Triangulating Meet-in-the-Middle Attack

Boxin Zhao[1] Qingliang Hou[3] Lingyue Qin [2,1,4] Xiaoyang Dong[2,1,4(✉)]

[1]Zhongguancun Laboratory, Beijing, P.R.China

[2]Tsinghua University, Beijing, P.R.China

[3]School of Cyber Science and Technology, Shandong University, Qingdao, P.R.China

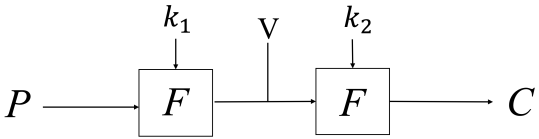
[4]State Key Laboratory of Cryptography and Digital Economy Security, Tsinghua University, Beijing, P.R.China

CRYPTO 2025 / August 17 - 21, 2025

Outline

Meet-in-the-Middle (MitM) Attack

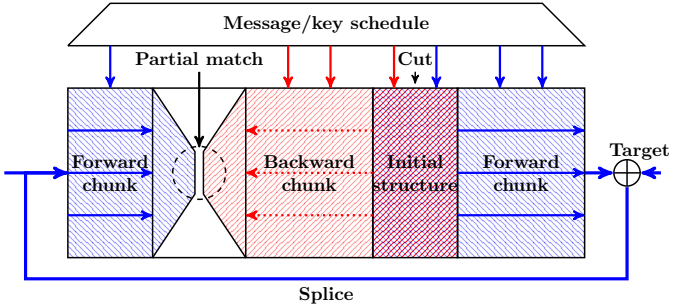
- MitM was first introduced by Diffie and Hellman in 1977 to attack Double-DES [DH77]
- Example: $C = E_K(P) = F_{k_2}(F_{k_1}(P))$, $K = k_1 \| k_2$
  - Neutral sets: k_1 and k_2 are independent of each other
  - Match: $F_{k_1}(P)$ and $F_{k_2}^{-1}(C)$
- Time complexity: $2^{|k_1|+|k_2|} \rightarrow 2^{|k_1|+|k_2|-n}$



- Enhanced techniques: splice-and-cut, initial structure, automated tools, $\cdots$
- Application to MD constructions: MD4, MD5, SHA-1, Whirpool, AES-MMO, Simpira-DM, $\cdots$

Splice-and-Cut MitM Attack Framework

- At SAC 2008, Aoki and Sasaki proposed the splice-and-cut technique [AS08].

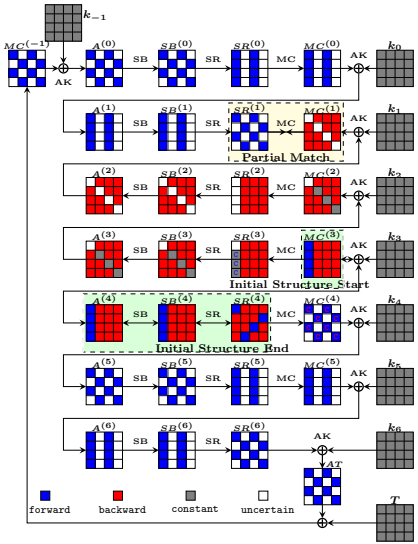


- Splice-and-Cut
- Initial Structure
- Partial Matching

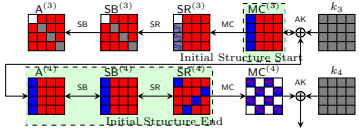
1. For $2^{d_{\mathcal{R}}}$ values of ■, compute backward to the matching points and store them in L_1.
2. For $2^{d_{\mathcal{B}}}$ values of ■, compute forward to the matching points and store them in L_2.
3. Find m-bit partial match between L_1 and L_2.

- Time complexity: $Time = 2^{h-(d_{\mathcal{R}}+d_{\mathcal{B}})} \cdot (2^{\max(d_{\mathcal{R}},d_{\mathcal{B}})} + 2^{d_{\mathcal{R}}+d_{\mathcal{B}}-m}) \simeq 2^{h-\min(d_{\mathcal{R}},d_{\mathcal{B}},m)}$

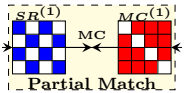
MitM Preimage attack on 7-round AES-like Hash [Sas11]



- Starting states(MC^3): $\lambda^+ = 4$ ■, $\lambda^- = 12$ ■
- Initial structure: $\ell^+ = 3$, $\ell^- = 8$



- Match through `MixColumn(MC)`



- $T = 2^{8\times(3+8)} \times (2^8 + 2^{8\times 4} + 2^{8\times(1+4-4)}) = 2^{120}$

Outline

Nonlinear Constrained Neutral Words

- At CRYPTO 2021, Dong et al. [DHS+21] gave a formal description of the MitM attack
- Nonlinear Constrained Neutral Words

$$\begin{cases} \pi_1^+(I^{\mathcal{E}}[\mathcal{G}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{G}^{\mathcal{K}}], I^{\mathcal{E}}[\mathcal{B}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{B}^{\mathcal{K}}]) = a_1 \\ \pi_2^+(I^{\mathcal{E}}[\mathcal{G}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{G}^{\mathcal{K}}], I^{\mathcal{E}}[\mathcal{B}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{B}^{\mathcal{K}}]) = a_2 \\ \cdots \quad \cdots \\ \pi_{\ell^+}^+(I^{\mathcal{E}}[\mathcal{G}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{G}^{\mathcal{K}}], I^{\mathcal{E}}[\mathcal{B}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{B}^{\mathcal{K}}]) = a_{\ell^+} \end{cases} \tag{1}$$

$$\begin{cases} \pi_1^-(I^{\mathcal{E}}[\mathcal{G}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{G}^{\mathcal{K}}], I^{\mathcal{E}}[\mathcal{R}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{R}^{\mathcal{K}}]) = b_1 \\ \pi_2^-(I^{\mathcal{E}}[\mathcal{G}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{G}^{\mathcal{K}}], I^{\mathcal{E}}[\mathcal{R}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{R}^{\mathcal{K}}]) = b_2 \\ \cdots \quad \cdots \\ \pi_{\ell^-}^-(I^{\mathcal{E}}[\mathcal{G}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{G}^{\mathcal{K}}], I^{\mathcal{E}}[\mathcal{R}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{R}^{\mathcal{K}}]) = b_{\ell^-} \end{cases} \tag{2}$$

