Multi-key Analysis of Tweakable Even-Mansour with Applications to Minalpher and OPP

Zhiyuan Guo[1,3] Wenling Wu[1,3] Renzhang Liu[2] Liting Zhang[1]

[1]TCA Laboratory, Institute of Software, Chinese Academy of Sciences, China

[2]Institute of Information Engineering, Chinese Academy of Sciences

[3]University of Chinese Academy of Sciences, China

gzhyuan@msn.cn

March 8, 2017

Outline

1. Introduction
2. Overview of Collision-Based Attacks on EM
3. Known-Plaintext Attack against TEM-1
4. Adaptive Chosen-Plaintext Attack on TEM-1
5. Application to AE Schemes Minalpher and OPP
6. Conclusion

1. Introduction
2. Overview of Collision-Based Attacks on EM
3. Known-Plaintext Attack against TEM-1
4. Adaptive Chosen-Plaintext Attack on TEM-1
5. Application to AE Schemes Minalpher and OPP
6. Conclusion

Single-key and Related-key Models in the Cryptanalysis

- Single-key setting
  - The adversary have access to the scheme equipped with a uniformly random key, without any knowledge of the key.
- Related-key setting
  - The scheme is equipped individually with related keys, whose values are secret but relations are known.

Single-key and Related-key Models in the Cryptanalysis

- Single-key setting
  - The adversary have access to the scheme equipped with a uniformly random key, without any knowledge of the key.
- Related-key setting
  - The scheme is equipped individually with related keys, whose values are secret but relations are known.

Even if the schemes show sufficient strength in such model, in practical applications, their keys need to be renewed within every key lifetime to avoid key guessing attacks by brute force.

Broadcast and Multi-user/key Models

- Broadcast setting
  - A single plaintext is encrypted for several times with distinct keys, and then sent to individual recipients.
- Multi-user setting
  - The same message is encrypted with multiple users, with each user having her own key.
- Multi-key setting
  - The messages need not be the same to different users.
  - The keys need not be corresponding to distinct users.

Broadcast and Multi-user/key Models

- Broadcast setting
  - A single plaintext is encrypted for several times with distinct keys, and then sent to individual recipients.
- Multi-user setting
  - The same message is encrypted with multiple users, with each user having her own key.
- Multi-key setting
  - The messages need not be the same to different users.
  - The keys need not be corresponding to distinct users.

Even for a single user, she may encrypt or authenticate messages with multiple keys due to the frequent re-keying operations.

☞

The multi-key setting is more close to practice than the broadcast and multi-user settings.

Tweakable Even-Mansour and TEM-1

The tweakable Even-Mansour construction generalizes the conventional Even-Mansour scheme

$$EM_{k_1,k_2}(m) = P(m \oplus k_1) \oplus k_2$$

through replacing round keys by strings derived from a master key and a tweak.

Tweakable Even-Mansour and TEM-1

The tweakable Even-Mansour construction generalizes the conventional Even-Mansour scheme

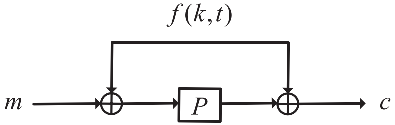
$$EM_{k_1,k_2}(m) = P(m \oplus k_1) \oplus k_2$$

through replacing round keys by strings derived from a master key and a tweak.

We give the multi-key analysis of TEM-1, a commonly used one-round tweakable Even-Mansour, which is expressed as

$$TEM(k,t,m) = f(k,t) \oplus P(f(k,t) \oplus m),$$

where k is a secret key, t is a tweak, and $f(k,t)$ is a function linear in k.



