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, Tokyo, Japan
k-minematsu@nec.com
[3] Yokohama National University, Kanagawa, Japan

Abstract. Facebook introduced message franking to enable users to report abusive content verifiably in end-to-end encrypted messaging. Grubbs et al. formalized the underlying primitive called compactly committing authenticated encryption with associated data (ccAEAD) and presented schemes with provable security. Dodis et al. proposed a core building block called encryptment and presented a generic construction of ccAEAD with encryptment and standard AEAD. This paper first proposes to use a tweakable block cipher instead of AEAD for the generic construction of Dodis et al. In the security analysis of the proposed construction, its ciphertext integrity is shown to require a new but feasible assumption on the ciphertext integrity of encryptment. Then, this paper formalizes remotely keyed ccAEAD (RK ccAEAD) and shows that the proposed construction works as RK ccAEAD. Finally, the confidentiality of the proposed construction as RK ccAEAD is shown to require a new variant of confidentiality for encryptment. The problem of remotely keyed encryption was posed by Blaze in 1996. It is now related to the problem of designing a cryptographic scheme using a trusted module and/or with leakage resiliency.

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 [14], Signal [31], and Whatsapp Messenger [33]. 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 content. To achieve this goal, Facebook introduced message franking [15]. It is a cryptographic protocol allowing users to report the receipt of abusive messages verifiably to Facebook.

Grubbs et al. [17] initiated the formal study of message franking and presented a new variant of AEAD called compactly committing AEAD (ccAEAD) as its underlying primitive. For ccAEAD, a small part of the ciphertext works as a commitment to the message and associated data. Dodis et al. [12] presented a core component of ccAEAD named encryptment and two transformations to ccAEAD from encryptment. One transformation uses AEAD, and the other is nonce-based and uses a PRF twice. In addition, Dodis et al. posed it as an open question to define and construct remotely keyed ccAEAD schemes in the full version [13] of [12].

Contribution. This work is inspired mainly by the work of Dodis et al. [12, 13]. First, the transformation to ccAEAD from encryptment using AEAD described above is modified: It is shown that AEAD can be replaced by a tweakable block cipher (TBC). The new generic construction is named ECT (EnCryptment-then-TBC). The security requirements of ECT are reduced to those of the underlying encryptment scheme and TBC with the use of the code-based game-playing proof technique [4]. The ciphertext integrity of ECT requires a new but feasible type of ciphertext unforgeability for encryptment. Actually, it is shown that the HFC (Hash-Function-Chaining) encryptment scheme [12] satisfies the new type of ciphertext unforgeability in the random oracle model.

Second, an answer is given to the open question mentioned above: Remotely keyed (RK) ccAEAD is formalized and it is confirmed that ECT works as secure RK ccAEAD. The formalization is based on that of RK authenticated encryption by Dodis and An [11]. The confidentiality of ECT as RK ccAEAD requires a new but viable variant of confidentiality for encryptment. The problem of remotely keyed encryption [6] is now related to the problem of designing a cryptographic scheme using a trusted module and/or with leakage resiliency. Notice that ECT has a similar structure with the AEAD scheme named CONCRETE [5], which offers ciphertext integrity in the presence of nonce misuse and leakage.

Related Work. Authenticated encryption is a topic attracting much interest in symmetric cryptography. The first formal treatments of authenticated encryption were conducted by Katz and Yung [23] and by Bellare and Namprempre [3].

Grubbs et al. [17] 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.

Dodis et al. [12] constructed the HFC encryptment scheme based on a Merkle-Damgård hash function [10, 30]. They also showed an attack on the Facebook message franking protocol: A malicious sender can send an abusive message, and the receiver cannot report it verifiably.

Message franking schemes enabling receivers to report an abusive message by revealing only the abusive parts were investigated independently by Leontiadis and Vaudenay [25] and by Chen and Tang [9]. Huguenin-Dumittan and Leontiadis formalized and instantiated a secure bidirectional channel with message franking [20]. Yamamuro et al. [34] 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. [32] formalized asymmetric message franking and constructed a scheme from signatures of knowledge [19] for designated verifier signatures [21].

Liskov et al. proposed and investigated TBCs [26, 27]. Hirose [18] instantiated the generic construction of nonce-based ccAEAD using encryptment and a PRF by Dodis et al. [12] only with a TBC.

Blaze [6] posed a problem of remotely keyed encryption, which inspired Lucks [28, 29], Blaze et al. [7], and Jakobsson et al. [22]. Dodis and An [11] 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.

Committing authenticated encryption was discussed by Farshim et al. [16], Albertini et al. [1], Len et al. [24], Bellare and Hoang [2], and Chan and Rogaway [8]. Their primary goal was to decrease the risk of error or misuse by application designers, and message franking was out of scope.