- π^+ and π^- represent certain constraints on the neutral words of the forward and backward computations

Solving Nonlinear Constrained Neutral Words

- Dong et al. [DHS+21] presented a table-based technique

Algorithm 1 Computing the solution spaces of the neutral words

Input: $(I^{\mathcal{E}}[\mathcal{G}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{G}^{\mathcal{K}}]) \in \mathbb{F}_2^{w\cdot(|\mathcal{G}^{\mathcal{E}}|+|\mathcal{G}^{\mathcal{K}}|)}$
Output: V, U

1 $V \leftarrow [\,]$, $U \leftarrow [\,]$
for $(I^{\mathcal{E}}[\mathcal{B}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{B}^{\mathcal{K}}]) \in \mathbb{F}_2^{w\cdot(|\mathcal{B}^{\mathcal{E}}|+|\mathcal{B}^{\mathcal{K}}|)}$ **do**
2 $\quad \mathbf{v} \leftarrow \boldsymbol{\pi}^{+}(I^{\mathcal{E}}[\mathcal{G}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{G}^{\mathcal{K}}], I^{\mathcal{E}}[\mathcal{B}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{B}^{\mathcal{K}}])$ by Eq. (1)
3 $\quad$ Insert $(I^{\mathcal{E}}[\mathcal{B}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{B}^{\mathcal{K}}])$ into V at index $\mathbf{v}$
4 **end**
5 **for** $(I^{\mathcal{E}}[\mathcal{R}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{R}^{\mathcal{K}}]) \in \mathbb{F}_2^{w\cdot(|\mathcal{R}^{\mathcal{E}}|+|\mathcal{R}^{\mathcal{K}}|)}$ **do**
6 $\quad \mathbf{u} \leftarrow \boldsymbol{\pi}^{-}(I^{\mathcal{E}}[\mathcal{G}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{G}^{\mathcal{K}}], I^{\mathcal{E}}[\mathcal{R}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{R}^{\mathcal{K}}])$ by Eq. (2)
7 $\quad$ Insert $(I^{\mathcal{E}}[\mathcal{R}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{R}^{\mathcal{K}}])$ into U at index $\mathbf{u}$
8 **end**

Solving Nonlinear Constrained Neutral Words

- Dong et al. [DHS+21] presented a table-based technique

Algorithm 2 Computing the solution spaces of the neutral words

Input: $(I^{\mathcal{E}}[\mathcal{G}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{G}^{\mathcal{K}}]) \in \mathbb{F}_2^{w\cdot(|\mathcal{G}^{\mathcal{E}}|+|\mathcal{G}^{\mathcal{K}}|)}$
Output: V, U

$V \leftarrow [\,]$, $U \leftarrow [\,]$
for $(I^{\mathcal{E}}[\mathcal{B}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{B}^{\mathcal{K}}]) \in \mathbb{F}_2^{w\cdot(|\mathcal{B}^{\mathcal{E}}|+|\mathcal{B}^{\mathcal{K}}|)}$ **do**
  $\mathbf{v} \leftarrow \boldsymbol{\pi}^{+}(I^{\mathcal{E}}[\mathcal{G}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{G}^{\mathcal{K}}], I^{\mathcal{E}}[\mathcal{B}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{B}^{\mathcal{K}}])$ by Eq. (1)
  Insert $(I^{\mathcal{E}}[\mathcal{B}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{B}^{\mathcal{K}}])$ into V at index $\mathbf{v}$
end
for $(I^{\mathcal{E}}[\mathcal{R}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{R}^{\mathcal{K}}]) \in \mathbb{F}_2^{w\cdot(|\mathcal{R}^{\mathcal{E}}|+|\mathcal{R}^{\mathcal{K}}|)}$ **do**
  $\mathbf{u} \leftarrow \boldsymbol{\pi}^{-}(I^{\mathcal{E}}[\mathcal{G}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{G}^{\mathcal{K}}], I^{\mathcal{E}}[\mathcal{R}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{R}^{\mathcal{K}}])$ by Eq. (2)
  Insert $(I^{\mathcal{E}}[\mathcal{R}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{R}^{\mathcal{K}}])$ into U at index $\mathbf{u}$
end

- Require a huge amount of memory to prepare two hash tables V and U

Solving Nonlinear Constrained Neutral Words

- If the nonlinear constraints of a certain MITM path are simple, the Triangulation algorithm (TA) can be used to solve them

$$\begin{cases} F(x \oplus s) \oplus v = 0, \\ G(x \oplus u) \oplus s \oplus L(y \oplus z) = 0, \\ v \oplus G(u \oplus s) = 0, \\ H(z \oplus s \oplus v) \oplus t = 0, \\ u \oplus H(t \oplus x) = 0. \end{cases}$$

- Khovratovich et al.'s Triangulation Algorithm [KBN09]
  - Repeat finding the variable involved in only one non-processed equation.

$$\begin{cases} L(y \oplus z) \oplus G(u \oplus x) \oplus s = 0, \\ z \oplus H^{-1}(t) \oplus v \oplus s = 0, \\ t \oplus H^{-1}(u) \oplus x = 0, \\ u \oplus G^{-1}(v) \oplus s = 0, \\ v \oplus F(x \oplus s) = 0. \end{cases}$$

Limitations of Khovratovich et al.'s Triangulation Algorithm

- If there is another byte equation

$$\begin{cases} F(x \oplus s) \oplus v = 0, \\ G(x \oplus u) \oplus s \oplus L(y \oplus z) = 0, \\ v \oplus G(u \oplus s) = 0, \\ H(z \oplus s \oplus v) \oplus t = 0, \\ u \oplus H(t \oplus x) = 0, \\ \boxed{P(s \oplus v \oplus t) \oplus z = 0} \end{cases}$$

Before TA:

s	t	u	v	x	y	z
1	0	0	1	1	0	0
1	0	1	0	1	1	1
1	0	1	1	0	0	0
1	1	0	1	0	0	1
0	1	1	0	1	0	0
1	1	0	1	0	0	1

