Compactly Committing Authenticated Encryption Using Encryptment and Tweakable Block Cipher

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

[1]University of Fukui

[2]NEC

[3]Yokohama National University

SAC 2023 (16-18/08/2023)

Background & Related Work (1/3)

Malicious senders may send harassing messages and/or harmful contents

Message franking

- introduced in the Facebook end-to-end messaging system
- a cryptographic scheme which enables users to report abusive messages to their service provider in a verifiable manner

Grubbs et al. [GLR17]

- formalized message franking in the symmetric-key setting and introduced ccAEAD (Compactly Committing AEAD)
- presented generic constructions with provable security

AEAD (Authenticated Encryption with Associated Data)

ccAEAD has additional functionality that a small part of the ciphertext can be used as a commitment to the message

Background & Related Work (2/3)

Dodis et al. [DGRW18]

- showed an attack on the message franking protocol of Facebook
- introduced a new primitive called encryptment as a core building block of ccAEAD
- presented a provably secure encryptment scheme HFC
- presented two transformations to ccAEAD from encryptment
  1. with one call to AEAD (randomized scheme)
  2. with two calls to PRF (nonce-based scheme)
- posed open questions
  1. Formalization of remotely keyed (RK) ccAEAD
  2. Construction of RK ccAEAD

Background & Related Work (3/3)

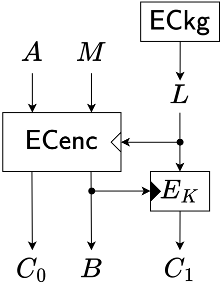
Remotely keyed encryption

- introduced by Blaze in 1996
- enables bulk encryption/decryption by utilizing
  - power of a host
  - security of a personal device storing a secret key
- relevant to leakage resilience

Our Contributions

1. New construction of ccAEAD: ECT (EnCryptment-then-Tbc)
2. Formalize Remotely Keyed (RK) ccAEAD
   - Follows RK AEAD by Dodis and An [DA03]
3. ECT works as secure RK ccAEAD

Encryption algorithm of ECT:



ccAEAD Syntax

ccAEAD CAE $:= (\mathsf{Kg}, \mathsf{Enc}, \mathsf{Dec}, \mathsf{Ver})$

Key generation $K \leftarrow \mathsf{Kg}$

- K: Secret key

Encryption $(C, B) \leftarrow \mathsf{Enc}(K, A, M)$

- A: Associated data; requires only authenticity
- M: Message; requires both privacy and authenticity
- C: Ciphertext
- B: Binding tag (used as commitment to message)

Decryption (M, L) or $\perp \leftarrow \mathsf{Dec}(K, A, C, B)$

Decryption returns $\perp$ if (A, C, B) is invalid w.r.t. K

- L: Opening key (for commitment)

Verification 0 or $1 \leftarrow \mathsf{Ver}(A, M, L, B)$

ccAEAD Security Requirements (Informal)

Confidentiality Real-or-random indistinguishability

Outputs of the encryption algorithm should look uniformly random

Ciphertext Integrity Unforgeability

Valid (A, C, B) should not be forged

Binding properties

Receiver binding A malicious receiver should not be able to blame a non-abusive sender for sending an abusive message

Sender binding A malicious sender of an abusive message should not be able to avoid being blamed

Remark

- Confidentiality and ciphertext integrity are also required of conventional AEAD
- Binding properties are specific to ccAEAD

Encryptment Syntax

Encryptment = Encryption + Commitment $\approx$ One-time ccAEAD

$\mathsf{EC} := (\mathsf{kg}, \mathsf{enc}, \mathsf{dec}, \mathsf{ver})$

Key generation $K_{\mathrm{ec}} \leftarrow \mathsf{kg}$

- K_{ec}: Secret key (used for both encryption and commitment)

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

- A: Associated data; requires only authenticity
- M: Message; requires both privacy and authenticity
- C: Ciphertext
- B: Binding tag (used as commitment to message)

