Secure Message Authentication Codes against Related-Key Attack

Rishiraj Bhattacharyya Arnab Roy

March 12, 2013
Outline

1. Background
   - Related-Key Attack
   - Message Authentication Codes

2. Related-Key Security of MAC
   - MAC against RK Adversary
   - RKD class
   - Attack against MAC

3. Related-Key Secure MAC
   - First Step
   - Design at a High Level
   - Construction
Outline

1 Background
   • Related-Key Attack
   • Message Authentication Codes

2 Related-Key Security of MAC
   • MAC against RK Adversary
   • RKD class
   • Attack against MAC

3 Related-Key Secure MAC
   • First Step
   • Design at a High Level
   • Construction
Adversary can make queries to the primitive with secret key as well as with some function of the secret key.
Adversary can make queries to the primitive with secret key as well as with some function of the secret key
Adversary can make queries to the primitive with secret key as well as with some function of the secret key.

\[ f(k, m) \]

\[ \phi: K \rightarrow K \] is the RKD function chosen by adversary.
Adversary can make queries to the primitive with secret key as well as with some function of the secret key.

\[
\begin{align*}
\text{Adversary} & \quad m \\
\downarrow f(k, m) \quad \downarrow \\
\text{Primitive} & \quad m, \phi \\
\text{Adversary} & \quad f(\phi(k), m)
\end{align*}
\]
Adversary can make queries to the primitive with secret key as well as with some function of the secret key.

\[ m \xrightarrow{f(k, m)} m, \phi \xleftarrow{f(\phi(k), m)} \]

\( \phi : \mathcal{K} \rightarrow \mathcal{K} \) is the RKD function chosen by adversary.
Proposed by Biham in 1993
Many well known attacks, including the attack on AES
Formal theoretical model introduced by Bellare and Kohno in 2003
A series of work in recent past (Bellare Cash 2010, Bellare Cash Miller 2011)
Related-key attack on HMAC AsiaCrypt 2012.
Outline

1. Background
   - Related-Key Attack
   - Message Authentication Codes

2. Related-Key Security of MAC
   - MAC against RK Adversary
   - RKD class
   - Attack against MAC

3. Related-Key Secure MAC
   - First Step
   - Design at a High Level
   - Construction
Message Authentication Codes: \( F : \mathcal{K} \times \mathcal{D} \rightarrow \mathcal{R} \)
Message Authentication Codes: $F : \mathcal{K} \times \mathcal{D} \rightarrow \mathcal{R}$
Message Authentication Codes: $F : \mathcal{K} \times \mathcal{D} \rightarrow \mathcal{R}$

\[ m_1 \leftrightarrow F(k, m_1) \]
Message Authentication Codes: $F: \mathcal{K} \times \mathcal{D} \rightarrow \mathcal{R}$

- $m_1 \xrightarrow{F(k, m_1)} m_q \xleftarrow{F(k, m_q)}$

- $m^* \in Q$
Message Authentication Codes: $F: \mathcal{K} \times \mathcal{D} \rightarrow \mathcal{R}$

- $m_1 \xrightarrow{F(k, m_1)} m_q$
- $(m^*, \sigma^*): m^* \notin \mathcal{Q}$
Outline

1. Background
   - Related-Key Attack
   - Message Authentication Codes

2. Related-Key Security of MAC
   - MAC against RK Adversary
   - RKD class
   - Attack against MAC

3. Related-Key Secure MAC
   - First Step
   - Design at a High Level
   - Construction
Outline

1. Background
   - Related-Key Attack
   - Message Authentication Codes

2. Related-Key Security of MAC
   - MAC against RK Adversary
   - RKD class
   - Attack against MAC

3. Related-Key Secure MAC
   - First Step
   - Design at a High Level
   - Construction
MAC against RK Adversary

Message Authentication Codes: $F : \mathcal{K} \times \mathcal{D} \rightarrow \mathcal{R}$
MAC against RK Adversary

- Message Authentication Codes: $F : \mathcal{K} \times \mathcal{D} \rightarrow \mathcal{R}$
MAC against RK Adversary

- Message Authentication Codes: $F : \mathcal{K} \times \mathcal{D} \rightarrow \mathcal{R}$

\[ (m_1, \phi) \quad \leftrightarrow \quad F(\phi(k), m_1) \]
MAC against RK Adversary

Message Authentication Codes: $F : \mathcal{K} \times \mathcal{D} \rightarrow \mathcal{R}$

- $(m_1, \phi)$
  - $F(\phi(k), m_1)$
- $(m_q, \phi)$
  - $F(\phi(k), m_q)$
**MAC against RK Adversary**

Message Authentication Codes: $F : \mathcal{K} \times \mathcal{D} \rightarrow \mathcal{R}$