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. All the proofs of theorems are given as 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 $\mathcal{P}_{n_\mathrm{t}, n_\mathrm{b}}$ and outputs 0 or

1. The advantage of $\mathbf{A}$ against TBC for a tweakable pseudorandom permutation (TPRP) is

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

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

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

2.2 ccAEAD

Syntax. ccAEAD [17] 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 takes as input 1^n, where n is a security parameter, and returns a secret key $K \in \mathcal{K}$.
- 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. 1 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

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

$\mathbf{A}$ 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**.

```
$K \leftarrow \mathsf{Kg}(1^n)$; $\mathcal{Y} \leftarrow \emptyset$
$b \leftarrow \mathbf{A}^{\mathbf{Enc},\mathbf{Dec},\mathbf{ChalEnc}}$
return $b$

Enc$(A, M)$
$(C, B) \leftarrow \mathsf{Enc}(K, A, M)$
$\mathcal{Y} \leftarrow \mathcal{Y} \cup \{(A, C, B)\}$
return $(C, B)$

Dec$(A, C, B)$
if $(A, C, B) \notin \mathcal{Y}$ then
    return $\perp$
end if
$(M, L) \leftarrow \mathsf{Dec}(K, A, C, B)$
return $(M, L)$

ChalEnc$(A, M)$
$(C, B) \leftarrow \mathsf{Enc}(K, A, M)$
return $(C, B)$
```

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

```
$K \leftarrow \mathsf{Kg}(1^n)$; $\mathcal{Y} \leftarrow \emptyset$
$b \leftarrow \mathbf{A}^{\mathbf{Enc},\mathbf{Dec},\mathbf{ChalEnc}}$
return $b$

Enc$(A, M)$
$(C, B) \leftarrow \mathsf{Enc}(K, A, M)$
$\mathcal{Y} \leftarrow \mathcal{Y} \cup \{(A, C, B)\}$
return $(C, B)$

Dec$(A, C, B)$
if $(A, C, B) \notin \mathcal{Y}$ then
    return $\perp$
end if
$(M, L) \leftarrow \mathsf{Dec}(K, A, C, B)$
return $(M, L)$

ChalEnc$(A, M)$
$(C, B) \twoheadleftarrow \Sigma^{\mathsf{clen}(|M|)} \times \Sigma^{\tau}$
return $(C, B)$
```

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

Fig. 1: Games for confidentiality of ccAEAD

Ciphertext Integrity. The game MO-CTXT shown in Fig. 2 is introduced to formalize the ciphertext integrity as unforgeability in the multi-opening setting. The advantage of an adversary **A** for ciphertext integrity is

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

A is allowed to make queries adaptively to the oracles **Enc**, **Dec**, and **ChalDec**. The game outputs `true` if **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 **A** for receiver binding is

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

The advantage of **A** for strong receiver binding is

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

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

```
$K \leftarrow \mathsf{Kg}(1^n)$; $\mathcal{Y} \leftarrow \emptyset$
$win \leftarrow$ false
$\mathbf{A}^{\mathbf{Enc},\mathbf{Dec},\mathbf{ChalDec}}$
return $win$

Enc$(A, M)$
$(C, B) \leftarrow \mathsf{Enc}(K, A, M)$
$\mathcal{Y} \leftarrow \mathcal{Y} \cup \{(A, C, B)\}$
return $(C, B)$

Dec$(A, C, B)$
return $\mathsf{Dec}(K, A, C, B)$

ChalDec$(A, C, B)$
if $(A, C, B) \in \mathcal{Y}$ then
    return $\perp$
end if
if $\mathsf{Dec}(K, A, C, B) \neq \perp$ then
    $win \leftarrow$ true
end if
return $\mathsf{Dec}(K, A, C, B)$
```

Fig. 2: Game MO-CTXT$^{\mathbf{A}}_{\mathsf{CAE}}$ for ciphertext integrity of ccAEAD

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

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

2.3 Encryptment

Syntax. Encryptment [12] 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 takes as input 1^{ℓ}, where ℓ is a security parameter, and returns a secret key $K_{\mathrm{ec}} \in \mathcal{K}_{\mathrm{ec}}$.
- 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 $\perp \notin \mathcal{M}$.
- 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. 3 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."

```
$K_{\mathrm{ec}} \leftarrow \mathsf{kg}(1^n)$
$b \leftarrow \mathbf{A}^{\mathbf{enc}}$
return $b$

enc$(A, M)$
$(C, B) \leftarrow \mathsf{enc}(K_{\mathrm{ec}}, A, M)$
return $(C, B)$
```

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

```
$b \leftarrow \mathbf{A}^{\mathbf{enc}}$
return $b$

enc$(A, M)$
$(C, B) \twoheadleftarrow \Sigma^{\mathsf{clen}(|M|)} \times \Sigma^{\tau}$
return $(C, B)$
```

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

Fig. 3: 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 $K_{\mathrm{ec}} \leftarrow \mathsf{kg}(1^n)$ 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

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

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

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

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

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

For strongly correct encryptment, Dodis et al. [12] 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 $\mathrm{Adv}^{\mathrm{scu}}_{\mathsf{EC}}(\mathbf{A}) \le \mathrm{Adv}^{\mathrm{r\text{-}bind}}_{\mathsf{EC}}(\dot{\mathbf{A}})$ and the run time of $\dot{\mathbf{A}}$ is at most about that of $\mathbf{A}$.*

Proof. Shown in Appendix F.