1. Introduction
2. Overview of Collision-Based Attacks on EM
3. Known-Plaintext Attack against TEM-1
4. Adaptive Chosen-Plaintext Attack on TEM-1
5. Application to AE Schemes Minalpher and OPP
6. Conclusion

The Basic Attack on Even-Mansour [FJM14]

For the single-key Even-Mansour

$$EM\left(m\right)=P\left(m\oplus k\right)\oplus k,$$

write two functions:

$$F_{EM}(m)=m\oplus EM(m),\quad F_{P}(m)=m\oplus P(m).$$

Note that any collision

$$F_{EM}(m)=F_{P}(m')$$

is equivalent to

$$m\oplus k\oplus P\left(m\oplus k\right)=m'\oplus P(m'),$$

which indicates $m\oplus m'$ is a likely candidate for the secret k.

The Basic Attack on Even-Mansour [FJM14]

As a result, the problem of attacking

$$EM\left(m\right) = P\left(m \oplus k\right) \oplus k$$

is reduced to the problem of finding a collision between

$$F_{EM}(m) = m \oplus EM(m), \quad F_P(m) = m \oplus P(m).$$

☞

After computing F_{EM} (resp. F_P) on D (resp. T) distinct random values, where $DT \approx 2^{|k|}$, one expects to find a required collision.

Distinguished Point Attack on Even-Mansour [FJM14]

For the single-key Even-Mansour $EM\left(m\right) = P\left(m \oplus k\right) \oplus k$, write two iterated functions:

$$\Phi_s = \Phi_{s-1} \oplus EM\left(\Phi_{s-1}\right) \oplus EM\left(\Phi_{s-1} \oplus \delta\right),$$

$$\phi_s = \phi_{s-1} \oplus P\left(\phi_{s-1}\right) \oplus P\left(\phi_{s-1} \oplus \delta\right),$$

where δ is a random non-zero constant and Φ_s (resp. ϕ_s) represents the s-th point on the on-line (resp. off-line) chain.

Distinguished Point Attack on Even-Mansour [FJM14]

For the single-key Even-Mansour $EM(m) = P(m \oplus k) \oplus k$, write two iterated functions:

$$\Phi_s = \Phi_{s-1} \oplus EM(\Phi_{s-1}) \oplus EM(\Phi_{s-1} \oplus \delta),$$

$$\phi_s = \phi_{s-1} \oplus P(\phi_{s-1}) \oplus P(\phi_{s-1} \oplus \delta),$$

where δ is a random non-zero constant and Φ_s (resp. ϕ_s) represents the s-th point on the on-line (resp. off-line) chain.

If $\Phi_i \oplus \phi_j = k$, then

$$\begin{aligned} EM(\Phi_i) \oplus EM(\Phi_i \oplus \delta) &= P(\Phi_i \oplus k) \oplus k \oplus P(\Phi_i \oplus k \oplus \delta) \oplus k \\ &= P(\phi_j) \oplus P(\phi_j \oplus \delta), \end{aligned}$$

implying $\Phi_{i+1} \oplus \phi_{j+1} = \Phi_i \oplus \phi_j = k$, i.e. two chains become **parallel**.

Distinguished Point Attack on Even-Mansour [FJM14]

A point is called **Distinguished Point**, if its filter meets the given condition.

- ϕ_j's filter: $P(\phi_j) \oplus P(\phi_j \oplus \delta)$.
- Φ_i's filter: $EM(\Phi_i) \oplus EM(\Phi_i \oplus \delta)$.

Distinguished Point Attack on Even-Mansour [FJM14]

A point is called **Distinguished Point**, if its filter meets the given condition.

- ϕ_j's filter: $P(\phi_j) \oplus P(\phi_j \oplus \delta)$.
- Φ_i's filter: $EM(\Phi_i) \oplus EM(\Phi_i \oplus \delta)$.

