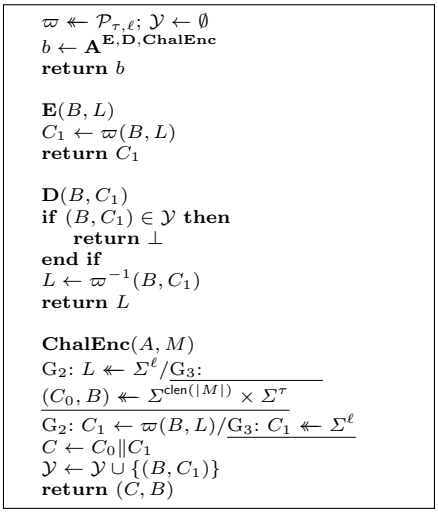


Fig. 14: RK-ROR-G$^{\mathbf{A}}_2$ and RK-ROR-G$^{\mathbf{A}}_3$

Ciphertext Integrity. The ciphertext integrity of RK ECT is reduced to the receiver-binding and the targeted ciphertext unforgeability of EC and the STPRP property of TBC:

Theorem 4 (Ciphertext Integrity). *Suppose that the encryptment scheme used for RK* ECT *satisfies strong correctness. Let* $\mathbf{A}$ *be an adversary against RK* ECT *making at most* q_{e}*,* q_{d}*, and* q_{c} *queries to* $\mathbf{E}$*,* $\mathbf{D}$*, and* **ChalDec***, respectively. Then, there exist adversaries* $\dot{\mathbf{A}}$*,* $\ddot{\mathbf{A}}$*, and* $\mathbf{D}$ *such that*

$$\mathrm{Adv}^{\text{rk-ctxt}}_{\mathsf{ECT}}(\mathbf{A}) \leq \mathrm{Adv}^{\text{r-bind}}_{\mathsf{EC}}(\dot{\mathbf{A}}) + (q_{\mathrm{d}} + q_{\mathrm{c}}) \cdot \mathrm{Adv}^{\text{tcu}}_{\mathsf{EC}}(\ddot{\mathbf{A}}) + \mathrm{Adv}^{\text{stprp}}_{\mathsf{TBC}}(\mathbf{D}) + (q_{\mathrm{e}} + q_{\mathrm{d}} + q_{\mathrm{c}})^2/2^{\ell}.$$

The run time of $\dot{\mathbf{A}}$*,* $\ddot{\mathbf{A}}$*, and* $\mathbf{D}$ *is at most about that of* $\text{RK-CTXT}^{\mathbf{A}}_{\mathsf{ECT}}$*.* $\mathbf{D}$ *makes at most* $q_{\mathrm{e}} + q_{\mathrm{d}} + q_{\mathrm{c}}$ *queries to its oracles.*

Proof. Shown in Appendix B. □

Binding Properties. To see ECT as RK ccAEAD does not affect the binding properties. Thus, as discussed in Sect. 3.2, RK ECT inherits both (strong) receiver binding and sender binding from EC.

6 Conclusions

We have studied the problem of constructing compactly committing AEAD (ccAEAD) based on encryptment, originally proposed by Dodis et al. [15,16] in the context of end-to-end messaging. We proposed ECT, a conceptually simplified, more efficient construction than those proposed by Dodis et al. by using a TBC instead of AEAD. We also present a formalization of remotely keyed variant of ccAEAD (RK ccAEAD) and show that our ECT is indeed RK ccAEAD, which addresses the open question posed by Dodis et al. [16] positively. This indicates that ECT is useful when ccAEAD is implemented on the platform consisting of (small, slow) trusted and untrusted (but cheap and fast) modules. Future work is to explore the relationship between remotely keyed ccAEAD and leakage-resilient AEAD. It is also interesting to see if other generic constructions such as CtE and CEP in [20] can be simplified.

Acknowledgements. The authors thank Akiko Inoue for fruitful discussions. The first author was supported by JSPS KAKENHI Grant Number 21K11885.

References

1. Albertini, A., Duong, T., Gueron, S., Kölbl, S., Luykx, A., Schmieg, S.: How to abuse and fix authenticated encryption without key commitment. In: Butler, K.R.B., Thomas, K. (eds.) 31st USENIX Security Symposium, USENIX Security 2022. pp. 3291–3308. USENIX Association (2022), `https://www.usenix.org/conference/usenixsecurity22/presentation/albertini`

