Two-Pass Authenticated Encryption Faster than Generic Composition

University of Mannheim, Germany
http://th.informatik.uni-mannheim.de/people/lucks/

Abstract. This paper introduces CCFB and CCFB+H, two patent-free authenticated encryption schemes. CCFB+H also supports the authentication of associated data. Our schemes can employ any block cipher and are provably secure under standard assumptions. The schemes and their proofs of security are simple and straightforward. CCFB and CCFB+H restrict the sizes of nonce and authentication tags and can, depending on these sizes, perform significantly better than both generic composition and other two-pass schemes for authenticated encryption, such as the EAX mode.

Keywords: authenticated encryption, associated data, provable security, OMAC

1 Introduction

Authenticated Encryption (AE)
both *and*

(associated data, AD)
Authenticated Encryption with Associated Data (AEAD)

1.1 The Development of Authenticated Encryption

generic composition

minimal-expanding[1]

plaintext size τ *bit for the authentication tag* τ

$1/2^{\tau}$

single-pass

[2]

single-pass

two-pass

1.2 Contributions and Outline of this Paper

before

[1] ... depending on the underlying encryption and MAC scheme.

[2] E.g., AES-RPC with 32-bit authentication tags is 50 % faster than AES-based generic composition.

– *minimal-expanding* [3] *two-pass*

– [4]

–

–

–

–

–

n

$$\overbrace{\qquad\qquad}^{\delta} = \overbrace{\quad}^{n} - \overbrace{\qquad\qquad}^{\tau}.$$

2 CCFB Authenticated Encryption

CCFB authenticated encryption $F : \{0,1\}^n \rightarrow \{0,1\}^n$ $\tau \leq n/2$ $\delta = n - \tau$ $(d,t) := F(\cdot)$ $d \in \{0,1\}^\delta$ $t \in \{0,1\}^\tau$ $i \in \{1,\ldots,2^\tau - 1\}$ $\langle i \rangle_\tau$ τ $\|$ X $\geq \lambda$ $_\lambda(X)$ λ

[3] We neither have, nor are aware of any patents or pending patents relevant to CCFB+H. We do not intend to apply for such patents.

[4] EAX and our instantiation of CCFB+H are dominated by the block cipher operations, and can run on any low-end device capable of running block cipher operations. This enables a "platform-independent" performance evaluation by counting the number of block cipher calls, see Section 8. In the same section, we also explain why CWC and GCM appear to be poor choices for low-end devices.

X $N \in \{0,1\}^\delta$
M $|M|$ 1
$(2^\tau - 3)\delta$

Algorithm:
Input: $N \in \{0,1\}^\delta$ $M \in \{0,1\}^*$ $1 \le |M| \le (2^\tau - 3)\delta$
First pass:
M $(M_1, \ldots, M_m)$
$|M_1| = \cdots = |M_{m-1}| = \delta$ $|M_m| \in \{1, \ldots, \delta\}$
$C_0 := N$
$1 \le i \le m-1$ $(\ , A_i) := F(C_{i-1}, \langle i \rangle_\tau)$
$C_i := \ \oplus M_i$
$(\ , A_m) := F(C_{m-1}, \langle m \rangle_\tau)$
$|M_m| = \delta$ $d := 1;$ $:= ()(*$ $*);$
$d := 2;$ $:= (1||0^{\delta - |M_m| - 1});$
$C_m := \ _{|M_m|}(\ ) \oplus M_m;$
$C' := \ \oplus (M_m||\ );$
$(\ , A_{m+1}) := F(C', \langle m + d \rangle_\tau)$
Second pass:
$T := A_1 \oplus \cdots \oplus A_{m+1}$
Output: $(C_1, \ldots, C_m, T)$
$C_1 \ C_{m-1} \in \{0,1\}^\delta$ $C_m \in \{0,1\}^{|M_m|}$

Fig. 1. CCFB encryption under $F : \{0,1\}^\delta \times \{0,1\}^\tau \to \{0,1\}^\delta \times \{0,1\}^\tau$.