1. Construct off-line chains by using the iterated function ϕ.
    - Once a distinguished point ϕ_u is detected, store
      $$(P(\phi_u) \oplus P(\phi_u), \phi_u)$$
      and sort the table according to the first element.
2. Create an on-line chain by using the iterated function Φ.
3. As soon as
   $$EM(\Phi_{i'}) \oplus EM(\Phi_{i'} \oplus \delta) = P\left(\phi_{j'}\right) \oplus P\left(\phi_{j'} \oplus \delta\right),$$
   $\Phi_{i'} \oplus \phi_{j'}$ will be regarded as a candidate value of k.

Multi-user Collisions on Even-Mansour [FJM14]

—Suppose L users are all using single-key EM based on the same permutation, with each user $U^{(i)}$ having its own key $k^{(i)}$.

—Define two iterated functions:

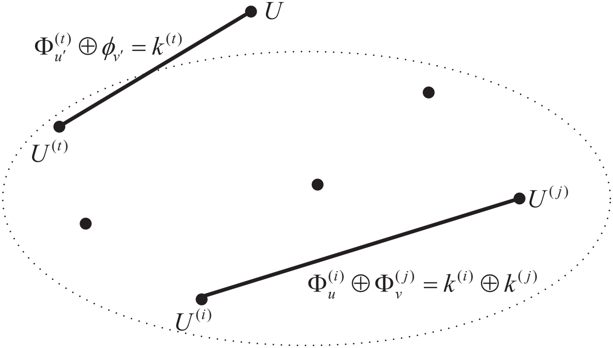
- $\phi_s = \phi_{s-1} \oplus P\left(\phi_{s-1}\right) \oplus P\left(\phi_{s-1} \oplus \delta\right).$
- $\Phi_s^{(i)} = \Phi_{s-1}^{(i)} \oplus EM^{(i)}\left(\Phi_{s-1}^{(i)}\right) \oplus EM^{(i)}\left(\Phi_{s-1}^{(i)} \oplus \delta\right).$

Multi-user Collisions on Even-Mansour [FJM14]

—Suppose L users are all using single-key EM based on the same permutation, with each user $U^{(i)}$ having its own key $k^{(i)}$.

—Define two iterated functions:

- $\phi_s = \phi_{s-1} \oplus P\left(\phi_{s-1}\right) \oplus P\left(\phi_{s-1} \oplus \delta\right).$
- $\Phi_s^{(i)} = \Phi_{s-1}^{(i)} \oplus EM^{(i)}\left(\Phi_{s-1}^{(i)}\right) \oplus EM^{(i)}\left(\Phi_{s-1}^{(i)} \oplus \delta\right).$


U
$\Phi_{u'}^{(t)} \oplus \phi_{v'} = k^{(t)}$
$U^{(t)}$
$U^{(j)}$
$\Phi_u^{(i)} \oplus \Phi_v^{(j)} = k^{(i)} \oplus k^{(j)}$
$U^{(i)}$

Multi-user Collisions on Even-Mansour [FJM14]

In fact, we are building a random graph based on Erdös - Rényi model.

Once the number of edges $cL/2$ is larger than the number of vertices L, there is with overwhelming probability a single giant component whose size is $(1 - t(c))L$, where

$$t(c) = \frac{1}{c} \sum_{k=1}^{\infty} \frac{k^{k-1}(ce^{-c})^k}{k!},$$

and c is a small constant.

For example, if $3L/2$ random edges are generated among the L vertices, it is very likely that 94% of these points are in a large component.

1. Introduction
2. Overview of Collision-Based Attacks on EM
3. Known-Plaintext Attack against TEM-1
4. Adaptive Chosen-Plaintext Attack on TEM-1
5. Application to AE Schemes Minalpher and OPP
6. Conclusion

Basic Idea of Our Known-Plaintext Attack

In a set of L independent keys, assume the number of message blocks under each key is D.

For any $k^{(i)}$, $1 \leq i \leq L$, the encryption of the s-th message block $m_s^{(i)}$ can be characterized as:

$$c_s^{(i)} \overset{\Delta}{=} TEM(k^{(i)}, s, m_s^{(i)}) = P(m_s^{(i)} \oplus f(k^{(i)}, s)) \oplus f(k^{(i)}, s).$$

Basic Idea of Our Known-Plaintext Attack

In a set of L independent keys, assume the number of message blocks under each key is D.