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. 4. They are also depicted in Appendix G. KG selects a secret key K for TBC from Σ^n. VER simply runs ver.

```
ENC($K, A, M$)
$L \leftarrow \mathsf{kg}(1^\ell)$
$(C_0, B) \leftarrow \mathsf{enc}(L, A, M)$
$C_1 \leftarrow \mathsf{E}_K(B, L)$
$C \leftarrow C_0 \| C_1$
return $(C, B)$

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

Fig. 4: The encryption and decryption algorithms of ECT

3.2 Security

For security analyses, it is assumed that KG and kg simply output $K \twoheadleftarrow \Sigma^n$ and $L \twoheadleftarrow \Sigma^\ell$, respectively.

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*

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

The run time of $\dot{\mathbf{A}}$ *and* $\mathbf{D}$ *is at most about that of* $\text{MO-REAL}_{\mathsf{ECT}}^{\mathbf{A}}$*.* $\mathbf{D}$ *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* $K_{\mathrm{ec}} \leftarrow \mathsf{kg}(1^{\ell})$*, and outputs* $(A, C) \in \mathcal{A} \times \mathcal{C}$*. The advantage of* $\mathbf{A}$ *for targeted ciphertext unforgeability is*

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

It is not difficult to see that the HFC encryptment scheme [12] satisfies targeted ciphertext unforgeability in the random oracle model, which is shown in Appendix E.

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*

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

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

Proof. Shown in Appendix B. □

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

ECT also inherits sender binding from EC. Suppose that (K, A, C, B) satisfies $\mathsf{DEC}(K, A, C, B) \ne \bot$ 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 $M \ne \bot$, 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.

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 takes as input 1^n, where n is a security parameter, and returns a secret key $K \in \mathcal{K}$.
- 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. 5 are introduced. An adversary **A** is given access to oracles **E**, **D** and **ChalEnc**. **A** is not allowed to decrypt (A, C, B) obtained by asking (A, M) to **ChalEnc**. The advantage of **A** for confidentiality is

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

```
$K \leftarrow \mathsf{RKKg}(1^n)$; $\mathcal{Y} \leftarrow \emptyset$
$b \leftarrow \mathbf{A}^{\mathbf{E},\mathbf{D},\mathbf{ChalEnc}}$
return $b$

$\mathbf{E}(Q_\mathrm{e})$
$R_\mathrm{e} \leftarrow \mathsf{TE}_K(Q_\mathrm{e})$
return $R_\mathrm{e}$

$\mathbf{D}(Q_\mathrm{d})$
if $Q_\mathrm{d} \in \mathcal{Y}$ then
    return $\perp$
end if
$R_\mathrm{d} \leftarrow \mathsf{TD}_K(Q_\mathrm{d})$
return $R_\mathrm{d}$

$\mathbf{ChalEnc}(A, M)$
$(C, B) \leftarrow \mathsf{RKEnc}(K, A, M)$
$(Q_\mathrm{d}, S_\mathrm{d}) \leftarrow \mathsf{Pre\text{-}TD}(A, C, B)$
$\mathcal{Y} \leftarrow \mathcal{Y} \cup \{Q_\mathrm{d}\}$
return $(C, B)$
```

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

```
$K \leftarrow \mathsf{RKKg}(1^n)$; $\mathcal{Y} \leftarrow \emptyset$
$b \leftarrow \mathbf{A}^{\mathbf{E},\mathbf{D},\mathbf{ChalEnc}}$
return $b$

$\mathbf{E}(Q_\mathrm{e})$
$R_\mathrm{e} \leftarrow \mathsf{TE}_K(Q_\mathrm{e})$
return $R_\mathrm{e}$

$\mathbf{D}(Q_\mathrm{d})$
if $Q_\mathrm{d} \in \mathcal{Y}$ then
    return $\perp$
end if
$R_\mathrm{d} \leftarrow \mathsf{TD}_K(Q_\mathrm{d})$
return $R_\mathrm{d}$

$\mathbf{ChalEnc}(A, M)$
$(C, B) \twoheadleftarrow \Sigma^{\mathsf{clen}(|M|)} \times \Sigma^{\tau}$
$(Q_\mathrm{d}, S_\mathrm{d}) \leftarrow \mathsf{Pre\text{-}TD}(A, C, B)$
$\mathcal{Y} \leftarrow \mathcal{Y} \cup \{Q_\mathrm{d}\}$
return $(C, B)$
```

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

Fig. 5: Games for confidentiality of RK ccAEAD

Ciphertext Integrity. The game RK-CTXT$^{\mathbf{A}}_{\mathsf{RKCAE}}$ shown in Fig. 6 is introduced. An adversary **A** is given access to oracles **E**, **D** and **ChalDec**. **A** is not allowed to repeat the same queries to **ChalDec**. The game outputs `true` if the number of valid ciphertexts produced by **A** is greater than the number of queries to **E** made by **A**. The advantage of **A** for ciphertext integrity is

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

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.

```
$K \leftarrow \mathsf{RKKg}(1^n)$
$win \leftarrow$ false; $ctr \leftarrow 0$
$\mathbf{A}^{\mathbf{E},\mathbf{D},\mathbf{ChalDec}}$
if $ctr < 0$ then
    $win \leftarrow$ true
end if
return $win$

$\mathbf{E}(Q_{\mathrm{e}})$
$ctr \leftarrow ctr + 1$
return $\mathsf{TE}_K(Q_{\mathrm{e}})$

$\mathbf{D}(Q_{\mathrm{d}})$
return $\mathsf{TD}_K(Q_{\mathrm{d}})$

$\mathbf{ChalDec}(A, C, B)$
if $\mathsf{RKDec}(K, A, C, B) \neq \perp$ then
    $ctr \leftarrow ctr - 1$
end if
return $\mathsf{RKDec}(K, A, C, B)$
```

Fig. 6: Game $\text{RK-CTXT}^{\mathbf{A}}_{\mathsf{RKCAE}}$ for ciphertext integrity of RK ccAEAD

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 crutial difference of RK ECT from 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. 7 are introduced to formalize the 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*

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

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*

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

```
$K_{\mathrm{ec}} \leftarrow \mathsf{kg}(1^\ell)$; $\varpi \twoheadleftarrow \mathcal{P}_{\tau,\ell}$
$b \leftarrow \mathbf{A}^{\mathbf{enc},(\varpi,\varpi^{-1})}$
return $b$