- $(m_1, \phi) \leftarrow F(\phi(k), m_1) \rightarrow (m_q, \phi)$
- $(m_q, \phi) \leftarrow F(\phi(k), m_q) \rightarrow (m^*, \sigma^* = F(k, m^*))$
MAC against RK Adversary

- **Message Authentication Codes**: \( F : \mathcal{K} \times \mathcal{D} \rightarrow \mathcal{R} \)

\[
\begin{align*}
(m_1, \phi) & \quad \iff \quad F(\phi(k), m_1) \\
F(\phi(k), m_q) & \quad \iff \quad (m_q, \phi)
\end{align*}
\]

\( (m^*, \sigma^* = F(k, m^*)) \)

\( (m^*, \text{id}) \notin Q \)
MAC against RK Adversary

- **Message Authentication Codes:** \( F : \mathcal{K} \times \mathcal{D} \rightarrow \mathcal{R} \)

\[
\begin{align*}
(m_1, \phi) & \quad \text{left} \quad \leftrightarrow \quad \text{right} \quad F(\phi(k), m_1) \\
& \quad \text{left} \quad \leftrightarrow \quad \text{right} \quad F(\phi(k), m_q) \\
(m_q, \phi) & \quad \text{left} \quad \leftrightarrow \quad \text{right} \quad F(\phi(k), m_q)
\end{align*}
\]

\( (m^*, \sigma^* = F(k, m^*)) \)

- \((m^*, \text{id}) \notin \mathcal{Q}\) or \((m^*, \phi) \notin \mathcal{Q}\)
Outline

1 Background
   - Related-Key Attack
   - Message Authentication Codes

2 Related-Key Security of MAC
   - MAC against RK Adversary
   - RKD class
   - Attack against MAC

3 Related-Key Secure MAC
   - First Step
   - Design at a High Level
   - Construction
For arbitrary RKD class, it is impossible to get provable security against Related Key Attack. (Bellare Kohno 2003).

For prf, RKD class should be collision resistant and entropy preserving (Bellare Kohno 2003); trivial attacks using constant RKD functions.
A closer look at the RKD class

- For arbitrary RKD class, it is impossible to get provable security against Related Key Attack. (Bellare Kohno 2003).
- For prf, RKD class should be collision resistant and entropy preserving (Bellare Kohno 2003); trivial attacks using constant RKD functions.

Theorem

If $F$ is a MAC then $F$ is related-key unforgeable against constant RKD.
Outline

1. Background
   - Related-Key Attack
   - Message Authentication Codes

2. Related-Key Security of MAC
   - MAC against RK Adversary
   - RKD class
   - Attack against MAC

3. Related-Key Secure MAC
   - First Step
   - Design at a High Level
   - Construction
Related-Key Attack against popular MACs

\[
\begin{align*}
E_{k_0}(m_0) & \rightarrow E_{k_0}(m_1) \\
E_{k_0}(m_1) & \rightarrow E_{k_0}(m_2) \\
\phi_i(k_0) & = k_0 \oplus i(M \oplus i, \sigma) \\
\end{align*}
\]
Related-Key Attack against popular MACs

\[ F(k_0, k_1 \oplus i, M) = F(k_0, k_1, M \oplus i) \]
Related-Key Attack against popular MACs

\[ F(k_0, k_1 \oplus i, M) = F(k_0, k_1, M \oplus i) \]

\[ \phi_i(k) = k \oplus i \]
Related-Key Attack against popular MACs

\[
F(k_0, k_1 \oplus i, M) = F(k_0, k_1, M \oplus i)
\]

\[
\phi_i(k) = k \oplus i
\]

\[
(M \oplus i, \sigma)
\]
Summary of Attacks

- XCBC is not related key secure
- Same attack can be applied to TMAC with little modification
- We also show related-key attacks against ECBC and FCBC
Outline

1. Background
   - Related-Key Attack
   - Message Authentication Codes

2. Related-Key Security of MAC
   - MAC against RK Adversary
   - RKD class
   - Attack against MAC

3. Related-Key Secure MAC
   - First Step
   - Design at a High Level
   - Construction
Outline

1. Background
   - Related-Key Attack
   - Message Authentication Codes

2. Related-Key Security of MAC
   - MAC against RK Adversary
   - RKD class
   - Attack against MAC

3. Related-Key Secure MAC
   - First Step
   - Design at a High Level
   - Construction
Technical Tool: ICTPR Hash Function

- Identity Collision Resistant Hash
Technical Tool: ICTPR Hash Function

- Identity Collision Resistant Hash
Identity Collision Resistant Hash

\[ m_1, \phi_1 \]

\[ H(\phi_1(k), m_1) \]
Technical Tool: ICTPR Hash Function

- Identity Collision Resistant Hash

\[\begin{align*}
H(\phi_1(k), m_1) &\quad \leftrightarrow \quad m_1, \phi_1 \\
H(\phi_q(k), m_q) &\quad \leftrightarrow \quad m_q, \phi_q
\end{align*}\]
Technical Tool: ICTPR Hash Function

- Identity Collision Resistant Hash

\[ H(\phi_1(k), m_1) = H(\phi_q(k), m_q) \]

\( (m_i, m_j): H(\phi_i(k), m_i) = H(k, m_j), i < j \)
Technical Tool: ICTPR Hash (contd.)

