SERMA
SAFETY & SECURITY

The Dangerous Message/Key Swap in HMAC

02/04/2025 CASCADE

Antoine Wurcker, David Marçais

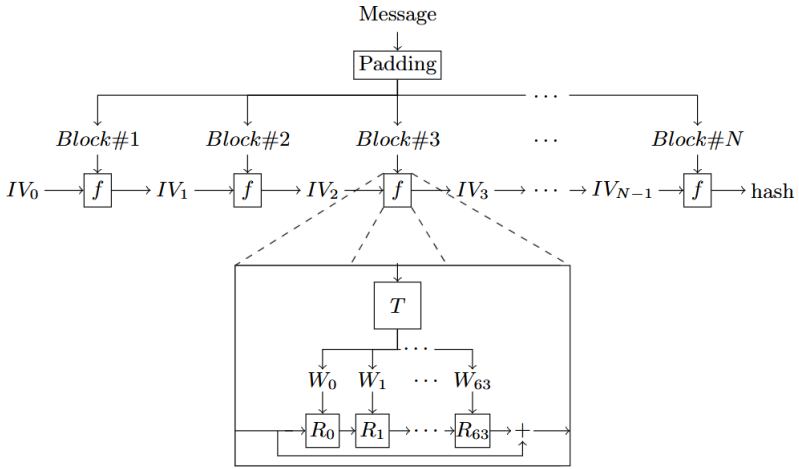
SECURE YOUR FUTURE

Summary

Summary

Introduction:
SHA-2

SHA-2 (256)
Global Scheme



SHA-2 (256)
IV and Message Transformation

$$IV$$

$$\Downarrow$$

$$\{A_0, B_0, C_0, D_0, E_0, F_0, G_0, H_0\}$$

Message Block

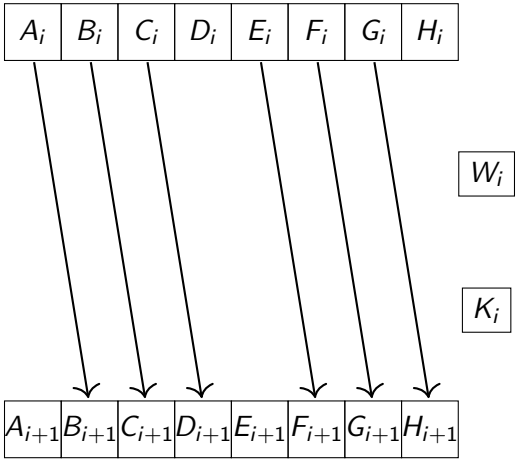
$$\Downarrow$$

$$\{W_0, \ldots, W_{15}\}$$

$$\Downarrow T \Downarrow$$

$$\{W_{16}, \ldots, W_{63}\}$$

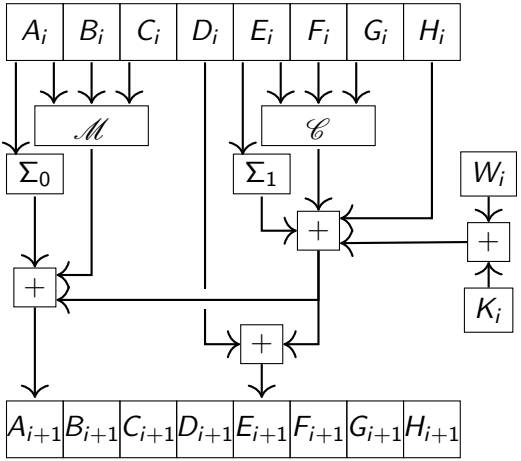
SHA-2 (256)
One Round in f



$$
\begin{aligned}
B_{i+1} &= A_i \\
C_{i+1} &= B_i \\
D_{i+1} &= C_i
\end{aligned}
$$

$$
\begin{aligned}
F_{i+1} &= E_i \\
G_{i+1} &= F_i \\
H_{i+1} &= G_i
\end{aligned}
$$