For any $k^{(i)}$, $1 \leq i \leq L$, the encryption of the s-th message block $m_s^{(i)}$ can be characterized as:

$$c_s^{(i)} \triangleq TEM(k^{(i)}, s, m_s^{(i)}) = P(m_s^{(i)} \oplus f(k^{(i)}, s)) \oplus f(k^{(i)}, s).$$

Searching for enough linear relations

- $m_u^{(i)} \oplus c_u^{(i)} = m_v^{(j)} \oplus c_v^{(j)}$

  $\Rightarrow m_u^{(i)} \oplus f(k^{(i)}, u)$ is a likely candidate value of $m_v^{(j)} \oplus f(k^{(j)}, v)$.

- $m_u^{(i)} \oplus c_u^{(i)} = P(x_v) \oplus x_v$

  $\Rightarrow m_u^{(i)} \oplus x_v$ is a likely candidate value of $f(k^{(i)}, u)$.

Procedure of Our Known-Plaintext Attack

1. For L independent keys, store $(m_s^{(i)}, s)$, $1 \leq s \leq D$, in an ordered table which is sorted according to the value of $m_s^{(i)} \oplus c_s^{(i)}$.
2. Build a graph whose vertices represent all of the keys. Search for collisions and add the corresponding edges.
3. Perform T off-line computations and search for matches from the table constructed in step (1).

Procedure of Our Known-Plaintext Attack

1. For L independent keys, store $(m_s^{(i)}, s)$, $1 \leq s \leq D$, in an ordered table which is sorted according to the value of $m_s^{(i)} \oplus c_s^{(i)}$.

2. Build a graph whose vertices represent all of the keys. Search for collisions and add the corresponding edges.

3. Perform T off-line computations and search for matches from the table constructed in step (1).

4. Verify $f(k^{(j)}, v)$ obtained in step (3) using a trial pair. If succeed, go to step (5). Otherwise return step (3).

5. Starting from the verified $f(k^{(j)}, v)$, we solve the system of linear equations which is generated in step (2).

Procedure of Our Known-Plaintext Attack

1. For L independent keys, store $(m_s^{(i)}, s)$, $1 \leq s \leq D$, in an ordered table which is sorted according to the value of $m_s^{(i)} \oplus c_s^{(i)}$.

2. Build a graph whose vertices represent all of the keys. Search for collisions and add the corresponding edges.

3. Perform T off-line computations and search for matches from the table constructed in step (1).

4. Verify $f(k^{(j)}, v)$ obtained in step (3) using a trial pair. If succeed, go to step (5). Otherwise return step (3).

5. Starting from the verified $f(k^{(j)}, v)$, we solve the system of linear equations which is generated in step (2).

Complexity of Our Known-Plaintext Attack

The expected number of collisions in step (2) is

$$Num = \binom{L}{2} \times D^2 \times \left[\frac{1}{2^n} + \left(1 - \frac{1}{2^n}\right) \times \frac{1}{2^n}\right].$$

The number of desirable collisions is

$$\widetilde{Num} = \frac{L(L-1)D^2}{2^{n+1}},$$

which means as long as we select parameters such that $\widetilde{Num} \geq cL$, almost all keys are in the component with correct edges.

1 Introduction

2 Overview of Collision-Based Attacks on EM

3 Known-Plaintext Attack against TEM-1

4 Adaptive Chosen-Plaintext Attack on TEM-1

5 Application to AE Schemes Minalpher and OPP

6 Conclusion

Target of Our Chosen-Plaintext Attack

We restrict the linear function f in TEM-1 to

$$f(k, s) = \beta\alpha^s k,$$

where α and β are two arbitrary invertible linear transformations.