$\xrightarrow[\text{Khovratovich et al.'s TA}]{\text{after extract } y}$

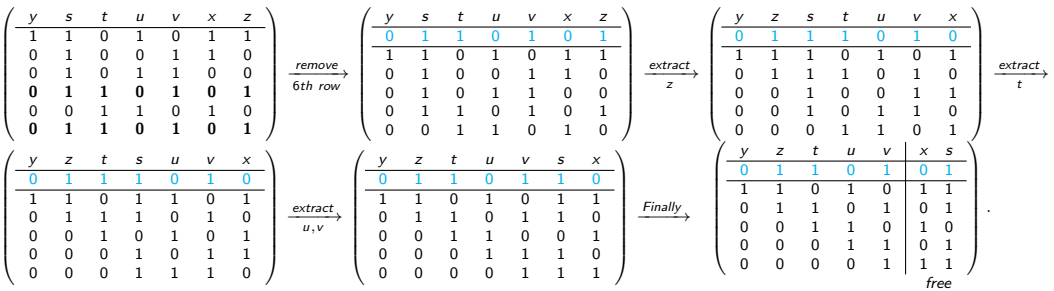
y	s	t	u	v	x	z
0	1	0	0	1	1	0
0	1	0	1	1	0	0
0	1	1	0	1	0	1
0	0	1	1	0	1	0
0	1	1	0	1	0	1
1	1	0	1	0	1	1
	free variables					

Improved Triangulation Algorithm

- Motived by Structured Gaussian elimination (SGE) [LO90]
- **Find the variable involved in only one unprocessed equation:**
  (a) Search for a variable that appears in only one unprocessed equation. If such a variable exists, mark the equation and the variable as processed.
  (b) If no such variable can be found, perform the following steps:
    i Count the number of variables present in each unprocessed equation.
    ii Identify the unprocessed equations that contain the largest number of variables.
    iii Remove one of the equations in (ii) from the system and mark it as processed. This reduces the scale of the remaining system.

Improved Triangulation Algorithm

$$
\begin{cases}
F(x \oplus s) \oplus v = 0, \\
G(x \oplus u) \oplus s \oplus L(y \oplus z) = 0, \\
v \oplus G(u \oplus s) = 0, \\
H(z \oplus s \oplus v) \oplus t = 0, \\
u \oplus H(t \oplus x) = 0, \\
\boxed{P(s \oplus v \oplus t) \oplus z = 0}
\end{cases}
$$



Solving Nonlinear Constrained Neutral Words with the New TA

- Nonlinear Constrained Neutral Words

$$\begin{cases} \pi_1^+(I^{\mathcal{E}}[\mathcal{G}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{G}^{\mathcal{K}}], I^{\mathcal{E}}[\mathcal{B}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{B}^{\mathcal{K}}]) = a_1 \\ \pi_2^+(I^{\mathcal{E}}[\mathcal{G}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{G}^{\mathcal{K}}], I^{\mathcal{E}}[\mathcal{B}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{B}^{\mathcal{K}}]) = a_2 \\ \cdots \quad \cdots \\ \pi_{\ell^+}^+(I^{\mathcal{E}}[\mathcal{G}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{G}^{\mathcal{K}}], I^{\mathcal{E}}[\mathcal{B}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{B}^{\mathcal{K}}]) = a_{\ell^+} \end{cases} \qquad \begin{cases} \pi_1^-(I^{\mathcal{E}}[\mathcal{G}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{G}^{\mathcal{K}}], I^{\mathcal{E}}[\mathcal{R}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{R}^{\mathcal{K}}]) = b_1 \\ \pi_2^-(I^{\mathcal{E}}[\mathcal{G}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{G}^{\mathcal{K}}], I^{\mathcal{E}}[\mathcal{R}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{R}^{\mathcal{K}}]) = b_2 \\ \cdots \quad \cdots \\ \pi_{\ell^-}^-(I^{\mathcal{E}}[\mathcal{G}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{G}^{\mathcal{K}}], I^{\mathcal{E}}[\mathcal{R}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{R}^{\mathcal{K}}]) = b_{\ell^-} \end{cases}$$

- Given global constants $(I^{\mathcal{E}}[\mathcal{G}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{G}^{\mathcal{K}}])$

$$\begin{cases} \pi_1^-(s, \_, \_, v, x, \_, \_) = b_1 \\ \pi_2^-(s, \_, u, \_, x, y, z) = b_2 \\ \pi_3^-(s, \_, u, v, \_, \_, \_) = b_3 \\ \pi_4^-(s, t, \_, v, \_, \_, z) = b_4 \\ \pi_5^-(\_, t, u, \_, x, \_, \_) = b_5 \\ \pi_6^-(s, t, \_, v, \_, \_, z) = b_6 \end{cases} \xrightarrow{\text{New TA}} \begin{cases} \pi_4^-(\_, z, t, \_, v, \_, s, \_) = b_4 \\ \pi_2^-(y, z, \_, u, \_, x, s, \_) = b_2 \\ \pi_6^-(\_, z, t, \_, v, \_, s, \_) = b_6 \\ \pi_5^-(\_, \_, t, u, \_, x, \_, \_) = b_5 \\ \pi_3^-(\_, \_, \_, u, v, \_, s, \_) = b_3 \\ \pi_1^-(\_, \_, \_, \_, v, x, s, \_) = b_1 \end{cases}$$

Solving Nonlinear Constrained Neutral Words with the New TA

- Nonlinear Constrained Neutral Words

$$\begin{cases} \pi_1^+(I^{\mathcal{E}}[\mathcal{G}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{G}^{\mathcal{K}}], I^{\mathcal{E}}[\mathcal{B}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{B}^{\mathcal{K}}]) = a_1 \\ \pi_2^+(I^{\mathcal{E}}[\mathcal{G}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{G}^{\mathcal{K}}], I^{\mathcal{E}}[\mathcal{B}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{B}^{\mathcal{K}}]) = a_2 \\ \cdots \quad \cdots \\ \pi_{\ell^+}^+(I^{\mathcal{E}}[\mathcal{G}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{G}^{\mathcal{K}}], I^{\mathcal{E}}[\mathcal{B}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{B}^{\mathcal{K}}]) = a_{\ell^+} \end{cases} \qquad \begin{cases} \pi_1^-(I^{\mathcal{E}}[\mathcal{G}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{G}^{\mathcal{K}}], I^{\mathcal{E}}[\mathcal{R}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{R}^{\mathcal{K}}]) = b_1 \\ \pi_2^-(I^{\mathcal{E}}[\mathcal{G}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{G}^{\mathcal{K}}], I^{\mathcal{E}}[\mathcal{R}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{R}^{\mathcal{K}}]) = b_2 \\ \cdots \quad \cdots \\ \pi_{\ell^-}^-(I^{\mathcal{E}}[\mathcal{G}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{G}^{\mathcal{K}}], I^{\mathcal{E}}[\mathcal{R}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{R}^{\mathcal{K}}]) = b_{\ell^-} \end{cases}$$