SHA-2 (256)
One Round in f



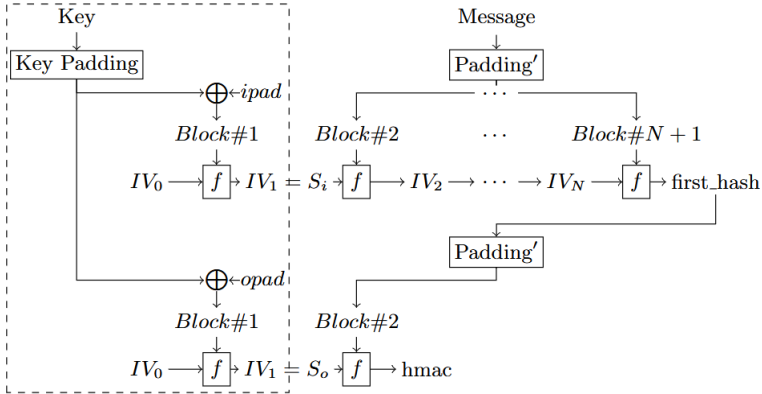
$$
\begin{aligned}
E_{i+1} &= K_i + W_i + H_i \\
&\quad + \mathscr{C}(E_i, F_i, G_i) \\
&\quad + \Sigma_1(E_i) + D_i
\end{aligned}
$$

$$
\begin{aligned}
A_{i+1} &= K_i + W_i + H_i \\
&\quad + \mathscr{C}(E_i, F_i, G_i) \\
&\quad + \Sigma_1(E_i) + \Sigma_0(A_i) \\
&\quad + \mathscr{M}(A_i, B_i, C_i)
\end{aligned}
$$

Summary

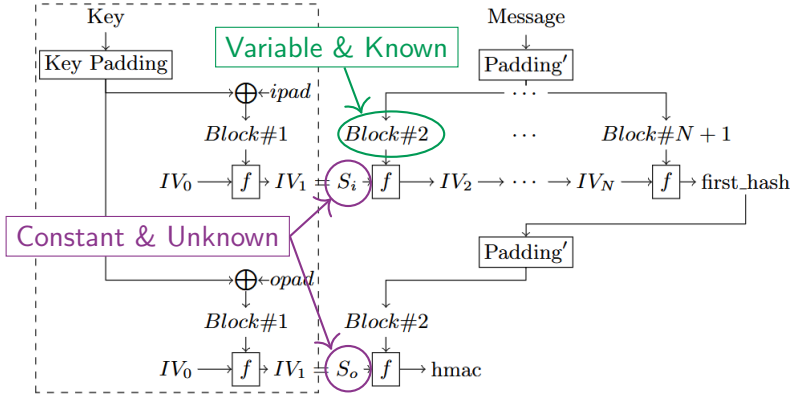
Introduction: HMAC

HMAC (SHA-2-256)
Global Scheme



HMAC (SHA-2-256)
Global Scheme

Known Constant
Known Variable
Unknown Constant
Unknown Variable



Classical HMAC Usage

Known Constant
Known Variable
Unknown Constant
Unknown Variable

IV

$\Downarrow$

$\{A_0, B_0, C_0, D_0, E_0, F_0, G_0, H_0\}$

Message Block

$\Downarrow$

$\{W_0, \ldots, W_{15}\}$

$\Downarrow T \Downarrow$

$\{W_{16}, \ldots, W_{63}\}$

Summary

State-of-the-Art:
Early Attacks

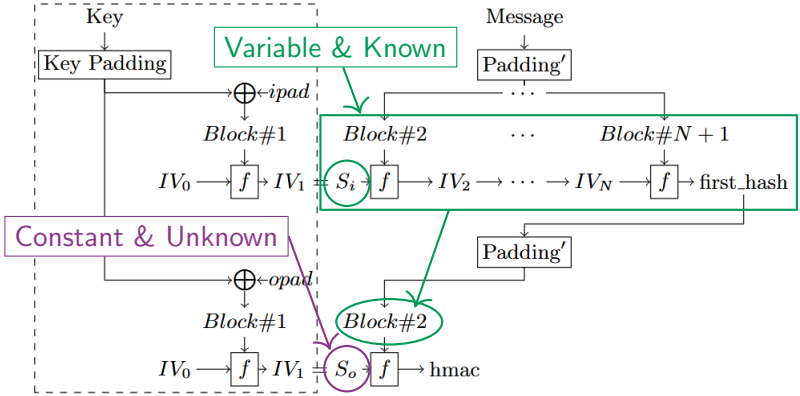
Early Attacks
MTMM07 & BBDGR13

One example of this kind of attack requires leakage on:

- A_i values.
- E_i values.
- "and" sub-operations in Choice ($\mathscr{C}$).
- "and" sub-operations in Majority ($\mathscr{M}$).