$|M|$ M δ $|M_m| = \delta$

- $1 \le i \le m$ $(\ , A_i) := F(C_{i-1}, \langle i \rangle_\tau)$
  $C_i := \ \oplus M_i$
- $(\ , A_{m+1}) := F(C_m, \langle m + 1 \rangle_\tau)$

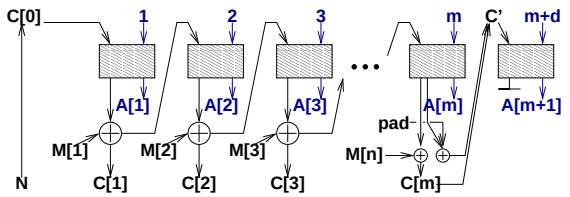


Fig. 2. 1st phase of CCFB encryption: compute the C_i and the local tags A_i; $d \in \{1, 2\}$.

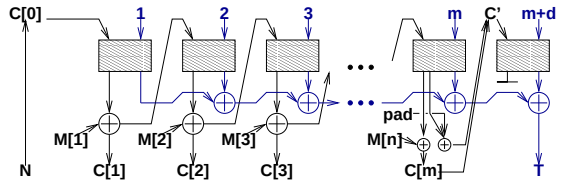


Fig. 3. Full CCFB encryption: The global tag T is computed in the second phase.

$|M|$ M $m = \lceil |M|/\delta \rceil + 1$ M_i
M $2m$ $m+1$

–
F
–
C_i
A_i
$T = \bigoplus A_i$
–

$N \in \{0,1\}^\delta$ $C = (C_1, \ldots, C_m, T)$ **CCFB decryption**

$(M_1, \ldots, M_m)$ $(M'_1, \ldots, M'_{m'})$
$C_1 \oplus C'_1 = M_1 \oplus M'_1$

3 Notions of Security for Authenticated Encryption

AEAD scheme (E, D) E
D

$$E: \text{KEY} \times \text{NONCE} \times \text{HEADER} \times \text{MESSAGE} \to \text{CIPHERTEXT},$$
$$D: \text{KEY} \times \text{NONCE} \times \text{HEADER} \times \text{CIPHERTEXT} \to \text{MESSAGE} \cup \quad .$$

KEY NONCE HEADER MESSAGE CIPHERTEXT
$\{0,1\}^*$ KEY **adversary**
encryption oracle $E(K, \cdot, \cdot, \cdot)$ (N^1, H^1, M^1)
$(N^q, H^q, M^q) \in \text{NONCE} \times \text{HEADER} \times \text{MESSAGE}$

$C^i = E(K, N^i, H^i, M^i)$ **nonce-respecting**
$i \neq j$ $N^i \neq N^j$ NONCE **nonce-randomising**
$N^i \in$ NONCE (N^i, H^i, M^i)

$F(K, \cdot, \cdot, \cdot)$ (N^i, H^i, M^i)
$F(N^i, H^i, M^i)$ $C^i =$
$E(K, N^i, H^i, M^i)$ K
p-**private**
A E F

$$\left|\Pr\left[A^{E(K,\cdot,\cdot,\cdot)} = 1\right] - \Pr\left[A^{F(\cdot,\cdot,\cdot)} = 1\right]\right| \leq p.$$

(N^1, H^1, M^1) (N^q, H^q, M^q)
C^1 C^q C
N H $(C, H) \notin \{(C^1, H^1) \ldots, (C^q, H^q)\}$[5]
$D(K, N, H, C) \neq$
p-**authentic**
A_F K

$$\Pr\left[A_F \quad\right] \leq p.$$

AE scheme
HEADER $= \{0\}$

4 Analysis of CCFB Authenticated Encryption

$\mathcal{A}$ q
$M^1 = (M^1_1 \quad M^1_{m_1})$ $M^q = (M^q_1 \quad M^q_{m_q})$ $r = \sum_{1 \leq i \leq q} m_i$
$N^1 = C^1_0$ $N^q = C^q_0$
$\mathcal{A}$ $C^1 = (C^1_1 \quad C^1_{m_1} \quad T^1)$ $C^q = (C^q_1 \quad C^1_{m_q} \quad T^q)$
F

$$D^i_k = \begin{cases} (C^i_k, k+1) & k < m_i \\ ((C')^i, m_i + d) & k = m_i \quad d = 1 \quad |M_m| = \delta \quad d = 2 \end{cases}$$

$(C')^i$ C'
(D^i_k, D^j_k)

$$D^i_k = D^j_k \qquad 1 \leq i < j \leq q \qquad k \in \{0, \ldots, \min\{m_i, m_j\}\}.$$

q
r $r = \sum_{1 \leq i \leq q} m_i$

[5] Even if the forger is nonce-respecting $N \in \{N^1, \ldots, N^q\}$ is permissable.