$\mathbf{enc}(A, M)$
$(C, B) \leftarrow \mathsf{enc}(K_{\mathrm{ec}}, A, M)$
$C' \leftarrow \varpi(B, K_{\mathrm{ec}})$
return $(C, B, C')$
```

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

```
$K_{\mathrm{ec}} \leftarrow \mathsf{kg}(1^\ell)$; $\varpi \twoheadleftarrow \mathcal{P}_{\tau,\ell}$
$b \leftarrow \mathbf{A}^{\mathbf{enc},(\varpi,\varpi^{-1})}$
return $b$

$\mathbf{enc}(A, M)$
$(C, B) \twoheadleftarrow \Sigma^{\mathsf{clen}(|M|)} \times \Sigma^{\tau}$
$C' \leftarrow \varpi(B, K_{\mathrm{ec}})$
return $(C, B, C')$
```

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

Fig. 7: The games for confidentiality of encryptment

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 ideal TBC* (ϖ, ϖ^{-1}). $\mathbf{D}$ *makes at most* $q_{\mathrm{e}}+q_{\mathrm{d}}+q_{\mathrm{c}}$ *queries to its oracle.*

Proof. Shown in Appendix C. □

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* **E**, **D**, *and* **ChalDec**, *respectively. Then, there exist adversaries* $\dot{\mathbf{A}}$, $\ddot{\mathbf{A}}$, *and* $\mathbf{D}$ *such that*

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

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 D. □

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.

Acknowledgements. The authors thank Akiko Inoue for fruitful discussions. The first author was supported by JSPS KAKENHI Grant Number JP18H05289 and 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. IACR Cryptology ePrint Archive p. 1456 (2020), https://eprint.iacr.org/2020/1456
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. 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
6. 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
7. 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
8. 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
9. 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
10. 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
11. 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
12. 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
13. 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
14. Facebook: Facebook messenger. https://www.messenger.com, accessed on 09/10/2022

15. Facebook: Messenger secret conversations. Technical Whitepaper (2016), https://fbnewsroomus.files.wordpress.com/2016/07/messenger-secret-conversations-technical-whitepaper.pdf
16. 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
17. 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
18. 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
19. 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
20. 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
21. 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
22. 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
23. 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)
24. 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
25. Leontiadis, I., Vaudenay, S.: Private message franking with after opening privacy. Cryptology ePrint Archive, Report 2018/938 (2018), https://eprint.iacr.org/2018/938
26. 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
27. 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
28. 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,
29. 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

30. 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
31. Signal Foundation: Signal. `https://signal.org/`, accessed on 09/10/2022
32. 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
33. WhatsApp: WhatsApp Messenger. `https://www.whatsapp.com`, accessed on 09/10/2022
34. 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 $\text{MO-REAL}_{\mathsf{ECT}}^{\mathbf{A}}$ and $\text{MO-RAND}_{\mathsf{ECT}}^{\mathbf{A}}$ in Fig. 8,

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

The game $\text{MO-ROR-G}_1^{\mathbf{A}}$ in Fig. 9 is different from $\text{MO-REAL}_{\mathsf{ECT}}^{\mathbf{A}}$ in that the former records all the histories of **Enc** by "$\mathrm{R}[A, C, B] \leftarrow (M, L)$" and uses them to answer to the queries to **Dec**. Thus,

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

The game $\text{MO-ROR-G}_2^{\mathbf{A}}$ in Fig. 10 is different from $\text{MO-ROR-G}_1^{\mathbf{A}}$ 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 $\text{MO-ROR-G}_1^{\mathbf{A}}$ or $\text{MO-ROR-G}_2^{\mathbf{A}}$ with the use of its oracle. Thus,

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

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

The game $\text{MO-ROR-G}_3^{\mathbf{A}}$ in Fig. 11 is different from $\text{MO-ROR-G}_2^{\mathbf{A}}$ 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, $\text{MO-ROR-G}_3^{\mathbf{A}}$ is equivalent to $\text{MO-ROR-G}_2^{\mathbf{A}}$. L is selected uniformly at random from Σ^ℓ, Thus,

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

The game MO-ROR-G_4 in Fig. 12 is different from $\text{MO-ROR-G}_3^{\mathbf{A}}$ 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

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

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

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

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

$\mathbf{D}_2$ 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$^{\mathbf{A}}_{\mathsf{ECT}}$.

```
$K \twoheadleftarrow \Sigma^n$; $\mathcal{Y} \leftarrow \emptyset$
$b \leftarrow \mathbf{A}^{\mathbf{Enc},\mathbf{Dec},\mathbf{ChalEnc}}$
return $b$

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

Dec$(A, C, B)$
if $(A, C, B) \notin \mathcal{Y}$ then
    return $\perp$
end if
$C_0 \| C_1 \leftarrow C$
$L \leftarrow \mathsf{D}_K(B, C_1)$
$M \leftarrow \mathsf{dec}(L, A, C_0, B)$
return $(M, L)$

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

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

```
$K \twoheadleftarrow \Sigma^n$; $\mathcal{Y} \leftarrow \emptyset$
$b \leftarrow \mathbf{A}^{\mathbf{Enc},\mathbf{Dec},\mathbf{ChalEnc}}$
return $b$

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

Dec$(A, C, B)$
if $(A, C, B) \notin \mathcal{Y}$ then
    return $\perp$
end if
$C_0 \| C_1 \leftarrow C$
$L \leftarrow \mathsf{D}_K(B, C_1)$
$M \leftarrow \mathsf{dec}(L, A, C_0, B)$
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 $(C, B)$
```