- Given global constants $(I^{\mathcal{E}}[\mathcal{G}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{G}^{\mathcal{K}}])$

$$\begin{cases} \pi_1^-(s, \_, \_, v, x, \_, \_) = b_1 \\ \pi_2^-(s, \_, u, \_, x, y, z) = b_2 \\ \pi_3^-(s, \_, u, v, \_, \_, \_) = b_3 \\ \pi_4^-(s, t, \_, v, \_, \_, z) = b_4 \\ \pi_5^-(\_, t, u, \_, x, \_, \_) = b_5 \\ \pi_6^-(s, t, \_, v, \_, \_, z) = b_6 \end{cases} \xrightarrow{\text{New TA}} \begin{cases} \pi_4^-(\_, z, t, \_, v, \_, s) = b_4 \\ \pi_2^-(y, z, \_, u, \_, x, s) = b_2 \\ \pi_6^-(\_, z, t, \_, v, \_, s) = b_6 \\ \pi_5^-(\_, \_, t, u, \_, x, \_) = b_5 \\ \pi_3^-(\_, \_, \_, u, v, \_, s) = b_3 \\ \pi_1^-(\_, \_, \_, \_, v, x, s) = b_1 \end{cases}$$

[DHS+21]

- Traverse 7-byte variables s, t, u, v, x, y, z
- Compute $(b_1, b_2, \cdots, b_6) \in \mathbb{F}_2^{48}$ and store the 7-byte string (s, t, u, v, x, y, z) into a hash table U
- Time and memory: 2^{56}

New TA

- Given b_2, b_6, b_5, b_3, b_1
- Traverse x, s, and duduce v, u, t, z, y and b_4
- Memory: 2^{16}

Solving Nonlinear Constrained Neutral Words with the New TA

Algorithm 3 Computing the value space of the neutral words with New TA and a memory-aided precomputation

Input: $(I^{\mathcal{E}}[\mathcal{G}^{\mathcal{E}}], I^{\mathcal{K}}[\mathcal{G}^{\mathcal{K}}]) \in \mathbb{F}_2^{w\cdot(|\mathcal{G}^{\mathcal{E}}|+|\mathcal{G}^{\mathcal{K}}|)}$

17 **for** $(b_2, b_6, b_5, b_3, b_1) \in \mathbb{F}_2^{8\times 5}$ **do**

18 $V \leftarrow [\,]$, $U \leftarrow [\,]$

for $(x, s) \in \mathbb{F}_2^{8\times 2}$ **do**

19 Compute v from $\pi_1^{-}()$

Compute u from $\pi_3^{-}()$

Compute t from $\pi_5^{-}()$

Compute z from $\pi_6^{-}()$

Compute y from $\pi_2^{-}()$

20 Compute $\mathbf{u} = b_4$ by equations marked by cyan

Store $U[\mathbf{u}] \leftarrow (x, s, v, u, t, z, y)$

21 **end**

22 Similarly, we can prepare V

Then, under each index i, j, compute the values from $U[i]$ backward, and independently, compute the values from $V[j]$ forward, and filter the states by the matching point.

23 **end**

Search Framework of Automatic Triangulating MitM Attack

The full search framework of our attacks consists of two steps:

1. The first step is to use the existing MILP models for MitM attacks on AES and other primitives to find massive MitM paths.
   E.g., for AES we use Dong et al.'s model [DHS+21] to search potential MitM paths, and more than 1000 MitM paths are found for 5-round AES-128.
2. The second step is to apply the improved TA to each MitM path to solve the systems of the nonlinear constrained neutral words and recognize the good MitM path with improved memory complexity.

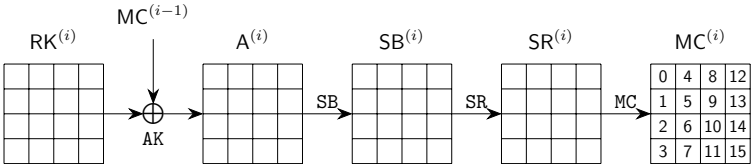
Outline

AES and Rijndael [DR02]

- AES: 128-bit block cipher with a 128/192/256-bit key
- Rijndael: the block length can be 128/192/256 bits

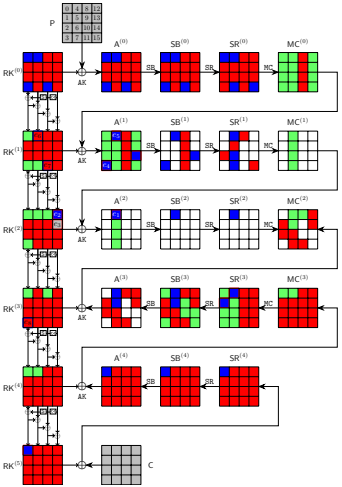
The i-th round function consists of the following operations:

- **AddRoundKey** (AK): XOR a round key $\mathrm{RK}^{(i)}$ into the state $\mathrm{MC}^{(i-1)}$ to produce $\mathrm{A}^{(i)}$.
- **SubBytes** (SB): Substitute each cell of $\mathrm{A}^{(i)}$ according to an S-box to get $\mathrm{SB}^{(i)}$.
- **ShiftRows** (SR): For $N_{col} = 4, 6$, rotate the ith row of $\mathrm{SB}^{(i)}$ to the left by i bytes ($i = 0, 1, 2, 3$). For $N_{col} = 8$, rotate the $0, 1, 2, 3$rd row to the left by $0, 1, 3, 4$ bytes, respectively.
- **MixColumns** (MC): Update each column of $\mathrm{SR}^{(i)}$ by left-multiplying an MDS matrix to get $\mathrm{MC}^{(i)}$.