8 attacks gives 8 equations with 8 unknown constants
$\Rightarrow S_i$ can be recovered.

Early Attacks
Outer Hash: Same Attack



Summary

State-of-the-Art:
Partial Attack

Partial Attack On HMAC
Slides RM13

This attack requires leakage on:

- A_i values.
- E_i values.
- ~~"and" sub-operations in Choice ($\mathscr{C}$).~~
- ~~"and" sub-operations in Majority ($\mathscr{M}$).~~

RM13 suggests to avoid harder to obtain leakage on "and".

Partial Attack On HMAC
Slides RM13

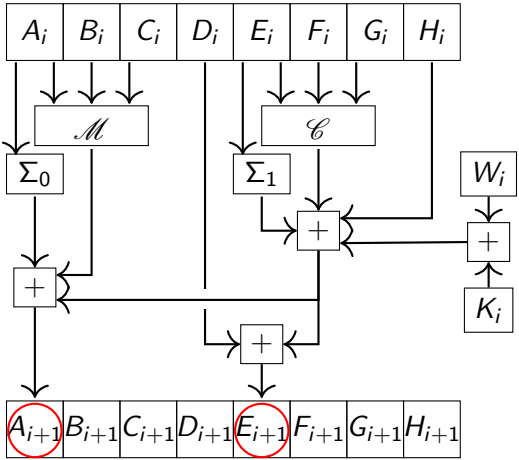
This attack requires leakage on:

- A_i values.
- E_i values.
- ~~"and" sub-operations in Choice ($\mathscr{C}$).~~
- ~~"and" sub-operations in Majority ($\mathscr{M}$).~~

RM13 suggests to avoid harder to obtain leakage on "and".
In counterpart:

- Message must be partially chosen.
- $\Rightarrow$ Cannot be applied on outer hash.

Partial Attack On HMAC
Leakages Requirements



Same leakage on four rounds.
Performed on four sets.

Set	Target	Constant	Variable
#1	A_1 & E_1	$\emptyset$	W_0
#2	A_2 & E_2	W_0	W_1
#3	A_3 & E_3	W_0, W_1	W_2
#4	A_4 & E_4	W_0, W_1, W_2	W_3

Partial Attack On HMAC
Gathering Equations

Known Constant
Known Variable
Unknown Constant
Unknown Variable

First Set:

$$E_1 = H_0 + \Sigma_1(E_0) + \mathscr{C}(E_0, F_0, G_0) + D_0 + K_0 + W_0$$
$$A_1 = H_0 + \Sigma_1(E_0) + \mathscr{C}(E_0, F_0, G_0) + \Sigma_0(A_0) + \mathscr{M}(A_0, B_0, C_0) + K_0 + W_0$$

Partial Attack On HMAC
Gathering Equations

Known Constant
Known Variable
Unknown Constant
Unknown Variable

First Set:

$E_1 = H_0 + \Sigma_1(E_0) + \mathscr{C}(E_0, F_0, G_0) + D_0 + K_0 + W_0$

$A_1 = H_0 + \Sigma_1(E_0) + \mathscr{C}(E_0, F_0, G_0) + \Sigma_0(A_0) + \mathscr{M}(A_0, B_0, C_0) + K_0 + W_0$

What if we continue on first set ?

$E_2 = G_0 + \Sigma_1(E_1) + \mathscr{C}(E_1, E_0, F_0) + C_0 + K_1 + W_1$

$A_2 = G_0 + \Sigma_1(E_1) + \mathscr{C}(E_1, E_0, F_0) + \Sigma_0(A_1) + \mathscr{M}(A_1, A_0, B_0) + K_1 + W_1$

What about $\mathscr{C}$ and $\mathscr{M}$ that combine Known Variable and Unknown Constant?

Partial Attack On HMAC
Gathering Equations

Known Constant
Known Variable
Unknown Constant
Unknown Variable

First Set:

$E_1 = H_0 + \Sigma_1(E_0) + \mathscr{C}(E_0, F_0, G_0) + D_0 + K_0 + W_0$

$A_1 = H_0 + \Sigma_1(E_0) + \mathscr{C}(E_0, F_0, G_0) + \Sigma_0(A_0) + \mathscr{M}(A_0, B_0, C_0) + K_0 + W_0$

What if we continue on first set ?