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

Fig. 8: Games for confidentiality of ECT

B Proof of Theorem 2

The game MO-CTXT$^{\mathbf{A}}_{\mathsf{ECT}}$ is shown in Fig. 13. Without loss of generality, it is assumed that $\mathbf{A}$ terminates right after *win* gets `true`.

```
$K \twoheadleftarrow \Sigma^n$; $\mathcal{Y} \leftarrow \emptyset$
$b \leftarrow \mathbf{A}^{\mathbf{Enc},\mathbf{Dec},\mathbf{ChalEnc}}$
return $b$

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

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

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

Fig. 9: MO-ROR-$\mathrm{G}_1^{\mathbf{A}}$

```
$\underline{\varpi \twoheadleftarrow \mathcal{P}_{\tau,\ell}; \mathcal{Y} \leftarrow \emptyset}$
$b \leftarrow \mathbf{A}^{\mathbf{Enc},\mathbf{Dec},\mathbf{ChalEnc}}$
return $b$

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

Fig. 10: MO-ROR-$\mathrm{G}_2^{\mathbf{A}}$

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

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

Fig. 11: 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$(A, M)$

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

Fig. 12: MO-ROR-$\mathrm{G}_4^{\mathbf{A}}$

The game MO-CTXT-G$_1^{\mathbf{A}}$ in Fig. 14 is different from MO-CTXT$_{\mathsf{ECT}}^{\mathbf{A}}$ 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,

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

The game MO-CTXT-G$_2^{\mathbf{A}}$ in Fig. 15 is different from MO-CTXT-G$_1^{\mathbf{A}}$ 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$_1^{\mathbf{A}}$ or MO-CTXT-G$_2^{\mathbf{A}}$ with the use of its oracle. Thus,

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

$\mathbf{D}$ 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$_{\mathsf{ECT}}^{\mathbf{A}}$.

In the game MO-CTXT-G$_3^{\mathbf{A}}$ shown in Fig. 15, **Dec** and **ChalDec** select L uniformly at random from Σ^ℓ, while they call ϖ^{-1} in MO-CTXT-G$_2^{\mathbf{A}}$. As long as no collision is found for L, the games are equivalent to each other. Thus,

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

Now, $\Pr[\text{MO-CTXT-G}_3^{\mathbf{A}} = \mathtt{true}]$ is evaluated. Suppose that *win* is set $\mathtt{true}$ by a query (A^*, C^*, B^*) to **ChalDec**. Let Win$_1$, Win$_2$, and Win$_3$ be the cases that

1. P$[B^*, C_1^*] \neq \perp$ and P$[B^*, C_1^*]$ is already set by **Enc**,
2. P$[B^*, C_1^*] \neq \perp$ and P$[B^*, C_1^*]$ is already set by **Dec** or **ChalDec**, and
3. P$[B^*, C_1^*] = \perp$,

respectively, where C_1^* is the least significant ℓ bits of C^*. Then,

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

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$_3^{\mathbf{A}}$ 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 $\mathsf{dec}(\dot{L}, A^*, C^*, B^*) \neq \perp$. Thus, $\mathrm{Adv}_{\mathsf{EC}}^{\mathrm{scu}}(\dot{\mathbf{A}}) = \Pr[\mathrm{Win}_1]/q_{\mathrm{e}}$.

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$_3^{\mathbf{A}}$ and guesses (B^*, C_1^*). It interrupts the execution of MO-CTXT-G$_3^{\mathbf{A}}$ 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$_3^{\mathbf{A}}$ by making use of state^*. Finally, $\ddot{\mathbf{A}}_2$ outputs (A^*, C_0^*) satisfying $\mathsf{dec}(\ddot{L}, A^*, C_0^*, B^*) \neq \perp$. Thus, $\mathrm{Adv}_{\mathsf{EC}}^{\mathrm{tcu}}(\ddot{\mathbf{A}}) = (\Pr[\mathrm{Win}_2] + \Pr[\mathrm{Win}_3])/(q_{\mathrm{d}} + q_{\mathrm{c}})$.

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

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

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

$\mathbf{ChalDec}(A, C, B)$
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
    $win \leftarrow \texttt{true}$
    $M \leftarrow \mathsf{dec}(L, A, C_0, B)$
    return $(M, L)$
end if
```

Fig. 13: Game MO-CTXT$^{\mathbf{A}}_{\mathsf{ECT}}$

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

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

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

$\mathbf{ChalDec}(A, C, B)$
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
    $win \leftarrow \texttt{true}$
    $M \leftarrow \mathsf{dec}(L, A, C_0, B)$
    return $(M, L)$
end if
```