Single-Plaintext Key-Recovery Attack on 5-round AES-128

- Starting state $\mathrm{RK}^{(0)}$ contains $\lambda^{+} = 4$ ■ bytes and $\lambda^{-} = 12$ ■ bytes
- 9 consumed DoFs of ■ on $\mathrm{A}^{(1)}[3]$, $\mathrm{A}^{(1)}[4]$, $\mathrm{A}^{(1)}[14]$, $\mathrm{RK}^{(2)}[12]$, $\mathrm{RK}^{(2)}[13]$, $\mathrm{A}^{(2)}[4]$, $\mathrm{SR}^{(3)}[1]$, $\mathrm{SR}^{(3)}[4]$, and $\mathrm{RK}^{(5)}[0]$ marked by ■/■
- 3 consumed DoFs of ■ on $\mathrm{RK}^{(1)}[4]$, $\mathrm{RK}^{(1)}[11]$, and $\mathrm{RK}^{(3)}[3]$ marked by ■
- DoM = 1 matching byte in round 2



Single-Plaintext Key-Recovery Attack on 5-round AES-128

- Denote starting state $\mathrm{RK}^{(0)}$ as k_0 to k_{15}
- 9 consumed DoFs of ■ on $\mathrm{A}^{(1)}[3]$, $\mathrm{A}^{(1)}[4]$, $\mathrm{A}^{(1)}[14]$, $\mathrm{RK}^{(2)}[12]$, $\mathrm{RK}^{(2)}[13]$, $\mathrm{A}^{(2)}[4]$, $\mathrm{SR}^{(3)}[1]$, $\mathrm{SR}^{(3)}[4]$, and $\mathrm{RK}^{(5)}[0]$

$$
\begin{cases}
\mathrm{A}^{(1)}[3] = S(k_5) \oplus S(k_{10}) \oplus 2 \cdot S(k_{15}) \oplus S(k_{12}) \oplus 3 \cdot S(k_0) \oplus k_3 \\
\mathrm{A}^{(1)}[4] = 3 \cdot S(k_9) \oplus S(k_{14}) \oplus S(k_{13}) \oplus 2 \cdot S(k_4) \oplus k_4 \oplus S(k_3) \oplus k_0 \\
\mathrm{A}^{(1)}[14] = S(k_{12}) \oplus S(k_1) \oplus 2 \cdot S(k_6) \oplus k_{14} \oplus k_{10} \oplus k_6 \oplus k_2 \oplus S(k_{15}) \oplus 3 \cdot S(k_{11}) \\
\mathrm{A}^{(2)}[4] = 3 \cdot S(S(k_8) \oplus 2 \cdot S(k_{13}) \oplus 3 \cdot S(k_2) \oplus S(k_7) \oplus k_9 \oplus k_5 \oplus k_1 \oplus S(k_{14})) \oplus \\
\qquad S(k_{13} \oplus k_9 \oplus k_5 \oplus k_1 \oplus S(k_{14})) \oplus k_4 \oplus S(\mathrm{A}^{(1)}[3]) \oplus 2 \cdot S(\mathrm{A}^{(1)}[4]) \oplus S(\mathrm{A}^{(1)}[14]) \\
\mathrm{RK}^{(2)}[12] = k_{12} \oplus S(k_{13} \oplus k_9 \oplus k_5 \oplus k_1 \oplus S(k_{14})) \oplus k_4 \\
\mathrm{RK}^{(2)}[13] = k_{13} \oplus k_5 \oplus S(k_{14} \oplus k_{10} \oplus k_6 \oplus k_2 \oplus S(k_{15})) \\
\mathrm{SR}^{(3)}[1] = 9 \cdot (S(\mathrm{RK}^{(0)}[13]) \oplus S(\mathrm{RK}^{(1)}[13]) \oplus S(\mathrm{RK}^{(2)}[13]) \oplus S(\mathrm{RK}^{(3)}[13])) \oplus \\
\qquad \mathtt{e} \cdot (\mathrm{MC}^{(3)}[1]) \oplus \mathtt{b} \cdot (\mathrm{MC}^{(3)}[2]) \oplus \mathtt{d} \cdot (\mathrm{MC}^{(3)}[3]) \oplus 9 \cdot (\mathrm{RK}^{(0)}[0] \oplus \mathrm{A}^{(4)}[0]) \\
\mathrm{SR}^{(3)}[4] = \mathtt{e} \cdot (S(\mathrm{RK}^{(0)}[13]) \oplus S(\mathrm{RK}^{(1)}[13]) \oplus S(\mathrm{RK}^{(2)}[13]) \oplus S(\mathrm{RK}^{(3)}[13]) \oplus \mathrm{RK}^{(3)}[4] \oplus \mathrm{A}^{(4)}[4]) \\
\qquad \oplus \mathtt{b} \cdot (\mathrm{MC}^{(3)}[5]) \oplus \mathtt{d} \cdot (\mathrm{MC}^{(3)}[6]) \oplus 9 \cdot (\mathrm{MC}^{(3)}[7]) \oplus \mathtt{e} \cdot (\mathrm{RK}^{(0)}[0]) \\
\mathrm{RK}^{(5)}[0] = S(\mathrm{RK}^{(0)}[13]) \oplus S(\mathrm{RK}^{(1)}[13]) \oplus S(\mathrm{RK}^{(2)}[13]) \oplus S(\mathrm{RK}^{(3)}[13]) \oplus S(\mathrm{RK}^{(4)}[13]) \oplus \mathrm{RK}^{(0)}[0]
\end{cases}
$$

Single-Plaintext Key-Recovery Attack on 5-round AES-128

- Excluding the parts related to blue bytes, we get the following equations which are only related to the red bytes, where the boxed parts are deleted