$E_2 = G_0 + \Sigma_1(E_1) + \mathscr{C}(E_1, E_0, F_0) + C_0 + K_1 + W_1$

$A_2 = G_0 + \Sigma_1(E_1) + \mathscr{C}(E_1, E_0, F_0) + \Sigma_0(A_1) + \mathscr{M}(A_1, A_0, B_0) + K_1 + W_1$

What about $\mathscr{C}$ and $\mathscr{M}$ that combine Known Variable and Unknown Constant?

$\Rightarrow$ Cannot attack because Unknown Variable

Partial Attack On HMAC
Gathering Equations

Known Constant
Known Variable
Unknown Constant
Unknown Variable

First Set:

$E_1 = H_0 + \Sigma_1(E_0) + \mathscr{C}(E_0, F_0, G_0) + D_0 + K_0 + W_0$

$A_1 = H_0 + \Sigma_1(E_0) + \mathscr{C}(E_0, F_0, G_0) + \Sigma_0(A_0) + \mathscr{M}(A_0, B_0, C_0) + K_0 + W_0$

What if we continue on first set ?

$E_2 = G_0 + \Sigma_1(E_1) + \mathscr{C}(E_1, E_0, F_0) + C_0 + K_1 + W_1$

$A_2 = G_0 + \Sigma_1(E_1) + \mathscr{C}(E_1, E_0, F_0) + \Sigma_0(A_1) + \mathscr{M}(A_1, A_0, B_0) + K_1 + W_1$

What about $\mathscr{C}$ and $\mathscr{M}$ that combine Known Variable and Unknown Constant?

$\Rightarrow$ Cannot attack because Unknown Variable

Solution: New set with fixed W_0 to Known Constant

$\Rightarrow$ E_1 and A_1 change from Known Variable to Known Constant

$\Rightarrow$ $\mathscr{C}$ and $\mathscr{M}$ change from Unknown Variable became Unknown Constant

Partial Attack On HMAC
Gathering Equations

Known Constant
Known Variable
Unknown Constant
Unknown Variable

First Set:

$$E_1 = H_0 + \Sigma_1(E_0) + \mathscr{C}(E_0, F_0, G_0) + D_0 + K_0 + W_0$$
$$A_1 = H_0 + \Sigma_1(E_0) + \mathscr{C}(E_0, F_0, G_0) + \Sigma_0(A_0) + \mathscr{M}(A_0, B_0, C_0) + K_0 + W_0$$

Second Set:

$$E_2 = G_0 + \Sigma_1(E_1) + \mathscr{C}(E_1, E_0, F_0) + C_0 + K_1 + W_1$$
$$A_2 = G_0 + \Sigma_1(E_1) + \mathscr{C}(E_1, E_0, F_0) + \Sigma_0(A_1) + \mathscr{M}(A_1, A_0, B_0) + K_1 + W_1$$

Partial Attack On HMAC
Gathering Equations

Known Constant
Known Variable
Unknown Constant
Unknown Variable

First Set:

$$E_1 = H_0 + \Sigma_1(E_0) + \mathscr{C}(E_0, F_0, G_0) + D_0 + K_0 + W_0$$
$$A_1 = H_0 + \Sigma_1(E_0) + \mathscr{C}(E_0, F_0, G_0) + \Sigma_0(A_0) + \mathscr{M}(A_0, B_0, C_0) + K_0 + W_0$$

Second Set:

$$E_2 = G_0 + \Sigma_1(E_1) + \mathscr{C}(E_1, E_0, F_0) + C_0 + K_1 + W_1$$
$$A_2 = G_0 + \Sigma_1(E_1) + \mathscr{C}(E_1, E_0, F_0) + \Sigma_0(A_1) + \mathscr{M}(A_1, A_0, B_0) + K_1 + W_1$$

Third Set:

$$E_3 = F_0 + \Sigma_1(E_2) + \mathscr{C}(E_2, E_1, E_0) + B_0 + K_2 + W_2$$
$$A_3 = F_0 + \Sigma_1(E_2) + \mathscr{C}(E_2, E_1, E_0) + \Sigma_0(A_2) + \mathscr{M}(A_2, A_1, A_0) + K_2 + W_2$$