**Target Preimage Resistant Hash**
Technical Tool: ICTPR Hash (contd.)

- Target Preimage Resistant Hash
Technical Tool: ICTPR Hash (contd.)

- Target Preimage Resistant Hash

\[
\{z_1, z_2, \ldots, z_t\} \in \mathcal{R} \text{ and } \Phi
\]
**Technical Tool: ICTPR Hash (contd.)**

- **Target Preimage Resistant Hash**

\[
\{z_1, z_2, ..., z_t\} \in \mathcal{R} \text{ and } \Phi
\]

\[
m_1, \phi_1 \\
H(\phi_1(k), m_1)
\]
Technical Tool: ICTPR Hash (contd.)

- Target Preimage Resistant Hash

\[ \{z_1, z_2, \ldots, z_t\} \in \mathcal{R} \text{ and } \Phi \]

\[
\begin{array}{c}
\text{Devil} & \quad & \text{Penguin} \\
\text{m_1, \phi_1} & \quad & \text{m_q, \phi_q} \\
H(\phi_1(k), m_1) & \quad & H(\phi_q(k), m_q)
\end{array}
\]
Target Preimage Resistant Hash

\[ \{z_1, z_2, \ldots, z_t\} \in \mathcal{R} \text{ and } \Phi \]

\[ m_1, \phi_1 \]

\[ H(\phi_1(k), m_1) \]

\[ m_q, \phi_q \]

\[ H(\phi_q(k), m_q) \]

\[ m^*: H(m^*, k) = z_i \]
Outline

1. Background
   - Related-Key Attack
   - Message Authentication Codes

2. Related-Key Security of MAC
   - MAC against RK Adversary
   - RKD class
   - Attack against MAC

3. Related-Key Secure MAC
   - First Step
   - Design at a High Level
   - Construction
ICTPR hash $H : \mathcal{K}_1 \times \{0, 1\}^* \rightarrow \mathcal{D}$ over $\Phi_1$

$F : \mathcal{K}_2 \times \mathcal{D} \rightarrow \mathcal{R}$ is weak RK unforgeable MAC over $\Phi_2$ with identity fingerprint $w_1, w_2, .., w_d$

Theorem

*With the above mentioned $F$ and $H$, $G : (\mathcal{K}_1 \times \mathcal{K}_2) \times \{0, 1\}^* \rightarrow \mathcal{R}$ defined as

$$G(k_1, k_2, m) = F(k_1, H(k_2, m \parallel F(k_1, w_1) \parallel F(k_1, w_2) \parallel \cdots \parallel F(k_1, w_d)))$$

is related-key unforgeable against chosen message attack, over component induced RKD set $\Phi_1 \times \Phi_2$*
Outline

1. Background
   - Related-Key Attack
   - Message Authentication Codes

2. Related-Key Security of MAC
   - MAC against RK Adversary
   - RKD class
   - Attack against MAC

3. Related-Key Secure MAC
   - First Step
   - Design at a High Level
   - Construction
Towards Main Construction

The construction of

\[ G(k_1, k_2, m) = F(k_1, H(k_2, m \| F(k_1, w_1) \| F(k_1, w_2) \| \cdots \| F(k_1, w_d))) \]

is in the line of previous work.
Towards Main Construction

- The construction of

\[ G(k_1, k_2, m) = F(k_1, H(k_2, m \parallel F(k_1, w_1) \parallel F(k_1, w_2) \parallel \cdots \parallel F(k_1, w_d))) \]

is in the line of previous work.

- **Major difference:** ICTPR Hash (instead of the unkeyed collision resistant hash function with tailor made range used by Bellare and Cash)
Towards Main Construction

The construction of

\[ G(k_1, k_2, m) = F(k_1, H(k_2, m\|F(k_1, w_1)\|F(k_1, w_2)\|\cdots\|F(k_1, w_d))) \]

is in the line of previous work.

**Major difference:** ICTPR Hash (instead of the unkeyed collision resistant hash function with tailor made range used by Bellare and Cash)

Next we construct ICTPR Hash function from FIL-RK unforgeable function
Towards Main Construction

- The construction of

\[ G(k_1, k_2, m) = F(k_1, H(k_2, m\|F(k_1, w_1)\|F(k_1, w_2)\|\cdots\|F(k_1, w_d))) \]

is in the line of previous work.