Decryptment M or $\perp \leftarrow \mathsf{dec}(K_{\mathrm{ec}}, A, C, B)$

Decryption returns $\perp$ if (A, C, B) is invalid w.r.t. K_{ec}

Verification 0 or $1 \leftarrow \mathsf{ver}(A, M, K_{\mathrm{ec}}, B)$

Encryptment Security Requirements

Encryptment $\approx$ One-time ccAEAD

Confidentiality One-time Real-or-random indistinguishability

An output of the encryptment algorithm should look uniformly random

Second ciphertext unforgeability

Valid (A, C, B) should not be forged for given B

Binding properties

- Receiver binding
- Sender binding
  - Similar to those of ccAEAD

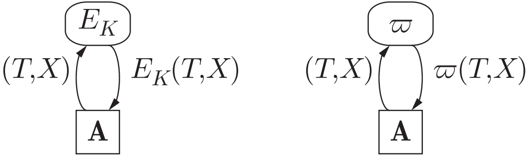
Tweakable Block Cipher (TBC)

TBC $\quad Y \leftarrow E_K(T, X)$

- K: Secret key, X: Plaintext, $\underline{T\text{: Tweak}}$, Y: Ciphertext
- $E_K(T, \cdot)$ is a permutation for any K $\underline{\text{and } T}$

Security requirement: Tweakable PRP (Pseudorandom Permutation)

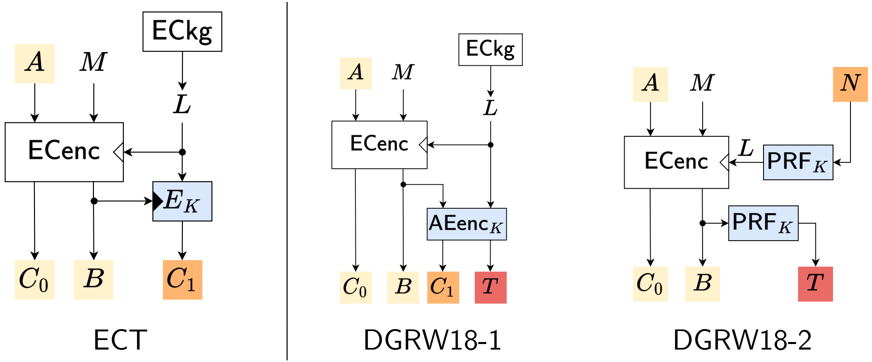
- indistinguishability between real world and ideal world
- K: uniform random key, ϖ: uniform random permutation



real world ideal world

Strong Tweakable PRP: $\mathbf{A}$ interacts with (E_K, E_K^{-1}) and (ϖ, ϖ^{-1}).

New construction of ccAEAD: ECT (EnCryptment-then-Tbc)



ECT is more efficient in terms of bandwidth.

- ECT has no tag T for binding tag B
- It is reasonable to assume $|L| = |C_1| \approx |N|$.

Security of ECT

Let $\ell := |B|$.

Theorem (Confidentiality)

ECT satisfies up to $(\ell/2)$-bit confidentiality $\Longleftarrow$

- Encryptment satisfies OT-RoR confidentiality, and
- TBC is TPRP.

Theorem (Ciphertext Integrity)

ECT satisfies up to $(\ell/2)$-bit CTXT-INT $\Longleftarrow$

- Encryptment satisfies SCU and TCU, and
- TBC is STPRP.

Cf.) TCU (Targeted Ciphertext Unforgeability) is new security notion.

Theorem (Binding properties)

ECT inherits binding properties of encryptment.

Targeted Ciphertext Unforgeability (TCU)

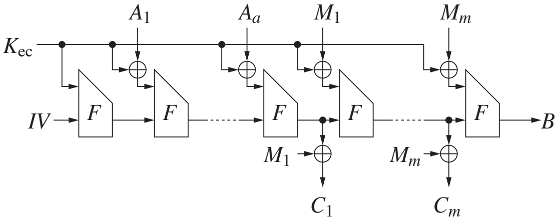
New security requirement for encryptment

Valid (A, C, B) is unforgeable if adversary chooses B before receiving K_{ec}

Adversary: $\mathbf{A} := (\mathbf{A}_1, \mathbf{A}_2)$

1. $(B, state) \leftarrow \mathbf{A}_1$
2. $(A, C) \leftarrow \mathbf{A}_2(B, state; K_{\mathrm{ec}})$, where $K_{\mathrm{ec}} \leftarrow$ kg

Theorem: HFC satisfies TCU in ROM. (TCU is feasible.)



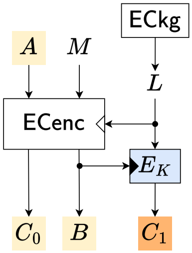
Cf.) TCU is relevant to everywhere preimage resistance.

Proof Sketch of CTXT-INT

Theorem (Ciphertext Integrity)

ECT satisfies up to $(\ell/2)$-bit CTXT-INT $\Longleftarrow$

- Encryptment satisfies SCU and TCU, and
- TBC is STPRP.