Fig. 14: MO-CTXT-G$^{\mathbf{A}}_1$. All the entries of the table P are initialized by $\perp$.

```
$\underline{\varpi \twoheadleftarrow \mathcal{P}_{\tau,\ell};\ \mathcal{Y} \leftarrow \emptyset}$
$\underline{win \leftarrow \texttt{false}}$
$\mathbf{A}^{\mathbf{Enc},\mathbf{Dec},\mathbf{ChalDec}}$
**return** $win$

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

$\mathbf{Dec}(A, C, B)$
$C_0 \| C_1 \leftarrow C$
**if** $\mathrm{P}[B, C_1] \neq \bot$ **then**
    $L \leftarrow \mathrm{P}[B, C_1]$
**else**
    $\underline{\mathrm{G}_2\text{: } L \leftarrow \varpi^{-1}(B, C_1) / \mathrm{G}_3\text{: } L \twoheadleftarrow \Sigma^\ell}$
    $\underline{\mathrm{P}[B, C_1] \leftarrow L}$
**end if**
**return** $\mathsf{dec}(L, A, C_0, B)$

$\mathbf{ChalDec}(A, C, B)$
**if** $(A, C, B) \in \mathcal{Y}$ **then**
    **return** $\bot$
**end if**
$C_0 \| C_1 \leftarrow C$
**if** $\mathrm{P}[B, C_1] \neq \bot$ **then**
    $L \leftarrow \mathrm{P}[B, C_1]$
**else**
    $\underline{\mathrm{G}_2\text{: } L \leftarrow \varpi^{-1}(B, C_1) / \mathrm{G}_3\text{: } L \twoheadleftarrow \Sigma^\ell}$
    $\underline{\mathrm{P}[B, C_1] \leftarrow L}$
**end if**
**if** $\mathsf{dec}(L, A, C_0, B) = \bot$ **then**
    **return** $\bot$
**else**
    $win \leftarrow \texttt{true}$
    $M \leftarrow \mathsf{dec}(L, A, C_0, B)$
    **return** $(M, L)$
**end if**
```

Fig. 15: MO-CTXT-$\mathrm{G}_2^{\mathbf{A}}$ and MO-CTXT-$\mathrm{G}_3^{\mathbf{A}}$

C Proof of Theorem 3

For the games RK-REAL$^{\mathbf{A}}_{\mathsf{ECT}}$ and RK-RAND$^{\mathbf{A}}_{\mathsf{ECT}}$ in Fig. 16,

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

The game RK-ROR-G$^{\mathbf{A}}_1$ in Fig. 17 is different from 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 RK-REAL$^{\mathbf{A}}_{\mathsf{ECT}}$ or 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 RK-REAL$^{\mathbf{A}}_{\mathsf{ECT}}$.

The game RK-ROR-G$^{\mathbf{A}}_2$ in Fig. 18 is different from 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 RK-REAL$^{\mathbf{A}}_{\mathsf{ECT}}$.

The game RK-ROR-G$^{\mathbf{A}}_3$ in Fig. 18 is different from 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, RK-ROR-G$^{\mathbf{A}}_3$ is equivalent to 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 RK-ROR-G$^{\mathbf{A}}_3$ and RK-RAND$^{\mathbf{A}}_{\mathsf{ECT}}$, similar to the transformation from RK-REAL$^{\mathbf{A}}_{\mathsf{ECT}}$ to 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 RK-RAND$^{\mathbf{A}}_{\mathsf{ECT}}$.

D Proof of Theorem 4

The game RK-CTXT$^{\mathbf{A}}_{\mathsf{ECT}}$ is shown in Fig. 19. The game RK-CTXT-G$^{\mathbf{A}}_1$ in Fig. 20 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. 21 uses a random tweakable permutation ϖ instead of TBC. In the game RK-CTXT-G$^{\mathbf{A}}_3$ shown in Fig. 21, $\mathbf{E}$ 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

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

```
$K \twoheadleftarrow \Sigma^n$; $\mathcal{Y} \leftarrow \emptyset$
$b \leftarrow \mathbf{A}^{\mathbf{E},\mathbf{D},\mathbf{ChalEnc}}$
return $b$

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

$\mathbf{D}(B, C_1)$
if $(B, C_1) \in \mathcal{Y}$ then
    return $\perp$
end if
$L \leftarrow \mathsf{D}_K(B, C_1)$
return $L$

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

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

```
$K \twoheadleftarrow \Sigma^n$; $\mathcal{Y} \leftarrow \emptyset$
$b \leftarrow \mathbf{A}^{\mathbf{E},\mathbf{D},\mathbf{ChalEnc}}$
return $b$

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

$\mathbf{D}(B, C_1)$
if $(B, C_1) \in \mathcal{Y}$ then
    return $\perp$
end if
$L \leftarrow \mathsf{D}_K(B, C_1)$
return $L$

$\mathbf{ChalEnc}(A, M)$

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

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

Fig. 16: Games for confidentiality of RK ECT

```
$\underline{\varpi \twoheadleftarrow \mathcal{P}_{\tau,\ell};}$ $\mathcal{Y} \leftarrow \emptyset$
$b \leftarrow \mathbf{A}^{\mathbf{E},\mathbf{D},\mathbf{ChalEnc}}$
return $b$

$\mathbf{E}(B, L)$
$\underline{C_1 \leftarrow \varpi(B, L)}$
return $C_1$

$\mathbf{D}(B, C_1)$
if $(B, C_1) \in \mathcal{Y}$ then
    return $\bot$
end if
$\underline{L \leftarrow \varpi^{-1}(B, C_1)}$
return $L$

$\mathbf{ChalEnc}(A, M)$
$L \twoheadleftarrow \Sigma^\ell$
$(C_0, B) \leftarrow \mathsf{enc}(L, A, M)$
$\underline{C_1 \leftarrow \varpi(B, L)}$
$C \leftarrow C_0 \| C_1$
$\mathcal{Y} \leftarrow \mathcal{Y} \cup \{(B, C_1)\}$
return $(C, B)$
```