2. Bellare, M., Hoang, V.T.: Efficient schemes for committing authenticated encryption. In: Dunkelman, O., Dziembowski, S. (eds.) EUROCRYPT 2022. Lecture Notes in Computer Science, vol. 13276, pp. 845–875. Springer (2022). https://doi.org/10.1007/978-3-031-07085-3_29
3. Bellare, M., Namprempre, C.: Authenticated encryption: Relations among notions and analysis of the generic composition paradigm. In: Okamoto, T. (ed.) ASIACRYPT 2000. Lecture Notes in Computer Science, vol. 1976, pp. 531–545. Springer (2000). https://doi.org/10.1007/3-540-44448-3_41
4. Bellare, M., Rogaway, P.: The security of triple encryption and a framework for code-based game-playing proofs. In: Vaudenay, S. (ed.) EUROCRYPT 2006. Lecture Notes in Computer Science, vol. 4004, pp. 409–426. Springer (2006). https://doi.org/10.1007/11761679_25
5. Bellizia, D., Bronchain, O., Cassiers, G., Grosso, V., Guo, C., Momin, C., Pereira, O., Peters, T., Standaert, F.: Mode-level vs. implementation-level physical security in symmetric cryptography - A practical guide through the leakage-resistance jungle. In: Micciancio, D., Ristenpart, T. (eds.) CRYPTO 2020. Lecture Notes in Computer Science, vol. 12170, pp. 369–400. Springer (2020). https://doi.org/10.1007/978-3-030-56784-2_13
6. Berti, F., Guo, C, Pereira, O., Peters, T., Standaert, F-X.,: TEDT, a leakage-resistant AEAD mode for high physical security applications. IACR Trans. Cryptogr. Hardw. Embed. Syst. 2020(1): 256-320 (2020). https://doi.org/10.13154/tches.v2020.i1.256-320
7. Berti, F., Pereira, O., Standaert, F.: Reducing the cost of authenticity with leakages: a CIML2-secure AE scheme with one call to a strongly protected tweakable block cipher. In: Buchmann, J., Nitaj, A., Rachidi, T. (eds.) AFRICACRYPT 2019. Lecture Notes in Computer Science, vol. 11627, pp. 229–249. Springer (2019). https://doi.org/10.1007/978-3-030-23696-0_12
8. Blaze, M.: High-bandwidth encryption with low-bandwidth smartcards. In: Gollmann, D. (ed.) FSE '96. Lecture Notes in Computer Science, vol. 1039, pp. 33–40. Springer (1996). https://doi.org/10.1007/3-540-60865-6_40
9. Blaze, M., Feigenbaum, J., Naor, M.: A formal treatment of remotely keyed encryption. In: Nyberg, K. (ed.) EUROCRYPT '98. Lecture Notes in Computer Science, vol. 1403, pp. 251–265. Springer (1998). https://doi.org/10.1007/BFb0054131
10. Chan, J., Rogaway, P.: On committing authenticated-encryption. In: Atluri, V., Pietro, R.D., Jensen, C.D., Meng, W. (eds.) ESORICS 2022. Lecture Notes in Computer Science, vol. 13555, pp. 275–294. Springer (2022). https://doi.org/10.1007/978-3-031-17146-8_14
11. Chen, L., Tang, Q.: People who live in glass houses should not throw stones: Targeted opening message franking schemes. Cryptology ePrint Archive, Report 2018/994 (2018), https://eprint.iacr.org/2018/994
12. Damgård, I.: A design principle for hash functions. In: Brassard, G. (ed.) CRYPTO '89. Lecture Notes in Computer Science, vol. 435, pp. 416–427. Springer (1989). https://doi.org/10.1007/0-387-34805-0_39
13. Dobraunig, C., Eichlseder, M., Mangard, S., Mendel, F., Mennink, B., Primas, R., and Unterluggauer, T.: Isap v2.0. IACR Trans. Symmetric Cryptol. 2020(S1): 390-416 (2020) https://doi.org/https://doi.org/10.13154/tosc.v2020.iS1.390-416
14. Dodis, Y., An, J.H.: Concealment and its applications to authenticated encryption. In: Biham, E. (ed.) EUROCRYPT 2003. Lecture Notes in Computer Science, vol. 2656, pp. 312–329. Springer (2003). https://doi.org/10.1007/3-540-39200-9_19

15. Dodis, Y., Grubbs, P., Ristenpart, T., Woodage, J.: Fast message franking: From invisible salamanders to encryptment. In: Shacham, H., Boldyreva, A. (eds.) CRYPTO 2018. Lecture Notes in Computer Science, vol. 10991, pp. 155–186. Springer (2018). https://doi.org/10.1007/978-3-319-96884-1_6
16. Dodis, Y., Grubbs, P., Ristenpart, T., Woodage, J.: Fast message franking: From invisible salamanders to encryptment. Cryptology ePrint Archive, Paper 2019/016 (2019), https://eprint.iacr.org/2019/016
17. Facebook: Facebook messenger. https://www.messenger.com, accessed on 09/10/2022
18. Facebook: Messenger secret conversations. Technical Whitepaper (2016), https://about.fb.com/wp-content/uploads/2016/07/messenger-secret-conversations-technical-whitepaper.pdf
19. Farshim, P., Orlandi, C., Rosie, R.: Security of symmetric primitives under incorrect usage of keys. IACR Transactions on Symmetric Cryptology **2017**(1), 449–473 (2017). https://doi.org/10.13154/tosc.v2017.i1.449-473
20. Grubbs, P., Lu, J., Ristenpart, T.: Message franking via committing authenticated encryption. In: Katz, J., Shacham, H. (eds.) CRYPTO 2017. Lecture Notes in Computer Science, vol. 10403, pp. 66–97. Springer (2017). https://doi.org/10.1007/978-3-319-63697-9_3
21. Hirose, S.: Compactly committing authenticated encryption using tweakable block cipher. In: Kutylowski, M., Zhang, J., Chen, C. (eds.) NSS 2020. Lecture Notes in Computer Science, vol. 12570, pp. 187–206. Springer (2020). https://doi.org/10.1007/978-3-030-65745-1_11
22. Huang, Q., Yang, G., Wong, D.S., Susilo, W.: Efficient strong designated verifier signature schemes without random oracle or with non-delegatability. International Journal of Information Security **10**(6), 373–385 (2011). https://doi.org/10.1007/s10207-011-0146-1
23. Huguenin-Dumittan, L., Leontiadis, I.: A message franking channel. In: Yu, Y., Yung, M. (eds.) Inscrypt 2021. Lecture Notes in Computer Science, vol. 13007, pp. 111–128. Springer (2021). https://doi.org/10.1007/978-3-030-88323-2_6
24. Jakobsson, M., Sako, K., Impagliazzo, R.: Designated verifier proofs and their applications. In: Maurer, U.M. (ed.) EUROCRYPT '96. Lecture Notes in Computer Science, vol. 1070, pp. 143–154. Springer (1996). https://doi.org/10.1007/3-540-68339-9_13
25. Jakobsson, M., Stern, J.P., Yung, M.: Scramble all, encrypt small. In: Knudsen, L.R. (ed.) FSE '99. Lecture Notes in Computer Science, vol. 1636, pp. 95–111. Springer (1999). https://doi.org/10.1007/3-540-48519-8_8
26. Katz, J., Yung, M.: Complete characterization of security notions for probabilistic private-key encryption. In: Proceedings of the Thirty-Second Annual ACM Symposium on Theory of Computing. pp. 245–254 (2000)
27. Len, J., Grubbs, P., Ristenpart, T.: Partitioning oracle attacks. In: Bailey, M., Greenstadt, R. (eds.) 30th USENIX Security Symposium, USENIX Security 2021. pp. 195–212. USENIX Association (2021), https://www.usenix.org/conference/usenixsecurity21/presentation/len
28. Leontiadis, I., Vaudenay, S.: Private message franking with after opening privacy. Cryptology ePrint Archive, Report 2018/938 (2018), https://eprint.iacr.org/2018/938
29. Liskov, M.D., Rivest, R.L., Wagner, D.A.: Tweakable block ciphers. In: Yung, M. (ed.) CRYPTO 2002. Lecture Notes in Computer Science, vol. 2442, pp. 31–46. Springer (2002). https://doi.org/10.1007/3-540-45708-9_3