Known Constant
Known Variable
Unknown Constant
Unknown Variable

Partial Attack On HMAC
Gathering Equations

First Set:

$$E_1 = H_0 + \Sigma_1(E_0) + \mathscr{C}(E_0, F_0, G_0) + D_0 + K_0 + W_0$$
$$A_1 = H_0 + \Sigma_1(E_0) + \mathscr{C}(E_0, F_0, G_0) + \Sigma_0(A_0) + \mathscr{M}(A_0, B_0, C_0) + K_0 + W_0$$

Second Set:

$$E_2 = G_0 + \Sigma_1(E_1) + \mathscr{C}(E_1, E_0, F_0) + C_0 + K_1 + W_1$$
$$A_2 = G_0 + \Sigma_1(E_1) + \mathscr{C}(E_1, E_0, F_0) + \Sigma_0(A_1) + \mathscr{M}(A_1, A_0, B_0) + K_1 + W_1$$

Third Set:

$$E_3 = F_0 + \Sigma_1(E_2) + \mathscr{C}(E_2, E_1, E_0) + B_0 + K_2 + W_2$$
$$A_3 = F_0 + \Sigma_1(E_2) + \mathscr{C}(E_2, E_1, E_0) + \Sigma_0(A_2) + \mathscr{M}(A_2, A_1, A_0) + K_2 + W_2$$

Fourth Set:

$$E_4 = E_0 + \Sigma_1(E_3) + \mathscr{C}(E_3, E_2, E_1) + A_0 + K_3 + W_3$$
$$A_4 = E_0 + \Sigma_1(E_3) + \mathscr{C}(E_3, E_2, E_1) + \Sigma_0(A_3) + \mathscr{M}(A_3, A_2, A_1) + K_3 + W_3$$

Partial Attack On HMAC Outer Hash

Described attack requires chosen message:

- Works on inner hash in chosen message context.
- Does not work on outer hash (only known, not chosen).

This is why it is a partial attack.

Summary

State-of-the-Art:
Complete Attack

Complete Attack On HMAC Schuhmacher22

This attack uses the partial attack on Inner hash.
Then proposes usage of same leakage (A_i & E_i) on last rounds of outer hash.
This requires:

- A_i leakage.
- E_i leakage.
- Chosen message context (partial attack requirement).
- Known MAC.

Detailed equations in the paper.

Summary

Our Contributions: Cost Reducing

Known Constant
Known Variable
Unknown Constant
Unknown Variable

Reducing State-of-the-Art Attacks Cost
Reminder of State-of-the-Art

First Set:

$$E_1 = H_0 + \Sigma_1(E_0) + \mathscr{C}(E_0, F_0, G_0) + D_0 + K_0 + W_0$$
$$A_1 = H_0 + \Sigma_1(E_0) + \mathscr{C}(E_0, F_0, G_0) + \Sigma_0(A_0) + \mathscr{M}(A_0, B_0, C_0) + K_0 + W_0$$

Second Set:

$$E_2 = G_0 + \Sigma_1(E_1) + \mathscr{C}(E_1, E_0, F_0) + C_0 + K_1 + W_1$$
$$A_2 = G_0 + \Sigma_1(E_1) + \mathscr{C}(E_1, E_0, F_0) + \Sigma_0(A_1) + \mathscr{M}(A_1, A_0, B_0) + K_1 + W_1$$

Third Set:

$$E_3 = F_0 + \Sigma_1(E_2) + \mathscr{C}(E_2, E_1, E_0) + B_0 + K_2 + W_2$$
$$A_3 = F_0 + \Sigma_1(E_2) + \mathscr{C}(E_2, E_1, E_0) + \Sigma_0(A_2) + \mathscr{M}(A_2, A_1, A_0) + K_2 + W_2$$

Fourth Set:

$$E_4 = E_0 + \Sigma_1(E_3) + \mathscr{C}(E_3, E_2, E_1) + A_0 + K_3 + W_3$$
$$A_4 = E_0 + \Sigma_1(E_3) + \mathscr{C}(E_3, E_2, E_1) + \Sigma_0(A_3) + \mathscr{M}(A_3, A_2, A_1) + K_3 + W_3$$

Known Constant
Known Variable
Unknown Constant
Unknown Variable

Reducing State-of-the-Art Attacks Cost Do Not Make Fourth Set!