$$
\begin{cases}
\widehat{\mathrm{A}}^{(1)}[3] = S(k_5) \oplus S(k_{10}) \oplus 2 \cdot S(k_{15}) \oplus S(k_{12}) \boxed{\oplus 3 \cdot S(k_0) \oplus k_3} \\
\widehat{\mathrm{A}}^{(1)}[4] = 3 \cdot S(k_9) \oplus S(k_{14}) \oplus S(k_{13}) \boxed{\oplus 2 \cdot S(k_4) \oplus k_4 \oplus S(k_3) \oplus k_0} \\
\widehat{\mathrm{A}}^{(1)}[14] = S(k_{12}) \oplus S(k_1) \oplus 2 \cdot S(k_6) \oplus k_{14} \oplus k_{10} \oplus k_6 \oplus k_2 \oplus S(k_{15}) \oplus \boxed{3 \cdot S(k_{11})} \\
\widehat{\mathrm{A}}^{(2)}[4] = 3 \cdot S(S(k_8) \oplus 2 \cdot S(k_{13}) \oplus 3 \cdot S(k_2) \oplus S(k_7) \oplus k_9 \oplus k_5 \oplus k_1 \oplus S(k_{14})) \oplus S(k_{13} \oplus k_9 \oplus k_5 \\
\qquad \oplus k_1 \oplus S(k_{14})) \boxed{\oplus k_4 \oplus S(\widehat{\mathrm{A}}^{(1)}[3] \oplus B_1) \oplus 2 \cdot S(\widehat{\mathrm{A}}^{(1)}[4] \oplus B_2) \oplus S(\widehat{\mathrm{A}}^{(1)}[14] \oplus B_3)} \\
\widehat{\mathrm{RK}}^{(2)}[12] = k_{12} \oplus S(k_{13} \oplus k_9 \oplus k_5 \oplus k_1 \oplus S(k_{14})) \boxed{\oplus k_4} \\
\widehat{\mathrm{RK}}^{(2)}[13] = k_{13} \oplus k_5 \oplus S(k_{14} \oplus k_{10} \oplus k_6 \oplus k_2 \oplus S(k_{15})) \\
\widehat{\mathrm{SR}}^{(3)}[1] = 9 \cdot (S(\mathrm{RK}^{(0)}[13]) \oplus S(\mathrm{RK}^{(1)}[13]) \oplus S(\widehat{\mathrm{RK}}^{(2)}[13]) \oplus S(\mathrm{RK}^{(3)}[13])) \oplus \\
\qquad \mathrm{e} \cdot (\mathrm{MC}^{(3)}[1]) \oplus \mathrm{b} \cdot (\mathrm{MC}^{(3)}[2]) \oplus \mathrm{d} \cdot (\mathrm{MC}^{(3)}[3]) \boxed{\oplus 9 \cdot (\mathrm{RK}^{(0)}[0] \oplus \mathrm{A}^{(4)}[0])} \\
\widehat{\mathrm{SR}}^{(3)}[4] = \mathrm{e} \cdot (S(\mathrm{RK}^{(0)}[13]) \oplus S(\mathrm{RK}^{(1)}[13]) \oplus S(\widehat{\mathrm{RK}}^{(2)}[13]) \oplus S(\mathrm{RK}^{(3)}[13]) \oplus \mathrm{RK}^{(3)}[4] \oplus \mathrm{A}^{(4)}[4]) \\
\qquad \oplus \mathrm{b} \cdot (\mathrm{MC}^{(3)}[5]) \oplus \mathrm{d} \cdot (\mathrm{MC}^{(3)}[6]) \oplus 9 \cdot (\mathrm{MC}^{(3)}[7]) \boxed{\oplus \mathrm{e} \cdot (\mathrm{RK}^{(0)}[0])} \\
\widehat{\mathrm{RK}}^{(5)}[0] = S(\mathrm{RK}^{(0)}[13]) \oplus S(\mathrm{RK}^{(1)}[13]) \oplus S(\widehat{\mathrm{RK}}^{(2)}[13]) \oplus S(\mathrm{RK}^{(3)}[13]) \oplus S(\mathrm{RK}^{(4)}[13]) \boxed{\oplus \mathrm{RK}^{(0)}[0]}
\end{cases}
$$

Single-Plaintext Key-Recovery Attack on 5-round AES-128

- No variable appears in only one unprocessed equation in begining matrix (a)
- Remove the 3 bold rows ($\widehat{\mathrm{SR}}^{(3)}[1], \widehat{\mathrm{SR}}^{(3)}[4], \widehat{\mathrm{RK}}^{(5)}[0]$) and label them as processed, get matrix (b)

	k_1	k_2	k_5	k_6	k_7	k_8	k_9	k_{10}	k_{12}	k_{13}	k_{14}	k_{15}
$\widehat{\mathrm{A}}^{(1)}[3]$	0	0	1	0	0	0	0	1	1	0	0	1
$\widehat{\mathrm{A}}^{(1)}[4]$	0	0	0	0	0	0	1	0	0	1	1	0
$\widehat{\mathrm{A}}^{(1)}[14]$	1	1	0	1	0	0	0	1	1	0	1	1
$\widehat{\mathrm{A}}^{(2)}[4]$	1	1	1	0	1	1	1	0	0	1	1	0
$\widehat{\mathrm{RK}}^{(2)}[12]$	1	0	1	0	0	0	1	0	1	1	1	0
$\widehat{\mathrm{RK}}^{(2)}[13]$	0	1	1	1	0	0	0	1	0	1	1	1
$\widehat{\mathrm{SR}}^{(3)}[1]$	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**
$\widehat{\mathrm{SR}}^{(3)}[4]$	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**
$\widehat{\mathrm{RK}}^{(5)}[0]$	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**

(a)

	k_1	k_2	k_5	k_6	k_7	k_8	k_9	k_{10}	k_{12}	k_{13}	k_{14}	k_{15}
$\widehat{\mathrm{SR}}^{(3)}[1]$	1	1	1	1	1	1	1	1	1	1	1	1
$\widehat{\mathrm{SR}}^{(3)}[4]$	1	1	1	1	1	1	1	1	1	1	1	1
$\widehat{\mathrm{RK}}^{(5)}[0]$	1	1	1	1	1	1	1	1	1	1	1	1
$\widehat{\mathrm{A}}^{(1)}[3]$	0	0	1	0	0	0	0	1	1	0	0	1
$\widehat{\mathrm{A}}^{(1)}[4]$	0	0	0	0	0	0	1	0	0	1	1	0
$\widehat{\mathrm{A}}^{(1)}[14]$	1	1	0	1	0	0	0	1	1	0	1	1
$\widehat{\mathrm{A}}^{(2)}[4]$	1	1	1	0	1	1	1	0	0	1	1	0
$\widehat{\mathrm{RK}}^{(2)}[12]$	1	0	1	0	0	0	1	0	1	1	1	0
$\widehat{\mathrm{RK}}^{(2)}[13]$	0	1	1	1	0	0	0	1	0	1	1	1

(b)