Lemma 1. *For CCFB encryption under a random function F, the probability for any nonce-respecting adversary to generate an input-collision is at most*

$$\frac{qr}{2^{\delta+1}}.$$

Similarly, the probability for any nonce-randomising adversary to generate an input-collision is at most

$$\frac{q(r+q)}{2^{\delta+1}}.$$

Proof.
$k = 0$ $k \geq 1$
$D_k^i = D_k^j$ $F(D_{k-1}^i) = F(D_{k-1}^j)$ $D_{k-1}^i \neq D_{k-1}^j$
$\Pr[D_k^i = D_k^j] \leq 1/2^\delta$ (i, j, k) $1 \leq i < j \leq q$
$1 < k \leq \min\{m_i, m_j\}$ $(q-1)r/2$
$\frac{(q-1)r}{2} * \frac{1}{2^\delta} = \frac{(q-1)r}{2^{\delta+1}}$.

$k = 0$
$k = 0$
$(q(q-1)/2)/2^\delta \leq q^2/2^{\delta+1}$
$qr + q^2 = q(r+q)$ □

Theorem 1 (Information-Theoretic Privacy of CCFB).
CCFB encryption using a random F is

$\frac{qr}{2^{\delta+1}}$*-private against nonce-respecting adversaries and*

$\frac{q(r+q)}{2^{\delta+1}}$*-private against nonce-randomising adversaries.*

Proof. D_k^i $k \geq 0$
F

□

Theorem 2 (Information-Theoretic Authenticity of CCFB).
CCFB encryption, using a random F, is

$\left(\frac{qr}{2^{\delta+1}} + \frac{1}{2^\tau}\right)$*-authentic with respect to nonce-respecting adversaries and*

$\left(\frac{q(r+q)}{2^{\delta+1}} + \frac{1}{2^\tau}\right)$*-authentic with respect to nonce-randomising adversaries.*

5 The CCFB+H AEAD Mode and its Analysis

$F' : \{0,1\}^* \to \{0,1\}^\delta$

F F'

F $H \in \{0,1\}^*$

$C_0 := N$ $C_0 := N \oplus F'(H)$

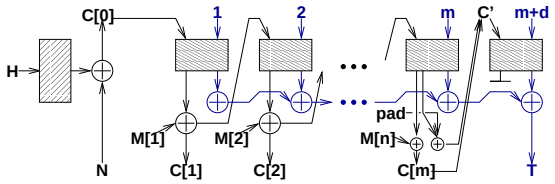


Fig. 4. CCFB Authenticated Encryption of Message $M[\cdot]$ with Associated Data H.

q r

Lemma 2. *For CCFB encryption under a random F, the probability for a nonce-respecting or nonce-randomising adversary to generate an input-collision is at most*

$$\frac{q(r+q)}{2^{\delta+1}}.$$

Proof.

$k = 0$ $q^2/2^{\delta+1}$

H^i i $H^i = H^j$ $D^i \neq D^j$

$H^i \neq H^j$ $\Delta(i,j) := F'(H^i) \oplus F'(H^j) \in \{0,1\}^\delta$ $C_0^i = C_0^j$ $N^i \oplus N^j = \Delta(i,j)$ $1/2^\delta$ $q(q-1)/2$ (i,j) $1 \leq i < j \leq q$ $k = 0$ $q(q-1)/2^{\delta+1}$ □

Theorem 3 (Information-Theoretic Privacy of CCFB+H). *CCFB encryption using a random F is*

$$\frac{qr+q^2}{2^{\delta+1}}\text{-}private.$$

Theorem 4 (Information-Theoretic Authenticity of CCFB+H). *CCFB encryption using a random F is*

$$\left(\frac{qr+q^2}{2^{\delta+1}}+\frac{1}{2^\tau}\right)\text{-}\textit{authentic.}$$