- **Major difference**: ICTPR Hash (instead of the unkeyed collision resistant hash function with tailor made range used by Bellare and Cash)

- Next we construct ICTPR Hash function from FIL-RK unforgeable function

- This is done in two steps:
Towards Main Construction

The construction of

\[ G(k_1, k_2, m) = F(k_1, H(k_2, m||F(k_1, w_1)||F(k_1, w_2)||\cdots||F(k_1, w_d))) \]

is in the line of previous work.

**Major difference:** ICTPR Hash (instead of the unkeyed collision resistant hash function with tailor made range used by Bellare and Cash)

Next we construct ICTPR Hash function from FIL-RK unforgeable function

This is done in two steps:

1. VIL ICTPR Hash from a FIL ICTPR compression function
Towards Main Construction

The construction of

\[ G(k_1, k_2, m) = F(k_1, H(k_2, m \| F(k_1, w_1) \| F(k_1, w_2) \| \cdots \| F(k_1, w_d))) \]

is in the line of previous work.

**Major difference:** ICTPR Hash (instead of the unkeyed collision resistant hash function with tailor made range used by Bellare and Cash)

Next we construct ICTPR Hash function from FIL-RK unforgeable function

This is done in two steps:

1. VIL ICTPR Hash from a FIL ICTPR compression function
2. FIL ICTPR Hash from FIL RK-MAC
VIL-ICTPR Hash from ICTPR Compression Function

\[ H = pfNi^{H'}(k, m) \]
Lemma:

If $H'$:

\[ H = pfNI^{H'}(k, m) \]

is ICTPR, then $H$:

\[ H : K \times \{0, 1\}^{2^n} \rightarrow \{0, 1\}^n \]

is ICTPR.
VIL-ICTPR Hash from ICTPR Compression Function

\[ H = pfNl^{H'}(k, m) \]

IV \[ \xrightarrow{} H' \xrightarrow{} H' \xrightarrow{} H' \xrightarrow{} H' \xrightarrow{} H' \xrightarrow{} C^H(m) \]

Lemma

If \( H' : \mathcal{K} \times \{0, 1\}^{2n} \rightarrow \{0, 1\}^n \) is ICTPR then \( H : \mathcal{K} \times \{0, 1\}^* \rightarrow \{0, 1\}^n \) is ICTPR.
Related-Key Secure MAC Construction

FIL-ICTPR Hash using FIL RK-MAC

- We take $H'_{k_1, k_2}(x_1, x_2) = F(k_1, x_1) \oplus F(k_2, x_2)$ where $F: \mathcal{K} \times \{0, 1\}^n \rightarrow \{0, 1\}^n$ RK unforgeable.

Lemma

If $F$ is RK unforgeable over RKD set $\Phi$ with identity fingerprint $w_1, w_2, \ldots, w_d$ then $H = pfNI^{H'}$ is ICTPR over the RKD set $\psi : \{0, 1\}^\kappa \times \{0, 1\}^\kappa \rightarrow \{0, 1\}^\kappa$ defined as $((\Phi \setminus \{id\}) \times \Phi) \cup (id, id)$
Modified Enciphered CBC preserves related-key unforgeability.
Constructions using Collision Resistant Hash Function

- $F : \mathcal{K}_2 \times \mathcal{D} \rightarrow \mathcal{R}$ is key-homomorphic MAC over $\Phi$ with identity fingerprint $w_1, w_2, \ldots, w_d$
- Collision Resistant hash $H : \{0, 1\}^* \rightarrow \mathcal{D} \setminus \{w_1, w_2, \ldots, w_d\}$

Theorem

$$G(k_1, k_2, m) = F(k_1, H(k_2, m || F(k_1, w_1) || F(k_1, w_2) || \cdots || F(k_1, w_d)))$$

is related-key unforgeable over $\Phi$
Constructions using Collision Resistant Hash Function

- $F : \mathcal{K}_2 \times \mathcal{D} \rightarrow \mathcal{R}$ is key-homomorphic MAC over $\Phi$ with identity fingerprint $w_1, w_2, .., w_d$
- Collision Resistant hash $H : \{0, 1\}^* \rightarrow \mathcal{D} \setminus \{w_1, w_2, .., w_d\}$

**Theorem**

$$G(k_1, k_2, m) = F(k_1, H(k_2, m\|F(k_1, w_1)\|F(k_1, w_2)\| \cdots \|F(k_1, w_d)))$$

is related-key unforgeable over $\Phi$

**Applications**

Two constructions from DDH/CDH assumptions for claw-free class.
Summary

- formal security definition for Related-Key MAC
- MAC is inherently RK unforgeable under constant RKD function
- Mode of operation for RK unforgeable functions
- Finally construction of RK unforgeable MAC from DDH assumption using collision resistant hash function
THANK YOU!