First Set:

$$E_1 = H_0 + \Sigma_1(E_0) + \mathscr{C}(E_0, F_0, G_0) + D_0 + K_0 + W_0$$
$$A_1 = H_0 + \Sigma_1(E_0) + \mathscr{C}(E_0, F_0, G_0) + \Sigma_0(A_0) + \mathscr{M}(A_0, B_0, C_0) + K_0 + W_0$$

Second Set:

$$E_2 = G_0 + \Sigma_1(E_1) + \mathscr{C}(E_1, E_0, F_0) + C_0 + K_1 + W_1$$
$$A_2 = G_0 + \Sigma_1(E_1) + \mathscr{C}(E_1, E_0, F_0) + \Sigma_0(A_1) + \mathscr{M}(A_1, A_0, B_0) + K_1 + W_1$$

Third Set:

$$E_3 = F_0 + \Sigma_1(E_2) + \mathscr{C}(E_2, E_1, E_0) + B_0 + K_2 + W_2$$
$$A_3 = F_0 + \Sigma_1(E_2) + \mathscr{C}(E_2, E_1, E_0) + \Sigma_0(A_2) + \mathscr{M}(A_2, A_1, A_0) + K_2 + W_2$$

Third Set Again (W_2 not fixed $\Rightarrow$ A_3 and E_3 remain Known Variable):

$$E_4 = E_0 + \Sigma_1(E_3) + \mathscr{C}(E_3, E_2, E_1) + A_0 + K_3 + W_3$$
$$A_4 = E_0 + \Sigma_1(E_3) + \mathscr{C}(E_3, E_2, E_1) + \Sigma_0(A_3) + \mathscr{M}(A_3, A_2, A_1) + K_3 + W_3$$

Reducing State-of-the-Art Attacks Cost Do Not Make Fourth Set!

Fourth set not required $\Rightarrow \sim 25\%$ reduced number of traces.

Summary

Our Contributions: Shifting Start

Shifting Start of State-of-the-Art Attacks

Partial attack requires leakage on 4 first rounds.

Shifting Start of State-of-the-Art Attacks

Partial attack requires leakage on 4 first rounds.

If countermeasure protects the 4 first rounds $\Rightarrow$ Attack thwarted.

Shifting Start of State-of-the-Art Attacks

Partial attack requires leakage on 4 first rounds.

If countermeasure protects the 4 first rounds $\Rightarrow$ Attack thwarted.

Our solution:

- Fix the 4 first message blocks W_0, W_1, W_2, W_3

Shifting Start of State-of-the-Art Attacks

Partial attack requires leakage on 4 first rounds.

If countermeasure protects the 4 first rounds $\Rightarrow$ Attack thwarted.

Our solution:

- Fix the 4 first message blocks W_0, W_1, W_2, W_3
- This fixes $\{A_4, \ldots, H_4\}$.

Shifting Start of State-of-the-Art Attacks

Partial attack requires leakage on 4 first rounds.

If countermeasure protects the 4 first rounds $\Rightarrow$ Attack thwarted.

Our solution:

- Fix the 4 first message blocks W_0, W_1, W_2, W_3
- This fixes $\{A_4, \ldots, H_4\}$.
- Same attack is performed on rounds 4 to 8.

Shifting Start of State-of-the-Art Attacks

Partial attack requires leakage on 4 first rounds.

If countermeasure protects the 4 first rounds $\Rightarrow$ Attack thwarted.

Our solution:

- Fix the 4 first message blocks W_0, W_1, W_2, W_3
- This fixes $\{A_4, \ldots, H_4\}$.
- Same attack is performed on rounds 4 to 8.

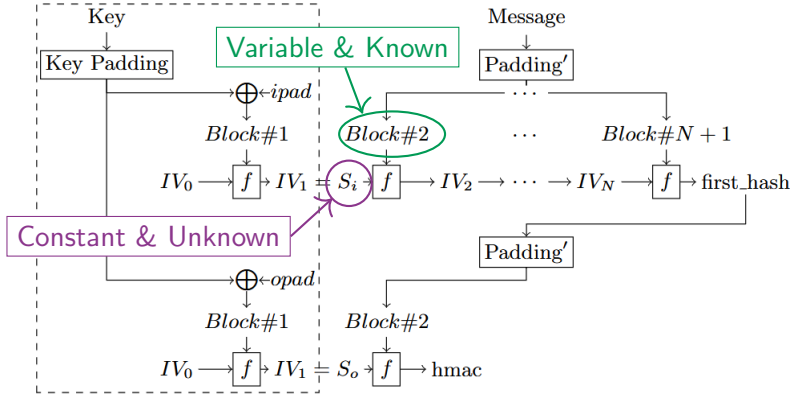
$\{A_4, \ldots, H_4\}$ is combined with W_0, W_1, W_2, W_3 to reveal $\{A_0, \ldots, H_0\}$