6 Using a Single Random Function f

$F : \{0,1\}^n \to \{0,1\}^n$

E_K K

$F' : \{0,1\}^* \to \{0,1\}^\delta$

F

$f : \{0,1\}^* \to \{0,1\}^n$ F F'

$$F(x) = f(x) \qquad x \in \{0,1\}^n$$
$$F'(y) = \quad_{|M_m|}(f(0^n||y)) \qquad y \in \{0,1\}^*$$

τ

F $2^{\tau-1}$

x $0^n||y$ f [6] F F'

7 Instantiating f by OMAC

[7]

$E_K : \{0,1\}^n \to \{0,1\}^n$

–
– E
– K
–

information-theoretical security as a variable-input-size PRF

Theorem 5 (Lemma 5.2 of [6]). *Consider OMAC under a random permutation $E_K : \{0,1\}^n \to \{0,1\}^n$. An adversary asking at most q' queries, each at most $\mu < 2^n/4$ blocks long, cannot distinguish OMAC from a random function with an advantage exceeding*

$$\frac{(5\mu^2+1)q'}{2^n}.$$

[6] In fact, we could replace $0^n||y$ by $0^\tau||y$. The only reason why we propose the longer 0^n-prefix is the improved efficiency for our OMAC based instantiation of f.

[7] [6] describes two flavours of OMAC, OMAC1 and OMAC2. In this paper, we set OMAC=OMAC1, but we could use OMAC2 just as well.

For the definition of u and "$*$" in GF(2^n) see [5,6]. We stress that computing $L*u$ and $L*u^2$ can be done very efficiently by shifting and conditional XORing.

Algorithm:
Init: $L_0 := E_K(0)$ $L_1 := L_0 * u$ $L_2 := (L_0 * u^2)$ $(*$ 2^n $*)$
Input: $X \in \{0,1\}^n$
X X_1 X_m
$Z := 0^n$
i $1 \le i \le m-1$ $Y := X_i \oplus Z$
$Z := E_K(Y)$
$|M_m| = n$ $Y := Y \oplus L_1$
$Y := Y \oplus L_2$
Output: $E_K(Y)$

Fig. 5. OMAC

f E
E K

– $F'(H)$ $_K$ $0^n||H)$
E_K $\lceil |H|/n \rceil$
$E_K(0) = L_0$

– $F(C_{i-1}, i)$ $F(C', m+d)$

$\Rightarrow$ H M

$$\left\lceil \frac{|H|}{n} \right\rceil + \left\lceil \frac{|M|}{\delta} + 1 \right\rceil$$

8 A Comparison: EAX ↔ CCFB+H

$2^{127} - 1$

2^w

τ

δ

τ

$\Theta(r^2/2^n)$ $\Theta(qr/2^{n-\tau})$

	provable privacy	provable authenticity	limit for τ
EAX	$\Theta\left(\frac{r^2}{2^n}\right)$	$\Theta\left(\min\left\{\frac{r^2}{2^n}, \frac{1}{2^\tau}\right\}\right)$	$\tau \leq n$
CCFB+H	$\Theta\left(\frac{qr}{2^{n-\tau}}\right)$	$\Theta\left(\min\left\{\frac{qr}{2^{n-\tau}}, \frac{1}{2^\tau}\right\}\right)$	$\tau \leq n - \delta$

$r = \sum m_i$: accumulated number of message blocks q: number of messages

Table 1. Asymptotical Security of EAX and CCFB+H.

$(n-\tau)(2^\tau - 3)$

2^τ

block cipher: E $n = 128$
tag size: $\tau = 32$ $\delta = 128 - 32 = 96$
number of messages in the lifetime of a secret key: $q \leq 2^{28}$
average message size: ≤ 16 $16 * \delta = 1536$ $\Rightarrow r \leq 2^{32}$

$\frac{qr+q^2}{2^{\delta+1}} \approx 2^{60}/2^{97} \approx 2^{-37}$
$\frac{qr+q^2}{2^{\delta+1}} + \frac{1}{2^\tau} \approx 2^{-37} + 2^{-32} \approx 2^{-32}$