Single-Plaintext Key-Recovery Attack on 5-round AES-128

- Extract a dependent variable k_7 and label the row as processed, get matrix (c)
- Remove 1 bold rows ($\widehat{\mathrm{A}}^{(1)}[14]$) and label it as processed, get matrix (d)

$$
\left(\begin{array}{c|cccccccccccc}
 & k_7 & k_1 & k_2 & k_5 & k_6 & k_8 & k_9 & k_{10} & k_{12} & k_{13} & k_{14} & k_{15} \\
\hline
\widehat{\mathrm{SR}}^{(3)}[1] & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\widehat{\mathrm{SR}}^{(3)}[4] & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\widehat{\mathrm{RK}}^{(5)}[0] & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\hline
\widehat{\mathrm{A}}^{(2)}[4] & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\
\widehat{\mathrm{A}}^{(1)}[3] & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\
\widehat{\mathrm{A}}^{(1)}[4] & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\
\widehat{\mathrm{A}}^{(1)}[14] & \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{0} & \mathbf{0} & \mathbf{1} & \mathbf{1} & \mathbf{0} & \mathbf{1} & \mathbf{1} \\
\widehat{\mathrm{RK}}^{(2)}[12] & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\
\widehat{\mathrm{RK}}^{(2)}[13] & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1
\end{array}\right) \quad (c)
$$

$$
\left(\begin{array}{c|cccccccccccc}
 & k_7 & k_1 & k_2 & k_5 & k_6 & k_8 & k_9 & k_{10} & k_{12} & k_{13} & k_{14} & k_{15} \\
\hline
\widehat{\mathrm{SR}}^{(3)}[1] & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\widehat{\mathrm{SR}}^{(3)}[4] & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\widehat{\mathrm{RK}}^{(5)}[0] & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
\widehat{\mathrm{A}}^{(1)}[14] & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 \\
\hline
\widehat{\mathrm{A}}^{(2)}[4] & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\
\widehat{\mathrm{A}}^{(1)}[3] & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\
\widehat{\mathrm{A}}^{(1)}[4] & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\
\widehat{\mathrm{RK}}^{(2)}[12] & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\
\widehat{\mathrm{RK}}^{(2)}[13] & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1
\end{array}\right) \quad (d)
$$

Single-Plaintext Key-Recovery Attack on 5-round AES-128

- Extract k_1, k_2, k_5, k_9 sequentially, get the matrix (f)
- Finally, 5 dependent variables (k_7, k_1, k_2, k_5, k_9) marked in green and 7 free variables ($k_6, k_8, k_{10}, k_{12}, k_{13}, k_{14}, k_{15}$)

(e)

	k_7	k_1	k_2	k_5	k_6	k_8	k_9	k_{10}	k_{12}	k_{13}	k_{14}	k_{15}
$\widehat{\mathrm{SR}}^{(3)}[1]$	1	1	1	1	1	1	1	1	1	1	1	1
$\widehat{\mathrm{SR}}^{(3)}[4]$	1	1	1	1	1	1	1	1	1	1	1	1
$\widehat{\mathrm{RK}}^{(5)}[0]$	1	1	1	1	1	1	1	1	1	1	1	1
$\widehat{\mathrm{A}}^{(1)}[14]$	0	1	1	0	1	0	0	1	1	0	1	1
$\widehat{\mathrm{A}}^{(2)}[4]$	1	1	1	1	0	1	1	0	0	1	1	0
$\widehat{\mathrm{RK}}^{(2)}[12]$	0	1	0	1	0	0	1	0	1	1	1	0
$\widehat{\mathrm{A}}^{(1)}[3]$	0	0	0	1	0	0	0	1	1	0	0	1
$\widehat{\mathrm{A}}^{(1)}[4]$	0	0	0	0	0	0	1	0	0	1	1	0
$\widehat{\mathrm{RK}}^{(2)}[13]$	0	0	1	1	1	0	0	1	0	1	1	1

(f)

	k_7	k_1	k_2	k_5	k_9	k_6	k_8	k_{10}	k_{12}	k_{13}	k_{14}	k_{15}
$\widehat{\mathrm{SR}}^{(3)}[1]$	1	1	1	1	1	1	1	1	1	1	1	1
$\widehat{\mathrm{SR}}^{(3)}[4]$	1	1	1	1	1	1	1	1	1	1	1	1
$\widehat{\mathrm{RK}}^{(5)}[0]$	1	1	1	1	1	1	1	1	1	1	1	1
$\widehat{\mathrm{A}}^{(1)}[14]$	0	1	1	0	1	0	0	1	1	0	1	1
$\widehat{\mathrm{A}}^{(2)}[4]$	1	1	1	1	1	0	1	0	0	1	1	0
$\widehat{\mathrm{RK}}^{(2)}[12]$	0	1	0	1	1	0	0	0	1	1	1	0
$\widehat{\mathrm{RK}}^{(2)}[13]$	0	0	1	1	0	1	0	1	0	1	1	1
$\widehat{\mathrm{A}}^{(1)}[3]$	0	0	0	1	0	0	0	1	1	0	0	1
$\widehat{\mathrm{A}}^{(1)}[4]$	0	0	0	0	1	0	0	0	0	1	1	0

free variables

Single-Plaintext Key-Recovery Attack on 5-round AES-128

- 3 consumed DoFs of blue byte ■ on $\mathrm{RK}^{(1)}[4]$, $\mathrm{RK}^{(1)}[11]$, and $\mathrm{RK}^{(3)}[3]$

$$\begin{cases} \mathrm{RK}^{(1)}[4] = k_4 \oplus k_0 \oplus S(k_{13}) \\ \mathrm{RK}^{(1)}[11] = k_{11} \oplus k_3 \oplus k_7 \oplus S(k_{12}) \\ \mathrm{RK}^{(3)}[3] = k_3 \oplus S(k_4 \oplus e_2) \oplus S(k_4 \oplus k_0 \oplus S(k_{13}) \oplus k_8 \oplus k_{12}) \oplus S(k_{12}) \end{cases}$$

- Assign the following formulas as constants (e_6, e_7, e_8)

$$\begin{cases} k_4 \oplus k_0 = e_6 \\ k_{11} \oplus k_3 = e_7 \\ k_3 \oplus S(k_4 \oplus e_2) = e_8 \end{cases}$$