Summary

Our Contributions: Swapped Message/Key

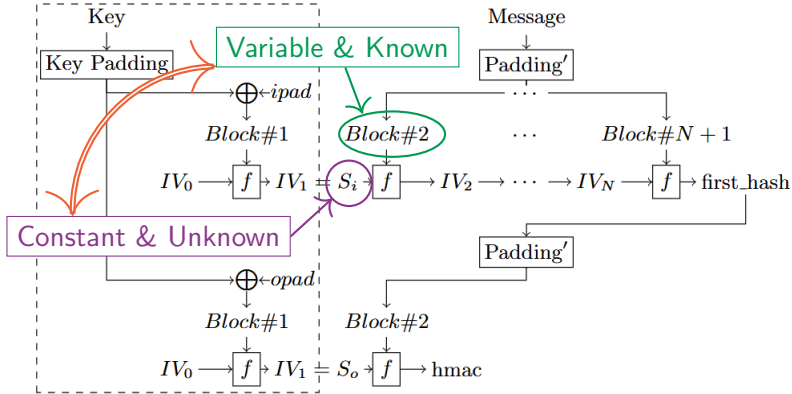
Known Constant
Known Variable
Unknown Constant
Unknown Variable

Attack in Swapped Message/Key Scenario
Reminder: Classical HMAC Usage



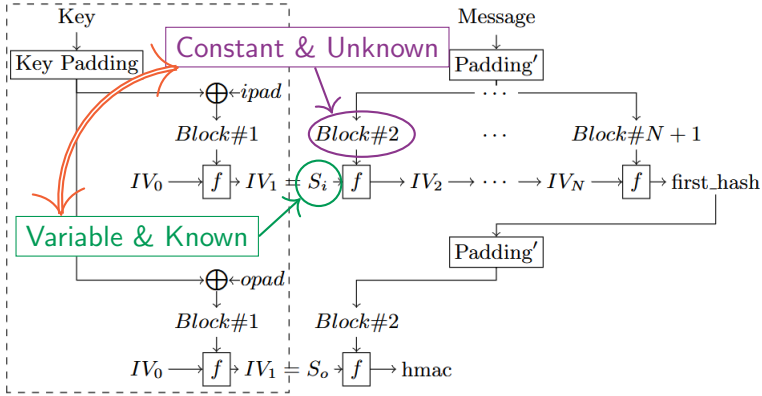
Attack in Swapped Message/Key Scenario
Reminder: Classical HMAC Usage

Known Constant
Known Variable
Unknown Constant
Unknown Variable



Attack in Swapped Message/Key Scenario
Swapped HMAC Usage

Known Constant
Known Variable
Unknown Constant
Unknown Variable



Attack in Swapped Message/Key Scenario Solving Equations

Known Constant
Known Variable
Unknown Constant
Unknown Variable

Reminder of previous attacks:
First Round:

$$E_1 = H_0 + \Sigma_1(E_0) + \mathscr{C}(E_0, F_0, G_0) + D_0 + K_0 + W_0$$
$$A_1 = H_0 + \Sigma_1(E_0) + \mathscr{C}(E_0, F_0, G_0) + \Sigma_0(A_0) + \mathscr{M}(A_0, B_0, C_0) + K_0 + W_0$$

Attack in Swapped Message/Key Scenario Solving Equations

Known Constant
Known Variable
Unknown Constant
Unknown Variable

Reminder of previous attacks:
First Round:

$$E_1 = H_0 + \Sigma_1(E_0) + \mathscr{C}(E_0, F_0, G_0) + D_0 + K_0 + W_0$$
$$A_1 = H_0 + \Sigma_1(E_0) + \mathscr{C}(E_0, F_0, G_0) + \Sigma_0(A_0) + \mathscr{M}(A_0, B_0, C_0) + K_0 + W_0$$