H M_i

$q' = q + r$ μ
$\mu \leq 2^\tau - 3$
$\mu \approx 2^\tau$

$$\frac{(5\mu^2 + 1)q'}{2^n} \leq 2^{-64}.$$

2^{-37} 2^{-32}

$F'(H)$ M

– H $\lceil |H|/128 \rceil$
–
  - $|M| \leq 96$
  - $|M|$ $97 \leq |M| \leq 128$ $128 \leq |M| \leq 192$
  - $|M|/64$ $|M|/96$

	full computation	header has been preprocessed
EAX	$\left\lceil \frac{\lvert M\rvert}{128} \right\rceil + \left\lceil \frac{\lvert M\rvert}{128} \right\rceil + 1 + \left\lceil \frac{\lvert H\rvert}{128} \right\rceil$	$\left\lceil \frac{\lvert M\rvert}{128} \right\rceil + \left\lceil \frac{\lvert M\rvert}{128} \right\rceil + 1$
CCFB+H	$\left\lceil \frac{\lvert M\rvert}{96} \right\rceil + 1 + \left\lceil \frac{\lvert H\rvert}{128} \right\rceil$	$\left\lceil \frac{\lvert M\rvert}{96} \right\rceil + 1$

$|M|$ = message length $|H|$ = header length nonce-length ≤ 128 bit

Table 2. Performance of AES-based EAX and CCFB+H in # of AES calls.

Acknowledgement

References

1. M. Bellare, P. Rogaway, D. Wagner. EAX: a conventional authenticated encryption mode. FSE 2004.
2. M. Bellare, P. Rogaway, D. Wagner. EAX: a conventional authenticated encryption mode. Extended version of [1]. http://www.cs.berkeley.edu/~daw/papers/eax-fse04.ps
3. M. Bellare, C. Namprempre. Authenticated Encryption: relations among notions and analysis of the generic composition paradigm. Asiacrypt 00.

4. V. Gligor, P. Donescu. Fast encryption and authentication: XCBC encryption and XECB authentication modes. FSE 01.
5. T. Iwata and K. Kurosawa. OMAC: One-Key CBC MAC. Fast Software Encryption, FSE 03.
6. T. Iwata and K. Kurosawa. OMAC: One-Key CBC MAC. Extended Version of [5]. http://crypt.cis.ibaraki.ac.jp/omac/docs/omac.pdf
7. C Jutla. Encryption modes with almost free message integrity. Eurocrypt 01.
8. J. Katz, M. Yung. Unforgeable encryption and adaptively secure modes of operation. FSE 00.
9. T. Kohno, J. Viega, D. Whiting. CWC: a high performance conventional authenticated encryption mode. FSE 04.
10. T. Kohno, J. Viega, D. Whiting. CWC: a high performance conventional authenticated encryption mode. Extended version of [9]. http://eprint.iacr.org/2003/106.ps.gz
11. D. McGrew, J. Viega. The Security and Performance of the Galois/Counter Mode of Operation (Full Version). http://eprint.iacr.org/2004/193
12. P. Rogaway. Authenticated encryption with associated data. Computer and Communications Security, ACM, 2002.
13. P. Rogaway, M. Bellare, J. Black, T. Krovetz. OCB: A block-cipher mode of operation for efficient authenticated encryption. Computer and Communications Security, ACM, 2001.
14. P. Rogaway, D. Wagner. A critique of CCM. Unpublished manuscript. February 2, 2003. http://www.cs.berkeley.edu/~daw/papers/ccm.html
15. D. Whiting, R. Hously, N. Ferguson. Counter with CBC-MAC (CCM). Submission to NIST.

Appendix: Deferred Proof and Figures

Theorem 2 (Information-Theoretic Authenticity of CCFB)
CCFB encryption, using a random F, is

$\left(\frac{qr}{2^{\delta+1}} + \frac{1}{2^{\tau}}\right)$*-authentic with respect to nonce-respecting adversaries and*

$\left(\frac{q(r+q)}{2^{\delta+1}} + \frac{1}{2^{\tau}}\right)$*-authentic with respect to nonce-randomising adversaries.*

Proof. *without*
$1/2^{\tau}$
A_j^i
q $T^i = A_1^i \oplus \bigoplus_{2 \le j \le m_i+1} A_j^i$ $1 \le i \le q$
2^{τ} T^i A_j^i $(j \ge 1)$
2^{τ}