30. Liskov, M.D., Rivest, R.L., Wagner, D.A.: Tweakable block ciphers. Journal of Cryptology **24**(3), 588–613 (2011). https://doi.org/10.1007/s00145-010-9073-y
31. Lucks, S.: On the security of remotely keyed encryption. In: Biham, E. (ed.) FSE '97. Lecture Notes in Computer Science, vol. 1267, pp. 219–229. Springer (1997). https://doi.org/10.1007/BFb0052349,
32. Lucks, S.: Accelerated remotely keyed encruption. In: Knudsen, L.R. (ed.) FSE '99. Lecture Notes in Computer Science, vol. 1636, pp. 112–123. Springer (1999). https://doi.org/10.1007/3-540-48519-8_9
33. Merkle, R.C.: One way hash functions and DES. In: Brassard, G. (ed.) CRYPTO '89. Lecture Notes in Computer Science, vol. 435, pp. 428–446. Springer (1989). https://doi.org/10.1007/0-387-34805-0_40
34. Naito, Y., Sasaki, Y., Sugawara, T.: Secret can be public: Low-memory AEAD mode for high-order masking. In: Dodis, Y., Shrimpton, T. (eds.) CRYPTO 2022. Lecture Notes in Computer Science, vol. 13509, pp. 315–345. Springer (2022). https://doi.org/10.1007/978-3-031-15982-4_11
35. Shen, Y., Peters, T., Standaert, F., Cassiers, G., Verhamme, C.: Triplex: an efficient and one-pass leakage-resistant mode of operation. IACR Trans. Cryptogr. Hardw. Embed. Syst. **2022**(4), 135–162 (2022). https://doi.org/10.46586/tches.v2022.i4.135-162
36. Signal Foundation: Signal. `https://signal.org/`, accessed on 09/10/2022
37. Tyagi, N., Grubbs, P., Len, J., Miers, I., Ristenpart, T.: Asymmetric message franking: Content moderation for metadata-private end-to-end encryption. In: Boldyreva, A., Micciancio, D. (eds.) CRYPTO 2019. Lecture Notes in Computer Science, vol. 11694, pp. 222–250. Springer (2019). https://doi.org/10.1007/978-3-030-26954-8_8
38. WhatsApp: WhatsApp Messenger. `https://www.whatsapp.com`, accessed on 09/10/2022
39. Yamamuro, H., Hara, K., Tezuka, M., Yoshida, Y., Tanaka, K.: Forward secure message franking. In: Park, J.H., Seo, S. (eds.) ICISC 2021. Lecture Notes in Computer Science, vol. 13218, pp. 339–358. Springer (2021). https://doi.org/10.1007/978-3-031-08896-4_18

A Proof of Theorem 1

For the games $\text{MO-REAL}^{\mathbf{A}}_{\mathsf{ECT}}$ and $\text{MO-RAND}^{\mathbf{A}}_{\mathsf{ECT}}$ in Fig. 15,

$$\text{Adv}^{\text{mo-ror}}_{\mathsf{ECT}}(\mathbf{A}) = \left|\Pr[\text{MO-REAL}^{\mathbf{A}}_{\mathsf{ECT}} = 1] - \Pr[\text{MO-RAND}^{\mathbf{A}}_{\mathsf{ECT}} = 1]\right|.$$

The game $\text{MO-ROR-G}^{\mathbf{A}}_1$ in Fig. 16 is different from $\text{MO-REAL}^{\mathbf{A}}_{\mathsf{ECT}}$ in that the former records all the histories of **Enc** by "$\text{R}[A, C, B] \leftarrow (M, L)$" and uses them to answer to the queries to **Dec**. Thus,

$$\Pr[\text{MO-ROR-G}^{\mathbf{A}}_1 = 1] = \Pr[\text{MO-REAL}^{\mathbf{A}}_{\mathsf{ECT}} = 1].$$

The game $\text{MO-ROR-G}^{\mathbf{A}}_2$ in Fig. 17 is different from $\text{MO-ROR-G}^{\mathbf{A}}_1$ in that the former uses a random tweakable permutation ϖ instead of E_K. Let $\mathbf{D}_1$ be an adversary against TBC. $\mathbf{D}_1$ has either E_K or ϖ as an oracle and simulates $\text{MO-ROR-G}^{\mathbf{A}}_1$ or $\text{MO-ROR-G}^{\mathbf{A}}_2$ with the use of its oracle. Thus,

$$\text{Adv}^{\text{tprp}}_{\mathsf{TBC}}(\mathbf{D}_1) = \left|\Pr[\text{MO-ROR-G}^{\mathbf{A}}_1 = 1] - \Pr[\text{MO-ROR-G}^{\mathbf{A}}_2 = 1]\right|.$$

$\mathbf{D}_1$ makes at most $q_\mathrm{e}+q_\mathrm{c}$ queries to its oracle, and its run time is at most about that of MO-REAL$^{\mathbf{A}}_{\mathsf{ECT}}$.

The game MO-ROR-G$^{\mathbf{A}}_3$ in Fig. 18 is different from MO-ROR-G$^{\mathbf{A}}_2$ in that the former selects C_1 uniformly at random from Σ^ℓ instead of asking (B,L) to ϖ. As long as no collision is found for L and C_1, MO-ROR-G$^{\mathbf{A}}_3$ is equivalent to MO-ROR-G$^{\mathbf{A}}_2$. L is selected uniformly at random from Σ^ℓ, Thus,

$$\left|\Pr[\text{MO-ROR-G}^{\mathbf{A}}_2=1]-\Pr[\text{MO-ROR-G}^{\mathbf{A}}_3=1]\right| \le (q_\mathrm{e}+q_\mathrm{c})^2/2^\ell.$$

The game MO-ROR-G$_4$ in Fig. 19 is different from MO-ROR-G$^{\mathbf{A}}_3$ in that the former selects (C_0,B) uniformly at random from $\Sigma^{\mathsf{clen}(|M|)}\times\Sigma^\tau$. Thus, from the hybrid argument, there exists some $\dot{\mathbf{A}}$ such that

$$\left|\Pr[\text{MO-ROR-G}^{\mathbf{A}}_3=1]-\Pr[\text{MO-ROR-G}^{\mathbf{A}}_4=1]\right| \le q_\mathrm{c}\cdot \mathrm{Adv}^{\text{ot-ror}}_{\mathsf{EC}}(\dot{\mathbf{A}})$$

and the run time of $\dot{\mathbf{A}}$ is at most about that of MO-REAL$^{\mathbf{A}}_{\mathsf{ECT}}$.

