**CTR + CBC-MAC (CCM)**

Petros Potikas  
NTUA  
Number Theory and Cryptography

---

**Intro**

- About block cipher and combined modes  
- Authenticated encryption  
- Nonce-using symmetric encryption scheme

---

**Attractive properties**

1. Certain parts of message are authenticated only and not encrypted.  
2. The underlying block cipher is used only in the forward “encryption” direction, e.g. an arbitrary pseudo-random function can be used.  
3. Uses well-known technologies (+20 years)  
4. All intellectual property rights are public released.

---

**Description**

- CTR + CBC-MAC provides privacy and authenticity  
- CCM is based on a pseudo-random function

\[
E : \{0,1\}^{k_0} \times \{0,1\}^{k_b} \rightarrow \{0,1\}^{k_s}
\]

- \(k_0\): key bit length  
- \(k_b\): block bit length

---

**Overview**

- The parties exchange a secret key, chosen uniformly at random from the set \(\{0,1\}^{k_0}\)  
- Input: \((N, H, M)\)  
- \(N\): nonce, fixed bit length \(k_n < k_b\)  
- \(H\): header, only authenticated, not encrypted  
- \(M\): message, authenticated and encrypted  
- An authentication tag \((k_r \leq k_b)\) is derived via CBC-MAC and encrypted together with the message via CTR

Output: A ciphertext of length \(|M| + k_t\)
Overview (cont’d)

- Nonce is non-repeating (“fresh”) during the lifetime of a key.
- Restrictions on input:
  - Lengths of header and message might be upper-bounded by a constant
  - A multiple of 8 or the block length

\[ V = \{ \text{all valid inputs} \} \]

\( (N, H, M) \)

\[ \pi(i, N, H, M) \neq \pi(i', N', H', M') \]

\( B_0 \)

\( B_0 \)

CTR encryption

Input \( (N, H, M) \), generates input blocks of CTR

\[ A_i = \pi(i, N, H, M) \]

\( k \), leftmost bits of \( E_k(A_i) \) are used for encryption of the tag, while the \( |M| \) leftmost bits of the string \( E_k(A_0), E_k(A_1), E_k(A_2), \ldots \) are used for the encryption of the message \( |M| \)

CBC-MAC computation

- Encoding function \( \beta \)

\[ \beta: V \rightarrow W^* \]

where \( W = \{0, 1 \}^k \)

- Output: \( B = B_0 \cdot B_1 \cdot \ldots \cdot B_r \)

- A tag \( T \) is derived by applying CBC-MAC to these blocks.

- \( B_0 \) is the CBC-MAC pre-IV

CTR encryption

- Encrypt the message \( M \) and the CBC-MAC tag \( T \).

- Use a CTR block-generator \( \pi = \pi(i, N, H, |M|) \) such that \( N \) and counter \( i \) can be uniquely determined by the CTR block generator.

\[ N \in \{0, 1 \}^k \quad \text{and} \quad 0 \leq i \leq \mu_{max} \quad \text{where} \quad \mu_{max} \quad \text{is scheme-specific parameter, determine the maximum number of message blocks} \quad \text{number of blocks} \leq \mu_{max} \cdot 2^k \]

Overview (cont’d)

- Restrictions on input:

  - Lengths of header and message might be upper-bounded by a constant
  - A multiple of 8 or the block length

\[ V = \{ \text{all valid inputs} \} \]

\( (N, H, M) \)

\[ \pi(i, N, H, M) \neq \pi(i', N', H', M') \]

\( B_0 \)

\( B_0 \)

CTR encryption

- Let \( \beta_0(N, H, M) \) be equal to the first block \( B_0 \) of \( \beta(N, H, M) \). We require that

\[ \pi(i, N, H, M) \neq \beta_0(N', H', M') \]

for all valid \( (N, H, M), (N', H', M') \) and \( 0 \leq i \leq \mu_{max} \)

- The nonce being non-repeating implies that all CTR input blocks \( A_i \), and all CBC-MAC pre-IV’s \( B_0 \) used during the lifetime of a key are distinct.
CCM Specification

- CBC-MAC computation:
  - Let $B_0, B_1, \ldots, B_r = \beta(N, H, M)$
  - Let $Y_0 = E_K(B_0)$
  - For $0 \leq i \leq r$, let $Y_i = E_K(Y_{i-1} \oplus B_i)$
  - Let $T$ be equal to the $k_1$ leftmost bits of $Y_r$