The encryption of the s-th message block m_s can be expressed as:

$$TEM(k, s, m_s) = P(m_s \oplus \beta\alpha^s k) \oplus \beta\alpha^s k.$$

Target of Our Chosen-Plaintext Attack

We restrict the linear function f in TEM-1 to

$$f(k, s) = \beta\alpha^s k,$$

where α and β are two arbitrary invertible linear transformations.

The encryption of the s-th message block m_s can be expressed as:

$$TEM(k, s, m_s) = P(m_s \oplus \beta\alpha^s k) \oplus \beta\alpha^s k.$$

Such f has been widely used in the tweakable Even-Mansour schemes and tweakable block ciphers.

- MEM construction
- OCB2, COPA, ELmD, OTR, POET and SHELL.

Main Idea of Our Chosen-Plaintext Attack

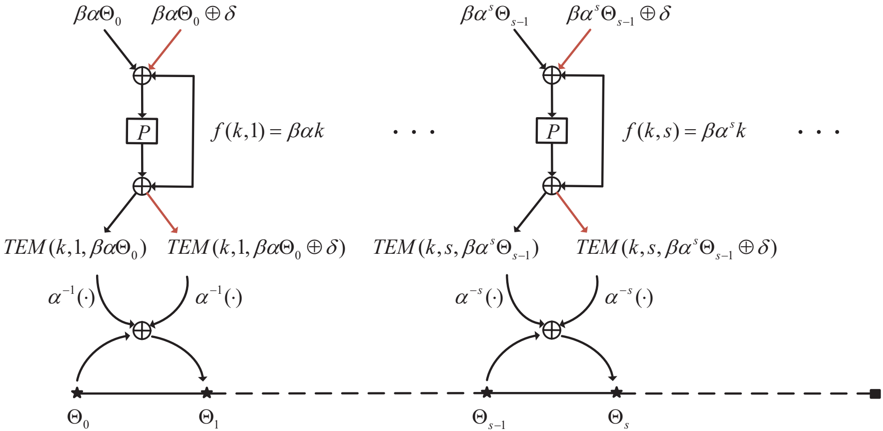
We randomly select a non-zero constant δ, and then define the on-line function as:

$$\Theta_s = \Theta_{s-1} \oplus \alpha^{-s} \cdot TEM\left(k, s, \beta\alpha^s\Theta_{s-1}\right) \oplus \alpha^{-s} \cdot TEM\left(k, s, \beta\alpha^s\Theta_{s-1} \oplus \delta\right).$$

Main Idea of Our Chosen-Plaintext Attack

We randomly select a non-zero constant δ, and then define the on-line function as:

$$\Theta_s = \Theta_{s-1} \oplus \alpha^{-s} \cdot TEM\left(k, s, \beta\alpha^s\Theta_{s-1}\right) \oplus \alpha^{-s} \cdot TEM\left(k, s, \beta\alpha^s\Theta_{s-1} \oplus \delta\right).$$



$\beta\alpha\Theta_0$
$\beta\alpha\Theta_0 \oplus \delta$
P
$f(k,1) = \beta\alpha k$
$TEM(k,1,\beta\alpha\Theta_0)$
$TEM(k,1,\beta\alpha\Theta_0 \oplus \delta)$
$\alpha^{-1}(\cdot)$
$\alpha^{-1}(\cdot)$
$\cdots$
$\beta\alpha^s\Theta_{s-1}$
$\beta\alpha^s\Theta_{s-1} \oplus \delta$
P
$f(k,s) = \beta\alpha^s k$
$\cdots$
$TEM(k,s,\beta\alpha^s\Theta_{s-1})$
$TEM(k,s,\beta\alpha^s\Theta_{s-1} \oplus \delta)$
$\alpha^{-s}(\cdot)$
$\alpha^{-s}(\cdot)$
Θ_0
Θ_1
Θ_{s-1}
Θ_s