For MO-ROR-G$^{\mathbf{A}}_4$ and MO-RAND$^{\mathbf{A}}_{\mathsf{ECT}}$, similar to the transformation from MO-REAL$^{\mathbf{A}}_{\mathsf{ECT}}$ to MO-ROR-G$^{\mathbf{A}}_3$, there exists some $\mathbf{D}_2$ such that

$$\left|\Pr[\text{MO-ROR-G}^{\mathbf{A}}_4]-\Pr[\text{MO-RAND}^{\mathbf{A}}_{\mathsf{ECT}}=1]\right| \le \mathrm{Adv}^{\text{tprp}}_{\mathsf{TBC}}(\mathbf{D}_2)+q_\mathrm{e}^2/2^\ell.$$

$\mathbf{D}_2$ makes at most q_e queries to its oracle, and its run time is at most about that of MO-RAND$^{\mathbf{A}}_{\mathsf{ECT}}$, which is at most about that of MO-REAL$^{\mathbf{A}}_{\mathsf{ECT}}$.

B Proof of Theorem 4

The game RK-CTXT$^{\mathbf{A}}_{\mathsf{ECT}}$ is shown in Fig. 20. The game RK-CTXT-G$^{\mathbf{A}}_1$ in Fig. 21 records all the histories of E_K and D_K and uses them to answer to queries to $\mathbf{E}$, $\mathbf{D}$, and **ChalDec**. The game RK-CTXT-G$^{\mathbf{A}}_2$ in Fig. 22 uses a random tweakable permutation ϖ instead of TBC. In the game RK-CTXT-G$^{\mathbf{A}}_3$ shown in Fig. 22, $\mathbf{E}$ selects C_1 uniformly at random from Σ^ℓ, and $\mathbf{D}$ and **ChalDec** select L uniformly at random from Σ^ℓ. Thus, similar to the proof of Theorem 2, there exists some adversary $\mathbf{D}$ such that

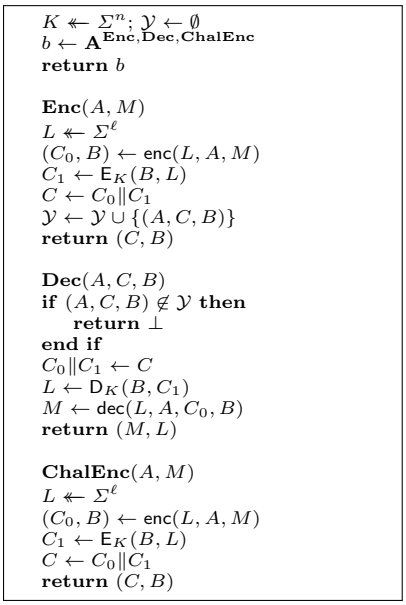
$$\mathrm{Adv}^{\text{rk-ctxt}}_{\mathsf{ECT}}(\mathbf{A}) \le \Pr[\text{RK-CTXT-G}^{\mathbf{A}}_3=\mathtt{true}]+\mathrm{Adv}^{\text{stprp}}_{\mathsf{TBC}}(\mathbf{D})+(q_\mathrm{e}+q_\mathrm{d}+q_\mathrm{c})^2/2^\ell.$$

$\mathbf{D}$ makes at most $q_\mathrm{e}+q_\mathrm{d}+q_\mathrm{c}$ queries to its oracles, and its run time is at most about that of RK-CTXT$^{\mathbf{A}}_{\mathsf{ECT}}$.

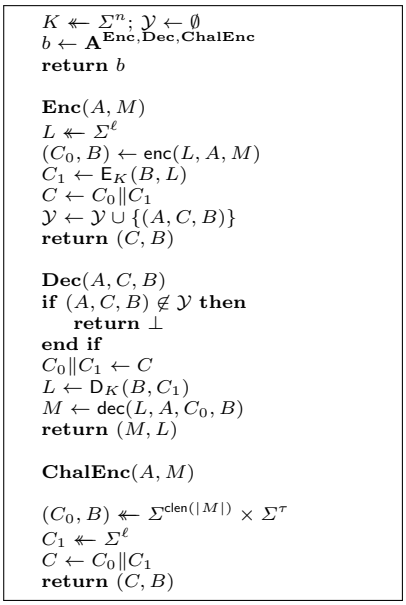
Now, $\Pr[\text{RK-CTXT-G}^{\mathbf{A}}_3=\mathtt{true}]$ is evaluated. Let $\mathcal{S}\subset\mathcal{A}\times\mathcal{C}\times\mathcal{T}$ be the sets of successful queries to **ChalDec** made by $\mathbf{A}$. Namely, their corresponding replies belong to $\mathcal{M}\times\mathcal{L}$. Let $\mathcal{P}$ be the sets of all (B,L,C_1)'s obtained by the queries to $\mathbf{E}$ made by $\mathbf{A}$.

Suppose that RK-CTXT-G$^{\mathbf{A}}_3$ outputs $\mathtt{true}$. Then, $|S|>|\mathcal{P}|$. Let Win_1 and Win_2 be the cases that

1. For any $(A,C,B)\in\mathcal{S}$, there exists some $(\tilde{B},\tilde{L},\tilde{C}_1)\in\mathcal{P}$ such that $(B,C_1)=(\tilde{B},\tilde{C}_1)$, where C_1 is the least significant ℓ bits of C, and