A_1^i q

(C_0, C) $C = (C_1, \ldots, C_{m-1}, C_m, T)$ C
C^i

$$T = A_1 \oplus \bigoplus_{2 \le j \le m+1} A_j$$

q

$T^i = \ldots$ A_j^i A_j $j \ge 1$
$1 \le i \le q$
$D_0 \notin \{D_0^1, \ldots, D_0^q\}$ [8] A_1
$D_0 = D_0^1$ $C_0 = C_0^1$ $A_1^1 = A_1$
T T^1

$$T^1 \oplus T = \bigoplus_{2 \le j \le m_1+1} A_j^1 \oplus \bigoplus_{2 \le j \le m+1} A_j.$$

$A_j^1 = A_j$ $D_j = D_j^k$

$$A^* = \{A_j^1 | 2 \le j \le m_1 + 1, D_j^1 \ne D_j\} \cup \{A_j | 2 \le j \le m + 1, D_j \ne D_j^1\}$$

$T^1 \oplus T$

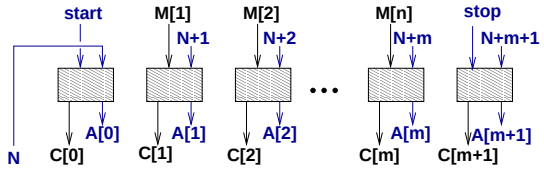
$$T^1 \oplus T = \bigoplus_{A \in A^*} A.$$

$C \ne C^i$ A^* [9] $i > 1$ $T^i = \ldots$
$i > 1$ $T^1 \oplus T$ A_1^i
T^i
q T^i
$T = A_1 \oplus \bigoplus_{2 \le j \le m+1} A_j$ $T \in$ 2^τ
T $T \in$ 2^τ
$1/2^\tau$ $\square$

[8] The inputs D_j for F are defined similarly to the D_j^i in Equation 1.
[9] Technically, $C \ne C^i$ could mean $T \ne T^i$, $m = m_i$, and $C_j = C_j^i$ for $1 \le j \le m$. But this type of forgery would fail: $A^* = \{\}$ and thus $T^1 \oplus T = 0$, contradicting $T \ne T^i$.

Algorithm:
Input: $N \in \{0,1\}^{\delta}$ $C \in \{0,1\}^{*}$ $\tau + 1 \leq |C| \leq (2^{\tau} - 3)\delta + \tau$
First pass:
C $(C_1, \ldots, C_m, T)$
$|C_1| = \cdots = |C_{m-1}| = \delta$ $|C_m| \in \{1, \ldots, \delta\}$ $|T| = \delta$
$C_0 := N$
$1 \leq i \leq m-1$ $(\ , A_i) := F(C_{i-1}, \langle i \rangle_{\tau})$
$M_i := \ \oplus C_i$
$(\ , A_m) := F(C_{m-1}, \langle m \rangle_{\tau})$
$|C_m| = \delta$ $d := 1;$ $:= ()(*\ \ *);$
$d := 2;$ $:= (1||0^{\delta - |C_m| - 1});$
$M_m := \ _{|C_m|}(\ ) \oplus C_m;$
$C' := \ \oplus (M_m||\ );$
$(\ , A_{m+1}) := F(C', \langle m + d \rangle_{\tau})$
Second pass:
$T' := A_1 \oplus \cdots \oplus A_{m+1}$
Output: $T = T'$
$(M_1, \ldots, M_m)$
$M_1 \ \ M_{m-1} \in \{0,1\}^{\delta}$ $M_m \in \{0,1\}^{|M_m|}$

Fig. 6. CCFB decryption under $F : \{0,1\}^{\delta} \times \{0,1\}^{\tau} \to \{0,1\}^{\delta} \times \{0,1\}^{\tau}$.



plaintext: $(M_1, \ldots M_m) \in \{0,1\}^{\delta m}$, $M_i \notin \{\text{start}, \text{stop}\}$;
nonce: $N \in \{0,1\}^{\tau}$; ciphertext: $((C_0, A_0), \ldots, (C_{m+1}, A_{m+1})) \in \{0,1\}^{n(m+2)}$

Fig. 7. RPC encryption under a permutation