Fig. 17: RK-ROR-$\mathrm{G}_1^{\mathbf{A}}$

```
$\varpi \twoheadleftarrow \mathcal{P}_{\tau,\ell}; \mathcal{Y} \leftarrow \emptyset$
$b \leftarrow \mathbf{A}^{\mathbf{E},\mathbf{D},\mathbf{ChalEnc}}$
return $b$

$\mathbf{E}(B, L)$
$C_1 \leftarrow \varpi(B, L)$
return $C_1$

$\mathbf{D}(B, C_1)$
if $(B, C_1) \in \mathcal{Y}$ then
    return $\bot$
end if
$L \leftarrow \varpi^{-1}(B, C_1)$
return $L$

$\mathbf{ChalEnc}(A, M)$
$\mathrm{G}_2$: $L \twoheadleftarrow \Sigma^\ell$/$\underline{\mathrm{G}_3\text{:}\qquad\qquad\qquad}$
$\underline{(C_0, B) \twoheadleftarrow \Sigma^{\mathsf{clen}(|M|)} \times \Sigma^\tau}$
$\mathrm{G}_2$: $C_1 \leftarrow \varpi(B, L)$/$\underline{\mathrm{G}_3\text{: } C_1 \twoheadleftarrow \Sigma^\ell}$
$C \leftarrow C_0 \| C_1$
$\mathcal{Y} \leftarrow \mathcal{Y} \cup \{(B, C_1)\}$
return $(C, B)$
```

Fig. 18: RK-ROR-$\mathrm{G}_2^{\mathbf{A}}$ and RK-ROR-$\mathrm{G}_3^{\mathbf{A}}$

$\mathbf{D}$ 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 $\mathrm{RK\text{-}CTXT}^{\mathbf{A}}_{\mathsf{ECT}}$.

Now, $\Pr[\mathrm{RK\text{-}CTXT\text{-}G}^{\mathbf{A}}_{3} = \mathtt{true}]$ 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 $\mathrm{RK\text{-}CTXT\text{-}G}^{\mathbf{A}}_{3}$ 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
2. otherwise,

respectively. Then,

$$\Pr[\mathrm{RK\text{-}CTXT\text{-}G}^{\mathbf{A}}_{3} = \mathtt{true}] = \Pr[\mathrm{Win}_1] + \Pr[\mathrm{Win}_2].$$

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 $\mathrm{RK\text{-}CTXT\text{-}G}^{\mathbf{A}}_{3}$.

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 $\mathrm{RK\text{-}CTXT\text{-}G}^{\mathbf{A}}_{3}$ and guesses (B^*, C^*_1) in the queries to $\mathbf{D}$ or **ChalDec**. It interrupts the execution of $\mathrm{RK\text{-}CTXT\text{-}G}^{\mathbf{A}}_{3}$ right after it finds (B^*, C^*_1). Then, $\ddot{\mathbf{A}}_2$ gets $\ddot{L} \twoheadleftarrow \Sigma^{\ell}$ and resumes the execution of $\mathrm{RK\text{-}CTXT\text{-}G}^{\mathbf{A}}_{3}$. Finally, $\ddot{\mathbf{A}}_2$ outputs (A^*, C^*_0) satisfying $\mathsf{dec}(\ddot{L}, A^*, C^*_0, B^*) \neq \bot$, where $C^* = C^*_0 \| C^*_1$. Thus, $\mathrm{Adv}^{\mathrm{tcu}}_{\mathsf{EC}}(\ddot{\mathbf{A}}) = \Pr[\mathrm{Win}_2]/(q_{\mathrm{d}} + q_{\mathrm{c}})$.

E HFC and Its Targeted Ciphertext Unforgeability

The HFC encryptment scheme [12] $\mathsf{HFC} := (\mathsf{Hkg}, \mathsf{Henc}, \mathsf{Hdec}, \mathsf{Hver})$ 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

```
$K \twoheadleftarrow \Sigma^n$
$win \leftarrow$ false; $ctr \leftarrow 0$
$\mathbf{A}^{\mathbf{E},\mathbf{D},\mathbf{ChalDec}}$
if $ctr < 0$ then
    $win \leftarrow$ 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. 19: Game RK-CTXT$^{\mathbf{A}}_{\mathsf{ECT}}$

```
$K \twoheadleftarrow \Sigma^n$; $\mathcal{Z} \leftarrow \emptyset$
$win \leftarrow$ false; $ctr \leftarrow 0$
$\mathbf{A}^{\mathbf{E},\mathbf{D},\mathbf{ChalDec}}$
if $ctr < 0$ then
    $win \leftarrow$ 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. 20: RK-CTXT-G$^{\mathbf{A}}_1$

```
$\varpi \twoheadleftarrow \mathcal{P}_{\tau,\ell}$; $\mathcal{Z} \leftarrow \emptyset$
$win \leftarrow$ false; $ctr \leftarrow 0$
$\mathbf{A}^{\mathbf{E},\mathbf{D},\mathbf{ChalDec}}$
if $ctr < 0$ then
    $win \leftarrow$ 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
    $\mathrm{G}_2$: $C_1 \leftarrow \varpi(B, L)$/$\mathrm{G}_3$: $C_1 \twoheadleftarrow \Sigma^\ell$
    $\mathcal{Z} \leftarrow \mathcal{Z} \cup \{(B, L, C_1)\}$
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
    $\mathrm{G}_2$: $L \leftarrow \varpi^{-1}(B, C_1)$/$\mathrm{G}_3$: $L \twoheadleftarrow \Sigma^\ell$
    $\mathcal{Z} \leftarrow \mathcal{Z} \cup \{(B, L, C_1)\}$
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
    $\mathrm{G}_2$: $L \leftarrow \varpi^{-1}(B, C_1)$/$\mathrm{G}_3$: $L \twoheadleftarrow \Sigma^\ell$
    $\mathcal{Z} \leftarrow \mathcal{Z} \cup \{(B, L, C_1)\}$
end if
if $\mathsf{dec}(L, A, C_0, B) \neq \bot$ then
    $ctr \leftarrow ctr - 1$
    $M \leftarrow \mathsf{dec}(L, A, C_0, B)$
    return $(M, L)$
else
    return $\bot$
end if
```