(a) MO-REAL$^{\mathbf{A}}_{\mathsf{ECT}}$



(b) MO-RAND$^{\mathbf{A}}_{\mathsf{ECT}}$

Fig. 15: Games for confidentiality of ECT

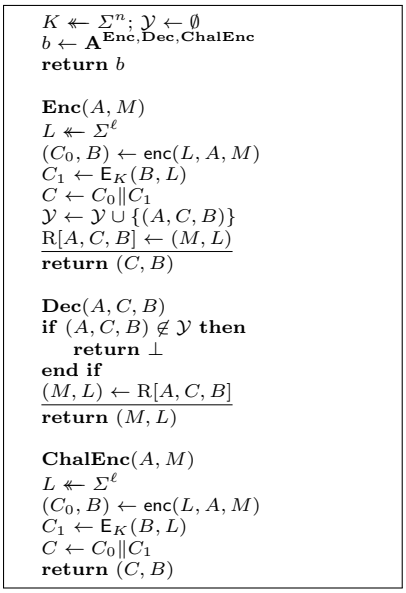


Fig. 16: MO-ROR-G$^{\mathbf{A}}_1$

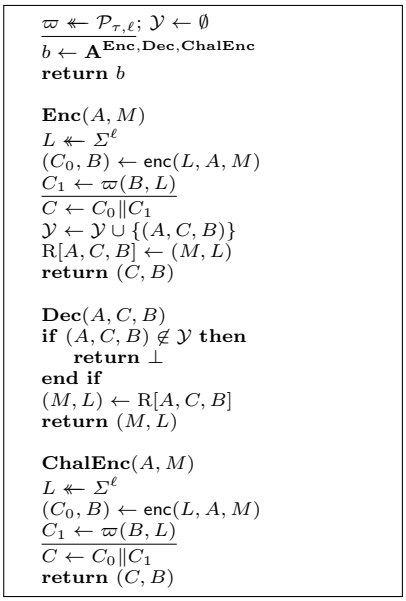


Fig. 17: MO-ROR-G$^{\mathbf{A}}_2$

$\mathcal{Y} \leftarrow \emptyset$
$b \leftarrow \mathbf{A}^{\mathbf{Enc},\mathbf{Dec},\mathbf{ChalEnc}}$
return b

Enc(A, M)
$L \twoheadleftarrow \Sigma^\ell$
$(C_0, B) \leftarrow \mathsf{enc}(L, A, M)$
$C_1 \twoheadleftarrow \Sigma^\ell$
$C \leftarrow C_0 \| C_1$
$\mathcal{Y} \leftarrow \mathcal{Y} \cup \{(A, C, B)\}$
$\mathrm{R}[A, C, B] \leftarrow (M, L)$
return (C, B)

Dec(A, C, B)
if $(A, C, B) \notin \mathcal{Y}$ **then**
  return $\perp$
end if
$(M, L) \leftarrow \mathrm{R}[A, C, B]$
return (M, L)

ChalEnc(A, M)
$L \twoheadleftarrow \Sigma^\ell$
$(C_0, B) \leftarrow \mathsf{enc}(L, A, M)$
$C_1 \twoheadleftarrow \Sigma^\ell$
$C \leftarrow C_0 \| C_1$
return (C, B)

Fig. 18: MO-ROR-$\mathrm{G}_3^{\mathbf{A}}$

$\mathcal{Y} \leftarrow \emptyset$
$b \leftarrow \mathbf{A}^{\mathbf{Enc},\mathbf{Dec},\mathbf{ChalEnc}}$
return b

Enc(A, M)
$L \twoheadleftarrow \Sigma^\ell$
$(C_0, B) \leftarrow \mathsf{enc}(L, A, M)$
$C_1 \twoheadleftarrow \Sigma^\ell$
$C \leftarrow C_0 \| C_1$
$\mathcal{Y} \leftarrow \mathcal{Y} \cup \{(A, C, B)\}$
$\mathrm{R}[A, C, B] \leftarrow (M, L)$
return (C, B)

Dec(A, C, B)
if $(A, C, B) \notin \mathcal{Y}$ **then**
  return $\perp$
end if
$(M, L) \leftarrow \mathrm{R}[A, C, B]$
return (M, L)

ChalEnc(A, M)

$(C_0, B) \twoheadleftarrow \Sigma^{\mathsf{clen}(|M|)} \times \Sigma^\tau$
$C_1 \twoheadleftarrow \Sigma^\ell$
$C \leftarrow C_0 \| C_1$
return (C, B)

Fig. 19: MO-ROR-$\mathrm{G}_4^{\mathbf{A}}$

2. otherwise,

respectively. Then,

$$\Pr[\text{RK-CTXT-G}_3^{\mathbf{A}} = \mathtt{true}] = \Pr[\mathrm{Win}_1] + \Pr[\mathrm{Win}_2].$$

For Win_1, since $|S| > |\mathcal{P}|$, there exist (A', C', B') and (A'', C'', B'') in $\mathcal{S}$ such that $(B', C_1') = (B'', C_1'')$ and $(A', C_0') \neq (A'', C_0'')$, where $C_0' \| C_1' = C'$ and $C_0'' \| C_1'' = C''$. Let $L' \leftarrow \mathsf{D}_K(B', C_1')$, $M' \leftarrow \mathsf{dec}(L', A', C_0', B')$, $L'' \leftarrow \mathsf{D}_K(B'', C_1'')$, and $M'' \leftarrow \mathsf{dec}(L'', A'', C_0'', B'')$. Then, $L' = L''$. Since EC is strongly correct, $\mathsf{enc}(L', A', M') = (C_0', B')$ and $\mathsf{enc}(L'', A'', M'') = (C_0'', B'')$. Thus, since EC is correct, $\mathsf{ver}(A', M', L', B') = 1$ and $\mathsf{ver}(A'', M'', L'', B'') = 1$. Suppose that $(L', A', M') = (L'', A'', M'')$. Then, $(C_0', B') = (C_0'', B'')$ since enc is determinisrtic, which contradicts $(A', C_0') \neq (A'', C_0'')$. Thus, $(A', M') \neq (A'', M'')$ since $L' = L''$. Consequently, there exists some adversary $\dot{\mathbf{A}}$ such that $\mathrm{Adv}^{\text{r-bind}}_{\mathsf{EC}}(\dot{\mathbf{A}}) = \Pr[\mathrm{Win}_1]$. $\dot{\mathbf{A}}$ simply runs RK-CTXT-$\mathrm{G}_3^{\mathbf{A}}$.

For Win_2, suppose that $(A^*, C^*, B^*) \in \mathcal{S}$ and that $(B^*, \tilde{L}, C_1^*) \notin \mathcal{P}$ for any $\tilde{L} \in \Sigma^\ell$, where C_1^* is the least significant ℓ bits of C^*. Then, the following adversary $\ddot{\mathbf{A}} = (\ddot{\mathbf{A}}_1, \ddot{\mathbf{A}}_2)$ against EC for targeted ciphertext unforgeability is successful. First, $\ddot{\mathbf{A}}_1$ executes RK-CTXT-$\mathrm{G}_3^{\mathbf{A}}$ and guesses (B^*, C_1^*) in the queries to $\mathbf{D}$ or $\mathbf{ChalDec}$. It interrupts the execution of RK-CTXT-$\mathrm{G}_3^{\mathbf{A}}$ right after it finds (B^*, C_1^*). Then, $\ddot{\mathbf{A}}_2$ gets $\ddot{L} \twoheadleftarrow \Sigma^\ell$ and resumes the execution of RK-CTXT-$\mathrm{G}_3^{\mathbf{A}}$. Finally, $\ddot{\mathbf{A}}_2$ outputs (A^*, C_0^*) satisfying $\mathsf{dec}(\ddot{L}, A^*, C_0^*, B^*) \neq \perp$, where $C^* = C_0^* \| C_1^*$. Thus, $\mathrm{Adv}^{\text{tcu}}_{\mathsf{EC}}(\ddot{\mathbf{A}}) = \Pr[\mathrm{Win}_2]/(q_\mathrm{d} + q_\mathrm{c})$.