Swapped Messsage/Key context:
First Round:

$$E_1 = H_0 + \Sigma_1(E_0) + \mathscr{C}(E_0, F_0, G_0) + D_0 + K_0 + W_0$$
$$A_1 = H_0 + \Sigma_1(E_0) + \mathscr{C}(E_0, F_0, G_0) + \Sigma_0(A_0) + \mathscr{M}(A_0, B_0, C_0) + K_0 + W_0$$

Attack in Swapped Message/Key Scenario
Solving Equations

Known Constant
Known Variable
Unknown Constant
Unknown Variable

Both equations for A and E give the same information, only one is necessary.
First Round:
$E_1 = H_0 + \Sigma_1(E_0) + \mathscr{C}(E_0, F_0, G_0) + D_0 + K_0 + W_0$

Known Constant
Known Variable
Unknown Constant
Unknown Variable

Attack in Swapped Message/Key Scenario Solving Equations

First Round:

$$E_1 = H_0 + \Sigma_1(E_0) + \mathscr{C}(E_0, F_0, G_0) + D_0 + K_0 + W_0$$

Second Round:

$$E_2 = G_0 + \Sigma_1(E_1) + \mathscr{C}(E_1, E_0, F_0) + C_0 + K_1 + W_1$$

Known Constant
Known Variable
Unknown Constant
Unknown Variable

Attack in Swapped Message/Key Scenario Solving Equations

First Round:

$$E_1 = H_0 + \Sigma_1(E_0) + \mathscr{C}(E_0, F_0, G_0) + D_0 + K_0 + W_0$$

Second Round:

$$E_2 = G_0 + \Sigma_1(E_1) + \mathscr{C}(E_1, E_0, F_0) + C_0 + K_1 + W_1$$

Third Round:

$$E_3 = F_0 + \Sigma_1(E_2) + \mathscr{C}(E_2, E_1, E_0) + B_0 + K_2 + W_2$$

Attack in Swapped Message/Key Scenario Solving Equations

Known Constant
Known Variable
Unknown Constant
Unknown Variable

First Round:

$$E_1 = H_0 + \Sigma_1(E_0) + \mathscr{C}(E_0, F_0, G_0) + D_0 + K_0 + W_0$$

Second Round:

$$E_2 = G_0 + \Sigma_1(E_1) + \mathscr{C}(E_1, E_0, F_0) + C_0 + K_1 + W_1$$

Third Round:

$$E_3 = F_0 + \Sigma_1(E_2) + \mathscr{C}(E_2, E_1, E_0) + B_0 + K_2 + W_2$$

Fourth Round:

$$E_4 = E_0 + \Sigma_1(E_3) + \mathscr{C}(E_3, E_2, E_1) + A_0 + K_3 + W_3$$

Known Constant
Known Variable
Unknown Constant
Unknown Variable

Attack in Swapped Message/Key Scenario Solving Equations

First Round:

$$E_1 = H_0 + \Sigma_1(E_0) + \mathscr{C}(E_0, F_0, G_0) + D_0 + K_0 + W_0$$

Second Round:

$$E_2 = G_0 + \Sigma_1(E_1) + \mathscr{C}(E_1, E_0, F_0) + C_0 + K_1 + W_1$$

Third Round:

$$E_3 = F_0 + \Sigma_1(E_2) + \mathscr{C}(E_2, E_1, E_0) + B_0 + K_2 + W_2$$

Fourth Round:

$$E_4 = E_0 + \Sigma_1(E_3) + \mathscr{C}(E_3, E_2, E_1) + A_0 + K_3 + W_3$$

And so on if necessary...

Attack in Swapped Message/Key Scenario
Advantages and Drawbacks

Advantages:

- Only needs A_i **OR** E_i leakages.
- Recovered data is directly the key.
- No need to attack outer hash.

Drawbacks:

- Requires a swapped Message/Key context. (e.g. HKDF)
- Value recovery is dependent of the success of recovery of the previous one.

Summary

Conclusion:

Conclusion

- Swapping Message and key roles can be dangerous in HMAC.
- Should be studied on other algorithms.
- Potential trace number reduction of state of the art attacks by $\sim 25\%$.
- Protecting only first rounds can be dangerous.

Thank you for your attention.

Do you have any question?

SERMA
SAFETY & SECURITY

14, rue Galilée
33600 PESSAC
05 57 26 08 88
contact-s3@serma.com