Main Idea of Our Chosen-Plaintext Attack

—Similarly, we define the off-line iterated function as:

$$\theta_s = \theta_{s-1} \oplus \alpha^{-s} \cdot P\left(\beta\alpha^s\theta_{s-1}\right) \oplus \alpha^{-s} \cdot P\left(\beta\alpha^s\theta_{s-1} \oplus \delta\right).$$

—The given conditions for the distinguished point are:

- Θ_{u-1}'s filter: $TEM(k, u, \beta\alpha^u\Theta_{u-1}) \oplus TEM(k, u, \beta\alpha^u\Theta_{u-1} \oplus \delta)$.
- θ_{v-1}'s filter: $P\left(\beta\alpha^v\theta_{v-1}\right) \oplus P\left(\beta\alpha^v\theta_{v-1} \oplus \delta\right)$.

Main Idea of Our Chosen-Plaintext Attack

—Similarly, we define the off-line iterated function as:

$$\theta_s = \theta_{s-1} \oplus \alpha^{-s} \cdot P\left(\beta\alpha^s\theta_{s-1}\right) \oplus \alpha^{-s} \cdot P\left(\beta\alpha^s\theta_{s-1} \oplus \delta\right).$$

—The given conditions for the distinguished point are:

- Θ_{u-1}'s filter: $TEM(k, u, \beta\alpha^u\Theta_{u-1}) \oplus TEM(k, u, \beta\alpha^u\Theta_{u-1} \oplus \delta)$.
- θ_{v-1}'s filter: $P\left(\beta\alpha^v\theta_{v-1}\right) \oplus P\left(\beta\alpha^v\theta_{v-1} \oplus \delta\right)$.

As long as

$$\alpha^u\Theta_{u-1} \oplus \alpha^v\theta_{v-1} = \alpha^u k,$$

two distinguished points, $\theta_{v-1+\tau}$ and $\Theta_{u-1+\tau}$, must collide.

☞

$\alpha^{-(u+\tau)}(\alpha^{u+\tau}\Theta_{u-1+\tau} \oplus \alpha^{v+\tau}\theta_{v-1+\tau})$ provides a candidate value for k.

Advantage of Our Chosen-Plaintext Attack

- Using the distinguished point technique and the giant component idea, we can complete the whole chosen-plaintext attack.
- The chains we construct become no longer parallel, but it has no influence on the key-recovery attack.

Advantage of Our Chosen-Plaintext Attack

- Using the distinguished point technique and the giant component idea, we can complete the whole chosen-plaintext attack.
- The chains we construct become no longer parallel, but it has no influence on the key-recovery attack.

We expect with $2^{n/3}$ independent keys in total, $c \cdot 2^{n/3}$ queries per key and $2^{n/3}$ unkeyed queries, to recover almost all the $2^{n/3}$ keys.

Compared with the known-plaintext attack, we remarkably reduce the memory cost from $2^{2n/3}$ to $2^{n/3}$.

1. Introduction
2. Overview of Collision-Based Attacks on EM
3. Known-Plaintext Attack against TEM-1
4. Adaptive Chosen-Plaintext Attack on TEM-1
5. Application to AE Schemes Minalpher and OPP
6. Conclusion

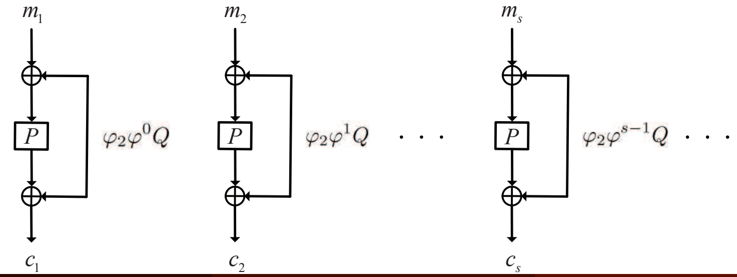
Mask-Recovery Attacks on Minalpher and OPP

The fundamental component of Minalpher and OPP is a tweakable EM primitive, which is used for processing message blocks in parallel.