$K \twoheadleftarrow \Sigma^n$
$win \leftarrow \texttt{false}$; $ctr \leftarrow 0$
$\mathbf{A}^{\mathbf{E},\mathbf{D},\mathbf{ChalDec}}$
if $ctr < 0$ **then**
  $win \leftarrow \texttt{true}$
end if
return win

$\mathbf{E}(B, L)$
$ctr \leftarrow ctr + 1$
$C_1 \leftarrow \mathsf{E}_K(B, L)$
return C_1

$\mathbf{D}(B, C_1)$
$L \leftarrow \mathsf{D}_K(B, C_1)$
return L

$\mathbf{ChalDec}(A, C, B)$
$C_0 \| C_1 \leftarrow C$
$L \leftarrow \mathsf{D}_K(B, C_1)$
if $\mathsf{dec}(L, A, C_0, B) \neq \perp$ **then**
  $ctr \leftarrow ctr - 1$
  $M \leftarrow \mathsf{dec}(L, A, C_0, B)$
  return (M, L)
else
  return $\perp$
end if

Fig. 20: Game RK-CTXT$^{\mathbf{A}}_{\mathsf{ECT}}$

$K \twoheadleftarrow \Sigma^n$; $\mathcal{Z} \leftarrow \emptyset$
$win \leftarrow \texttt{false}$; $ctr \leftarrow 0$
$\mathbf{A}^{\mathbf{E},\mathbf{D},\mathbf{ChalDec}}$
if $ctr < 0$ **then**
  $win \leftarrow \texttt{true}$
end if
return win

$\mathbf{E}(B, L)$
$ctr \leftarrow ctr + 1$
if $(B, L, \tilde{C}_1) \in \mathcal{Z}$ **then**
  $C_1 \leftarrow \tilde{C}_1$
else
  $C_1 \leftarrow \mathsf{E}_K(B, L)$
  $\underline{\mathcal{Z} \leftarrow \mathcal{Z} \cup \{(B, L, C_1)\}}$
end if
return C_1

$\mathbf{D}(B, C_1)$
if $(B, \tilde{L}, C_1) \in \mathcal{Z}$ **then**
  $L \leftarrow \tilde{L}$
else
  $L \leftarrow \mathsf{D}_K(B, C_1)$
  $\underline{\mathcal{Z} \leftarrow \mathcal{Z} \cup \{(B, L, C_1)\}}$
end if
return L

$\mathbf{ChalDec}(A, C, B)$
$C_0 \| C_1 \leftarrow C$
if $(B, \tilde{L}, C_1) \in \mathcal{Z}$ **then**
  $L \leftarrow \tilde{L}$
else
  $L \leftarrow \mathsf{D}_K(B, C_1)$
  $\underline{\mathcal{Z} \leftarrow \mathcal{Z} \cup \{(B, L, C_1)\}}$
end if
if $\mathsf{dec}(L, A, C_0, B) \neq \perp$ **then**
  $ctr \leftarrow ctr - 1$
  $M \leftarrow \mathsf{dec}(L, A, C_0, B)$
  return (M, L)
else
  return $\perp$
end if

Fig. 21: RK-CTXT-G$^{\mathbf{A}}_1$

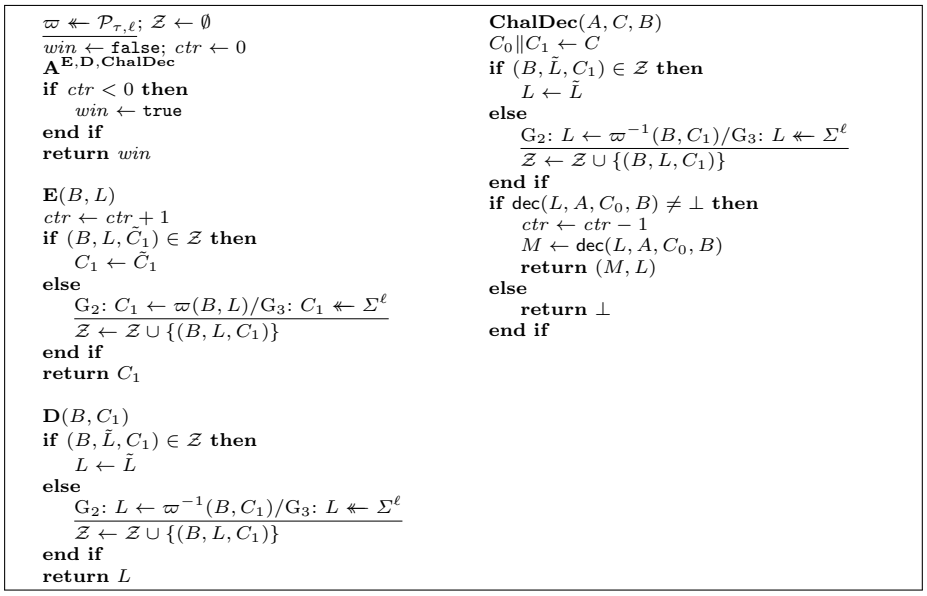


Fig. 22: RK-CTXT-$\mathrm{G}_2^{\mathbf{A}}$ and RK-CTXT-$\mathrm{G}_3^{\mathbf{A}}$

C HFC and Its Security for New Security Notions

The HFC encryptment scheme [15] $\mathsf{HFC} := (\mathsf{Hkg}, \mathsf{Henc}, \mathsf{Hdec}, \mathsf{Hver})$ uses a compression function $\mathsf{f} : \Sigma^\tau \times \Sigma^\ell \to \Sigma^\tau$, where τ and ℓ satisfies $\ell \geq \tau \geq 128$. The key space is Σ^ℓ, and the binding-tag space is Σ^τ. To simplify the description, it is assumed that the associated-data space is $\bigcup_{i>0} \Sigma^{\ell i}$ and the message and ciphertext spaces are $\bigcup_{i>0} \Sigma^{\tau i}$. Let $\mathtt{parse}_w$ be a function which takes $X \in \bigcup_{i>0} \Sigma^{wi}$ as input and outputs $X_1, X_2, \ldots, X_x$ such that $X = X_1 \| X_2 \| \cdots \| X_x$ and $|X_i| = w$ for $1 \leq i \leq x$.