- CTR encryption:
  - Let $\mu = \lfloor |M|/k_0 \rfloor$
  - For $0 \leq i \leq \mu$, $A_i = \pi(i, N, H, M)$
  - Let $S$ be equal to the $|M|$ leftmost bits of $S_1, \ldots, S_m$ and $S'$ the $|T|$ leftmost bits of $S_0$
  - Let $C = [M \oplus S], [T \oplus S']$

Example (cont'd)

- Block cipher: AES, proposed in IEEE 802.11
- Block length $k_0 = 128$
- Key length, $k_0 = 128, 192, 256$
- All strings are of length a multiple of 8
- $k_1 = 32(16 \ldots 128$
- $k_2 = 56(8) \ldots 112$
- Number of octets in a message $\leq 2^{120-k_1}-1$
- $k_{max} = 120-k_n$, $\mu_{max} = 2^{k_{max}}-4$
- Each block contains $2^4$ octets
- Input is valid if $N \in \{0,1\}^{k_0}$, $0 \leq |H|/8 < 2^{16}$, $0 \leq |M|/8 < 2^{k_{max}}$

Example (cont’d)

- $N$ is uniquely determined by $B_0$
- $\beta$ is prefix free
- Input $(N, H, M)$ is uniquely determined by $\beta(N, H, M)$, because of the inclusion of the octet length of $H$ and $M$

Example (Decryption)

CCM decryption of a ciphertext $C$ with nonce $N$ and header $H$:
1. Apply the reverse of step 2 to $C$ to obtain a message $M$ and a CBC-MAC tag $T$ (the CTR block generator is applied on $(N, H, |C| - k_1)$).
2. Apply CBC-MAC to the obtained message $M$ to get a tag $T'$. If $T = T'$, then $T$ is valid, and $M$ is output. Otherwise, $T$ is not valid, and an error is output.

Note: The decryption operation must not release the message or any part of it, until the the tag has been verified.

Example (cont’d)

- $B_0 = (0b)_2, (k/16-1)_3, (k_{max}/8-1)_3, (N)_{k_2}, (|M|/8)_{k_{max}}$
  - $b = 0$, if $H$ is the empty string, 1 o.w. and the two leftmost octets of $B_0$, are equal to the $|H|/8$.
  - Let $L_H = [|H|/8]_{16}$ if $|H| > 0$, o.w. the empty string then $\beta(N, H, M) = B_0 \cdot L_H \cdot H \cdot Z_1 \cdot M \cdot Z_2$
  - where $Z_1$ and $Z_2$ are strings with zeros, such that $L_H \cdot H \cdot Z_1$ and $M \cdot Z_2$ are multiples of the block length 128.

Example (cont’d)

- The CTR block generator is defined as $\pi(i, N) = (00000)_2, (k_{max}/8-1)_3, (N)_{k_2}, (i)_{k_{max}}$

This cannot be equal to a CBC-MAC pre-IV $B_0$; the first five bits in $B_0$ are not all equal to zeros, since $(k/16-1)$ is nonzero.
Security analysis - Privacy

Goal of the adversary: distinguish the ciphertexts from random gibberish (a bit string chosen uniformly at random from the set of all possible bit strings of a specified length)

N is required to be fresh, so CTR input blocks and the CBC-MAC pre-IV's are new and distinct.

The output ciphertext is very close to random gibberish even if the adversary knows the plaintext.

Two attacks:
I. A “birthday” attack: All input blocks of CTR are distinct, so no collisions appear among the output blocks, but true random gibberish will contain block collisions, with probability $O(q^2)2^{-b}$ ($q$ number of applications of the block cipher)
II. An anomaly can occur inside the CBC-MAC computations (e.g. an internal collision or a tag to coincide with some CTR output block). This happens with probability $O(q^2)2^{-b}$

Security analysis - Authenticity

Possible to tell anything non-trivial about internal block of the CBC-MAC computation has probability $O(q^2)2^{-b}$ even if all plaintexts are known.

Unless $q$ is very large, the adversary knows close to nothing about the internal block, so modifying any previous encryption query, results in unpredictable modification of the tag.

As $\beta$ is prefix-free, any forgery attempt $B_0.B_1.\cdots$ is unique. If there is a previous encryption query, then they must differ at some point.

Guess the tag: probability less than $2^{-k}$.