Fig. 21: RK-CTXT-$\mathrm{G}_2^{\mathbf{A}}$ and RK-CTXT-$\mathrm{G}_3^{\mathbf{A}}$

are described in Fig. 22. The description of the verification algorithm Hver is omitted since it is apparent from Hdec.

```
$\mathsf{Henc}(K_{\mathrm{ec}}, A, M)$
$(A_1, \ldots, A_a) \leftarrow \mathtt{parse}_\ell(A)$
$(M_1, \ldots, M_m) \leftarrow \mathtt{parse}_\tau(M)$
$V_0 \leftarrow \mathsf{f}(IV, K_{\mathrm{ec}})$
for $i = 1$ to $a$ do
    $V_i \leftarrow \mathsf{f}(V_{i-1}, K_{\mathrm{ec}} \oplus A_i)$
end for
for $i = 1$ to $m$ do
    $C_i \leftarrow M_i \oplus V_{a+i-1}$
    $M'_i \leftarrow M_i \| 0^{\ell-\tau}$
    $V_{a+i} \leftarrow \mathsf{f}(V_{a+i-1}, K_{\mathrm{ec}} \oplus M'_i)$
end for
$M'_{m+1} \leftarrow 0^{\ell-128} \| \langle A \rangle_{64} \| \langle M \rangle_{64}$
$B \leftarrow \mathsf{f}(V_{a+m}, K_{\mathrm{ec}} \oplus M'_{m+1})$
$C \leftarrow C_1 \| C_2 \| \cdots \| C_m$
return $(C, B)$
```

```
$\mathsf{Hdec}(K_{\mathrm{ec}}, A, C, B)$
$(A_1, \ldots, A_a) \leftarrow \mathtt{parse}_\ell(A)$
$(C_1, \ldots, C_c) \leftarrow \mathtt{parse}_\tau(C)$
$V_0 \leftarrow \mathsf{f}(IV, K_{\mathrm{ec}})$
for $i = 1$ to $a$ do
    $V_i \leftarrow \mathsf{f}(V_{i-1}, K_{\mathrm{ec}} \oplus A_i)$
end for
for $i = 1$ to $c$ do
    $M_i \leftarrow C_i \oplus V_{a+i-1}$
    $M'_i \leftarrow M_i \| 0^{\ell-\tau}$
    $V_{a+i} \leftarrow \mathsf{f}(V_{a+i-1}, K_{\mathrm{ec}} \oplus M'_i)$
end for
$M'_{c+1} \leftarrow 0^{\ell-128} \| \langle A \rangle_{64} \| \langle C \rangle_{64}$
$B' \leftarrow \mathsf{f}(V_{a+c}, K_{\mathrm{ec}} \oplus M'_{c+1})$
if $B' = B$ then
    $M \leftarrow M_1 \| M_2 \| \cdots \| M_c$
    return $M$
else
    return $\perp$
end if
```

Fig. 22: 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 $X \in \Sigma^*$.

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 $(Y_{1,j_1}, W_{1,j_1}) \in \Sigma^\tau \times \Sigma^\ell$. 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 $\mathsf{Hdec}(K_{\mathrm{ec}}, A, C, B) \neq \bot$, 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,

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

□

F 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 $K_{\mathrm{ec}} \leftarrow \mathsf{kg}(1^n)$ 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 $\mathsf{dec}_{K_{\mathrm{ec}}}(A', C', B) = \bot$ 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 $\mathsf{dec}_{K_{\mathrm{ec}}}(A', C', B) = M' \neq \bot$, then $(A, M) \neq (A', M')$ and $\mathsf{ver}(A', M', K_{\mathrm{ec}}, B) = 1$.

Suppose that $\mathsf{dec}_{K_{\mathrm{ec}}}(A', C', B) \neq \bot$. 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.

G Diagrams of ECT

Diagrams of encryption and decryption algorithms of ECT are given in Fig. 23.

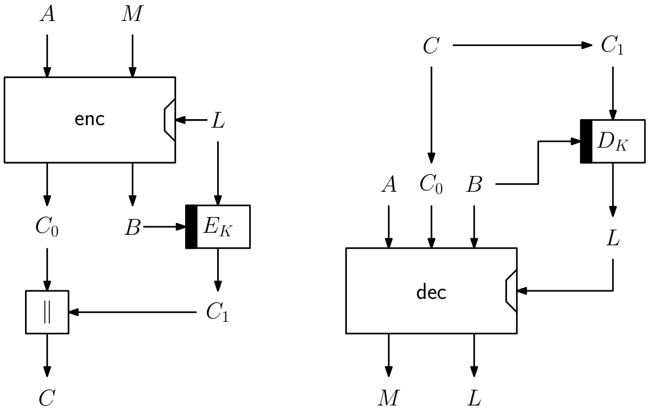

Fig. 23: Diagrams of encryption and decryption algorithms of ECT