The key generation algorithm Hkg simply selects K_{ec} uniformly at random from Σ^ℓ. The encryptment algorithm Henc and the decryptment algorithm Hdec are described in Fig. 23. The description of the verification algorithm Hver is omitted since it is apparent from Hdec.

HFC satisfies targeted ciphertext unforgeability if the underlying compression function f is a random oracle:

Theorem 5. *Suppose that* f *is a random oracle. Then, for any adversary* $\mathbf{A} := (\mathbf{A}_1, \mathbf{A}_2)$ *against* HFC *concerning targeted ciphertext unforgeability such that* $\mathbf{A}_1$ *and* $\mathbf{A}_2$ *make at most* q_1 *and* q_2 *queries to* f*, respectively,*

$$\mathrm{Adv}^{\mathrm{tcu}}_{\mathsf{HFC}}(\mathbf{A}) \leq (q_1 + 1)q_2/2^\tau + q_1/2^\ell.$$

Proof. Suppose that $\mathbf{A}_2$ takes $(B, state)$ and K_{ec} as input and outputs (A, C), where $(B, state)$ is the output of $\mathbf{A}_1$ and $K_{\mathrm{ec}} \twoheadleftarrow \Sigma^\ell$. Suppose that, for $1 \leq j_1 \leq q_1$, $\mathbf{A}_1$ receives $Z_{1,j_1} \in \Sigma^\tau$ from f as a response to a query $(Y_{1,j_1}, W_{1,j_1}) \in$

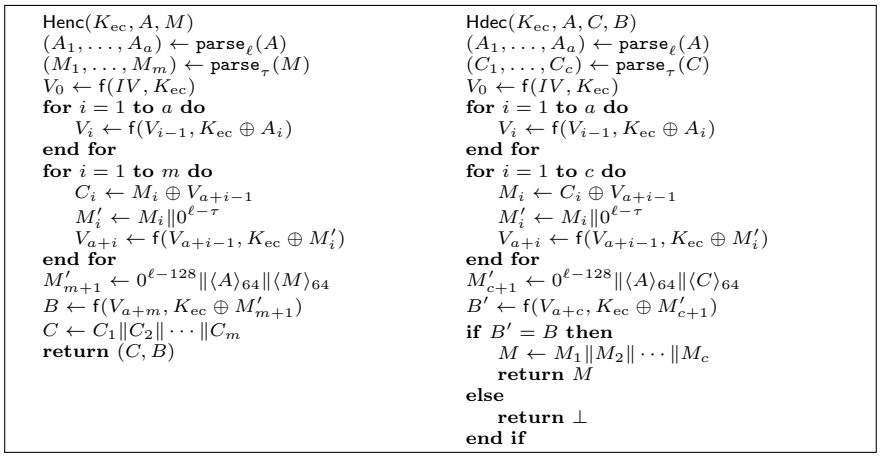


Fig. 23: Henc and Hdec. $IV \in \Sigma^\tau$ is a fixed initial vector. $\langle X \rangle_{64}$ denotes the 64-bit binary representation of $|X|$ for $X \in \Sigma^*$.

$\Sigma^\tau \times \Sigma^\ell$. Suppose that, for $1 \leq j_2 \leq q_2$, $\mathbf{A}_2$ receives $Z_{2,j_2} \in \Sigma^\tau$ from f as a response to a query $(Y_{2,j_2}, W_{2,j_2}) \in \Sigma^\tau \times \Sigma^\ell$. Without loss of generality, it is assumed that all the queries made by $\mathbf{A}_1$ and $\mathbf{A}_2$ to f are distinct from each other and sufficient to compute $\mathsf{Hdec}(K_{\mathrm{ec}}, A, C, B)$.

Let $\mathtt{Col}_{\mathrm{K}}$ be the event that there exists some j_1^* such that $K_{\mathrm{ec}} = W_{1,j_1^*}$. Then,

$$\begin{aligned}\mathrm{Adv}^{\mathrm{tcu}}_{\mathsf{HFC}}(\mathbf{A}) &\leq \Pr[\mathsf{Hdec}(K_{\mathrm{ec}}, A, C, B) \neq \perp] \\ &\leq \Pr[\mathtt{Col}_{\mathrm{K}}] + \Pr[\mathsf{Hdec}(K_{\mathrm{ec}}, A, C, B) \neq \perp \mid \overline{\mathtt{Col}_{\mathrm{K}}}],\end{aligned}$$

and $\Pr[\mathtt{Col}_{\mathrm{K}}] \leq q_1/2^\ell$. Suppose that $\mathtt{Col}_{\mathrm{K}}$ does not happen. Then, to satisfy $\mathsf{Hdec}(K_{\mathrm{ec}}, A, C, B) \neq \perp$, it is necessary that there exists some j_2^* such that $Z_{2,j_2^*} = B$ or $Z_{2,j_2^*} = Z_{1,j_1}$ for some j_1. Thus,

$$\Pr[\mathsf{Hdec}(K_{\mathrm{ec}}, A, C, B) \neq \perp \mid \overline{\mathtt{Col}_{\mathrm{K}}}] \leq (q_1 + 1)q_2/2^\tau.$$

□

HFC satisfies confidentiality with attachment if the underlying compression function f is a random oracle:

Theorem 6. *Suppose that* f *is a random oracle. Let* $\mathbf{A}$ *be any adversary against* HFC *concerning confidentiality with attachment. Suppose that* $\mathbf{A}$ *makes at most* q_{t} *and* q_{f} *queries to* (ϖ, ϖ^{-1}) *and* f*, respectively. Suppose that a query to* **enc** *made by* $\mathbf{A}$ *induces* σ *calls to* f*. Then,*

$$\widetilde{\mathrm{Adv}}^{\text{ot-ror}}_{\mathsf{HFC}}(\mathbf{A}) \leq q_{\mathrm{f}}/2^\ell + \sigma(\sigma+1)/2^{\ell+1} + (q_{\mathrm{f}} + q_{\mathrm{t}})/(2^\ell - q_{\mathrm{f}} - q_{\mathrm{t}}).$$