Let φ, $\varphi_2 = \varphi^2 + \varphi + Id$ be two invertible linear transformations. Then the encryption of OPP with empty auxiliary data is expressed as:

$$TEM(k, s, m_s) = P(m_s \oplus f(Q, s)) \oplus f(Q, s),$$

where $Q = P(k||N)$ and $f(Q, s) = \varphi_2 \varphi^{s-1} Q$.



Mask-Recovery Attacks in the Known-Plaintext Setting

- Our known-plaintext attack can be directly used for evaluating the multi-key security of Minalpher and OPP.

- After recovering the mask under each independent key:

  1. we are able to achieve the associated ciphertext of arbitrary message string without even inquiring the encryption oracle.

  2. we can make valid forgeries of arbitrary form under this (k, N) pair.

Mask-Recovery Attacks in the Chosen-Plaintext Setting

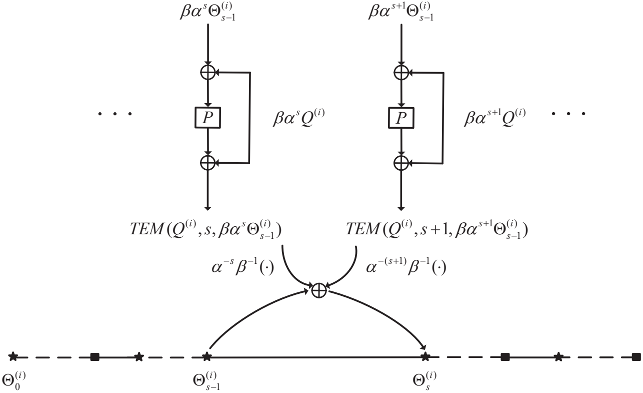
Our previous chosen-plaintext attack requires to reuse nonce to ensure that the mask under each independent key is unchanged.

To build one on-line chain without nonce reuse, we define new iterated functions and choose plaintexts in the blockwise-adaptive way.

Mask-Recovery Attacks in the Chosen-Plaintext Setting

Our previous chosen-plaintext attack requires to reuse nonce to ensure that the mask under each independent key is unchanged.

To build one on-line chain without nonce reuse, we define new iterated functions and choose plaintexts in the blockwise-adaptive way.



$\beta\alpha^{s}\Theta_{s-1}^{(i)}$
$\beta\alpha^{s+1}\Theta_{s-1}^{(i)}$
$\cdots$
P
$\beta\alpha^{s}Q^{(i)}$
P
$\beta\alpha^{s+1}Q^{(i)}$
$\cdots$
$TEM(Q^{(i)}, s, \beta\alpha^{s}\Theta_{s-1}^{(i)})$
$TEM(Q^{(i)}, s+1, \beta\alpha^{s+1}\Theta_{s-1}^{(i)})$
$\alpha^{-s}\beta^{-1}(\cdot)$
$\alpha^{-(s+1)}\beta^{-1}(\cdot)$
$\Theta_{0}^{(i)}$
$\Theta_{s-1}^{(i)}$
$\Theta_{s}^{(i)}$

1 Introduction

2 Overview of Collision-Based Attacks on EM

3 Known-Plaintext Attack against TEM-1

4 Adaptive Chosen-Plaintext Attack on TEM-1

5 Application to AE Schemes Minalpher and OPP

6 Conclusion

Conclusion

1. Introduce multi-key analysis on tweakable Even-Mansour, in both known-plaintext and chosen-plaintext models.

2. Reduce security margins of Minalpher and OPP against multi-key attacks.

3. Raise an alert : permutation-based modes seem to be weaker than blockcipher-based modes in the multi-key setting.

Thanks for your attention !