(Proof sketch) Suppose that $\mathbf{A}$ succeeds in forging (A, C_0, B, C_1).

1. (B, C_1) is not new.
   $\Longrightarrow$ $\mathbf{A}$ already obtained (A', C_0', B, C_1) from encryption oracle s.t. $(A', C_0') \neq (A, C_0)$.
   $\Longrightarrow$ $\mathbf{A}$ succeeds in breaking SCU.
2. (B, C_1) is new.
   $\Longrightarrow$ $L = E_K^{-1}(B, C_1)$ is random since E_K is STPRP.
   $\Longrightarrow$ $\mathbf{A}$ succeeds in breaking TCU.

RK ccAEAD Syntax

RKCAE := (RKKg, RKEnc, RKDec, RKVer)

Key generation $K \leftarrow$ RKKg

Encryption $(C, B) \leftarrow$ RKEnc(K, A, M) proceeds as follows:

1. $(Q_\mathrm{e}, S_\mathrm{e}) \leftarrow$ Pre-TE(A, M)
2. $R_\mathrm{e} \leftarrow$ TE$_K(Q_\mathrm{e})$ (run by a trusted device)
3. $(C, B) \leftarrow$ Post-TE$(R_\mathrm{e}, S_\mathrm{e})$

Decryption (M, L) or $\perp \leftarrow$ RKDec(K, A, C, B) proceeds as follows:

1. $(Q_\mathrm{d}, S_\mathrm{d}) \leftarrow$ Pre-TD(A, C, B)
2. $R_\mathrm{d} \leftarrow$ TD$_K(Q_\mathrm{d})$ (run by a trusted device)
3. $(M, L)/\perp \leftarrow$ Post-TD$(R_\mathrm{d}, S_\mathrm{d})$

Verification 0 or $1 \leftarrow$ RKVer(A, M, L, B)

For simplifying security analyses, TE$_K$ and TD$_K$ are called only once.

RK ccAEAD Security Requirements (Informal)

Adversaries have direct access to TE_K and TD_K

Confidentiality Real-or-random indistinguishability

Outputs of the encryption algorithm should look uniformly random

- Adversaries are not allowed to ask TD_K queries on ciphertexts from the encryption oracle

Ciphertext Integrity Unforgeability

Valid (A, C, B) should not be forged

- Successful forgeries are easy since TE_K is available
- $(\#$ of successful forgeries$) \leq (\#$ of queries to $\mathsf{TE}_K)$

Binding properties Same as those of ccAEAD

ECT is Secure RK ccAEAD

Let $\ell := |B|$.

Theorem (Confidentiality)

ECT satisfies up to $(\ell/2)$-bit confidentiality $\Longleftarrow$

- Encryptment satisfies confidentiality with attachment, and
- TBC is TPRP.

Cf.) Confidentiality with attachment is new security notion.

Theorem (Ciphertext Integrity)

ECT satisfies up to $(\ell/2)$-bit CTXT-INT $\Longleftarrow$

- Encryptment satisfies receiver binding and TCU, and
- TBC is STPRP.

Theorem (Binding properties)

ECT inherits binding properties of encryptment.

Confidentiality with Attachment

New security requirement for encryptment

- specific to ECT for RK ccAEAD
- somewhat artificial

One-time real-or-random indistinguishability

- $\mathbf{A}$ can ask a single query to encryptment
- $\mathbf{A}$ can also ask queries to encryption and decryption of ideal TBC
  - $\mathbf{A}$ has direct access to TE_K and TD_K
  - TBC is used for TE_K and TD_K

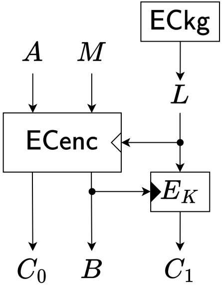
Theorem: HFC satisfies confidentiality with attachment in ROM.

(Confidentiality with attachment is feasible.)

Conclusion

Summary

1. New construction of ccAEAD: ECT (EnCryptment-then-Tbc)
2. Formalize Remotely Keyed (RK) ccAEAD
3. ECT is secure (RK) ccAEAD
4. New security requirements for encryptment
   - Targeted ciphertext unforgeability
   - Confidentiality with attachment
5. HFC satisfies both requirements in ROM



Future work

- Designs of simpler ccAEAD
- Applications of ccAEAD