Proof. $\mathbf{A}$ is given f as an oracle in addition to **enc** and (ϖ, ϖ^{-1}). Let $\mathcal{Q}_1^{\mathbf{A}}$ and $\mathcal{Q}_2^{\mathbf{A}}$ be the set of queries to f made by $\mathbf{A}$ before and after the query to **enc**, respectively, where $\mathcal{Q}_i^{\mathbf{A}} \subseteq \Sigma^\tau \times \Sigma^\ell$ for $i \in \{1, 2\}$. Let $\mathcal{Q}^{\mathsf{Henc}} \subseteq \Sigma^\tau \times \Sigma^\ell$ be the set of queries to f made by Henc for the query to **enc**. Let us first specify the following events in $\widetilde{\mathrm{otREAL}}^{\mathbf{A}}_{\mathsf{HFC}}$:

- $\mathtt{Dup}_i$ is the event that $\mathcal{Q}_i^{\mathbf{A}} \cap \mathcal{Q}^{\mathsf{Henc}} \neq \emptyset$ for $i \in \{1, 2\}$;
- $\mathtt{Col}$ is the event that there exists some $X \in \mathcal{Q}^{\mathsf{Henc}}$ such that $\mathsf{f}(X) = IV$ or $\mathsf{f}(X) = \mathsf{f}(X')$ for some $X' \in \mathcal{Q}^{\mathsf{Henc}}$ such that $X \neq X'$;
- $\mathtt{Hit}$ is the event that $\mathbf{A}$ asks (B, K_{ec}) to ϖ.

Notice that Henc asks each query in $\mathcal{Q}^{\mathsf{Henc}}$ only once if $\mathtt{Col}$ does not happen. $\widetilde{\mathrm{otREAL}}^{\mathbf{A}}_{\mathsf{HFC}}$ is equivalent to $\widetilde{\mathrm{otRAND}}^{\mathbf{A}}_{\mathsf{HFC}}$ as long as $\overline{\mathtt{Dup}_1}$, $\overline{\mathtt{Col}}$, $\overline{\mathtt{Dup}_2}$, and $\overline{\mathtt{Hit}}$ in $\widetilde{\mathrm{otREAL}}^{\mathbf{A}}_{\mathsf{HFC}}$. Thus,

$$\begin{aligned}
\widetilde{\mathrm{Adv}}^{\text{ot-ror}}_{\mathsf{EC}}(\mathbf{A}) &= \left|\Pr[\widetilde{\mathrm{otREAL}}^{\mathbf{A}}_{\mathsf{EC}} = 1] - \Pr[\widetilde{\mathrm{otRAND}}^{\mathbf{A}}_{\mathsf{EC}} = 1]\right| \\
&\leq \Pr[\mathtt{Dup}_1 \vee \mathtt{Col} \vee \mathtt{Dup}_2 \vee \mathtt{Hit}] \\
&\leq \Pr[\mathtt{Dup}_1] + \Pr[\mathtt{Col}] + \Pr[\mathtt{Dup}_2 \vee \mathtt{Hit} \,|\, \overline{\mathtt{Dup}_1} \wedge \overline{\mathtt{Col}}\,].
\end{aligned}$$

Without loss of generality, K_{ec} is assumed to be chosen right after the query to **enc** made by $\mathbf{A}$. Thus, $\Pr[\mathtt{Dup}_1] \leq q_{\mathrm{f}}/2^\ell$. It is easy to see $\Pr[\mathtt{Col}] \leq \sigma(\sigma + 1)/2^{\ell+1}$.

If $\overline{\mathtt{Dup}_1} \wedge \overline{\mathtt{Col}}$ happens, then a query to f made by $\mathbf{A}$ reduces at most one candidate for K_{ec} as long as $\mathtt{Dup}_2$ does not happen. As long as $\mathtt{Hit}$ does not happen, a query to (ϖ, ϖ^{-1}) made by $\mathbf{A}$ also reduces at most one candidates for K_{ec}. Thus, $\Pr[\mathtt{Dup}_2 \vee \mathtt{Hit} \,|\, \overline{\mathtt{Dup}_1} \wedge \overline{\mathtt{Col}}\,] \leq (q_{\mathrm{f}} + q_{\mathrm{t}})/(2^\ell - q_{\mathrm{f}} - q_{\mathrm{t}})$. □

D Proof of Proposition 1

Let $\dot{\mathbf{A}}$ be an adversary against EC for receiver binding. $\dot{\mathbf{A}}$ runs $\mathbf{A}$. For a query (A, M) made by $\mathbf{A}$ to enc, $\dot{\mathbf{A}}$ executes $K_{\mathrm{ec}} \leftarrow \mathsf{kg}$ and $(C, B) \leftarrow \mathsf{enc}_{K_{\mathrm{ec}}}(A, M)$. After receiving K_{ec} and (C, B) from $\dot{\mathbf{A}}$, $\mathbf{A}$ outputs (A', C'). Finally, $\dot{\mathbf{A}}$ outputs $((K_{\mathrm{ec}}, A, M), (K_{\mathrm{ec}}, A', M'), B)$, where M' is chosen at random if $\mathsf{dec}_{K_{\mathrm{ec}}}(A', C', B) = \perp$ and $M' \leftarrow \mathsf{dec}_{K_{\mathrm{ec}}}(A', C', B)$ otherwise.

Since EC is correct, $\mathsf{ver}(A, M, K_{\mathrm{ec}}, B) = 1$. It is shown in the remaining parts that, if $(A, C) \neq (A', C')$ and $\mathsf{dec}_{K_{\mathrm{ec}}}(A', C', B) = M' \neq \perp$, then $(A, M) \neq (A', M')$ and $\mathsf{ver}(A', M', K_{\mathrm{ec}}, B) = 1$.

Suppose that $\mathsf{dec}_{K_{\mathrm{ec}}}(A', C', B) \neq \perp$. Then, $\mathsf{enc}_{K_{\mathrm{ec}}}(A', M') = (C', B)$ since EC is strongly correct. Thus, $\mathsf{ver}(A', M', K_{\mathrm{ec}}, B) = 1$ since EC is correct. In addition, suppose that $(A, C) \neq (A', C')$. If $A \neq A'$, then $(A, M) \neq (A', M')$. If $A = A'$, then $C \neq C'$. Suppose that $M = M'$. Then, it contradicts with $C \neq C'$ since $\mathsf{enc}_{K_{\mathrm{ec}}}(A, M) = (C, B)$, $\mathsf{enc}_{K_{\mathrm{ec}}}(A', M') = (C', B)$ and enc is a deterministic algorithm.