- 3 dependent variables (k_3, k_4, k_{11}) and 1 free variable k_0

Single-Plaintext Key-Recovery Attack on 5-round AES-128

- Time: about $2^{128-8\cdot\min\{\mathrm{DoF}^+,\mathrm{DoF}^-,\mathrm{DoM}\}} = 2^{120}$
- Memory: about 2^{40} to store U

for 2^{ζ} *values of* $(e_1, e_2, e_3, e_4, e_5) \in \mathbb{F}_2^{40}$ **do**
  for $(e_6, e_7, e_8) \in \mathbb{F}_2^{24}$ **do**
    for $\mathsf{RK}^{(0)}[14, 15] \in \mathbb{F}_2^{16}$ **do**
      $U \leftarrow [\,]$
      $(\widehat{\mathsf{A}}^{(1)}[4], \widehat{\mathsf{RK}}^{(2)}[12], \widehat{\mathsf{RK}}^{(2)}[13], \widehat{\mathsf{A}}^{(1)}[3], \widehat{\mathsf{A}}^{(2)}[4]) \leftarrow (e_1, e_2, e_3, e_4, e_5)$
      for $\mathsf{RK}^{(0)}[6, 8, 10, 12, 13] \in \mathbb{F}_2^{40}$ **do**
        Compute $\mathsf{RK}^{(0)}[7, 1, 2, 5, 9] = (k_7, k_1, k_2, k_5, k_9)$ by Eq. (13)-(f)
        Compute $\mathbf{u} = (\widehat{\mathsf{SR}}^{(3)}[1], \widehat{\mathsf{SR}}^{(3)}[4], \widehat{\mathsf{RK}}^{(5)}[0], \widehat{\mathsf{A}}^{(1)}[14]) \in \mathbb{F}_2^{32}$
        $U[\mathbf{u}] \leftarrow \mathsf{RK}^{(0)}[1, 2, 5-10, 12-15] \in \mathbb{F}_2^{8\times 12}$
        /* The nonlinear system solving and memory-aided precomputation are combined to get the solution space of the neutral words. There are about 2^8 elements in $U[\mathbf{u}]$ for each $\mathbf{u}$. */
      end
      for $\mathbf{u} \in \mathbb{F}_2^{32}$ **do**
        $L \leftarrow [\,]$
        for $\mathsf{RK}^{(0)}[0] = k_0 \in \mathbb{F}_2^8$ **do**
          Compute $\mathsf{RK}^{(0)}[3, 4, 11] = (k_3, k_4, k_{11})$ by Eq. (15)
          Compute the 1-byte matching point $v = \mathsf{SR}^{(2)}[4] \oplus e \cdot \mathsf{MC}^{(2)}[4] \oplus b \cdot \mathsf{MC}^{(2)}[5]$
          $L[v] \leftarrow (k_0, k_3, k_4, k_{11})$
        end
        for *values in* $U[\mathbf{u}]$ **do**
          Compute the 1-byte matching point $v' = e \cdot \mathsf{MC}^{(2)}[4] \oplus b \cdot \mathsf{MC}^{(2)}[5] \oplus d \cdot \mathsf{MC}^{(2)}[6] \oplus 9 \cdot \mathsf{MC}^{(2)}[7]$
          for *values in* $L[v']$ **do**
            if $E(Key = \mathsf{RK}^{(0)}, P) = C$ **then**
              return $\mathsf{RK}^{(0)}$
            end
          end
        end
      end
    end
  end
end

Outline

Summary of applications

Target	Methods	Rounds	Data	Time	Memory	Generic	Ref.
AES-128	MitM	$3^{\dagger}/10$	1KP	2^{96}	2^{72}	2^{128}	[BDF11]
	MitM	$4^{\dagger}/10$	1KP	2^{120}	2^{80}	2^{128}	[BDF11]
	MitM	$4^{\dagger}/10$	1KP	2^{120}	$\mathbf{2^{24}}$	2^{128}	ours
	MitM	$4^{\dagger}/10$	1KP	$\mathbf{2^{112}}$	$\mathbf{2^{56}}$	2^{128}	ours
	MitM	5/10	1KP	2^{120}	2^{120}	2^{128}	[Bou11]
	MitM	5/10	1KP	2^{120}	2^{96}	2^{128}	[Der13]
	MitM	5/10	1KP	2^{120}	$\mathbf{2^{40}}$	2^{128}	ours
	MitM	$4^{\dagger}/10$	2CP	2^{80}	2^{80}	2^{128}	[BDF11]
	MitM	$5^{\dagger}/10$	8CP	2^{64}	2^{56}	2^{128}	[Der13]
	Partial Sum	5/10	2^{8}CP	2^{40}	small	2^{128}	[Tun12]
	R-Boomerang	5/10	2^{9}ACC	2^{23}	2^{9}	2^{128}	[DKRS24]
	Yoyo	5/10	2^{11}ACC	2^{31}	small	2^{128}	[RBH17]
AES-192	MitM	6/12	2KP	2^{176}	2^{72}	2^{192}	ours
	MitM	6/12	2^{8}CP	$2^{109.6}$	$2^{109.6}$	2^{192}	[Der13]
	Multiple-of-8	7/12	2^{26}CP	$2^{146.3}$	2^{40}	2^{192}	[BDK+18]
AES-256	MitM	7/14	2KP	2^{248}	2^{72}	2^{256}	ours
	MitM	6/14	2^{8}CP	2^{122}	2^{113}	2^{256}	[Der13]
	MitM	7/14	2^{8}CP	2^{170}	2^{186}	2^{256}	[Der13]
	MitM	7/14	2^{26}CP	2^{146}	2^{40}	2^{256}	[BDK+18]

†: The attacks cover x full rounds of AES.

Summary of applications

Target	Methods	Rounds	Data	Time	Memory	Generic	Ref.
Rijndael-EM-128	MitM	7/10	1KP	2^{112}	2^{32}	2^{128}	ours
Rijndael-EM-192	MitM	8/12	1KP	2^{176}	2^{16}	2^{192}	ours
Rijndael-EM-256	MitM	9/14	1KP	2^{248}	2^{8}	2^{256}	ours

Thank You!

Q&A Contact:

Boxin Zhao
zhaobx@zgclab.edu.cn
(Zhongguancun Laboratory)

Reference I

[AS08] Kazumaro Aoki and Yu Sasaki.
Preimage attacks on one-block MD4, 63-step MD5 and more.
In SAC 2008, volume 5381, pages 103–119. Springer, 2008.

[BDF11] Charles Bouillaguet, Patrick Derbez, and Pierre-Alain Fouque.
Automatic search of attacks on round-reduced AES and applications.
In Phillip Rogaway, editor, Advances in Cryptology - CRYPTO 2011 - 31st Annual Cryptology Conference, Santa Barbara, CA, USA, August 14-18, 2011. Proceedings, volume 6841 of Lecture Notes in Computer Science, pages 169–187. Springer, 2011.

[BDK+18] Achiya Bar-On, Orr Dunkelman, Nathan Keller, Eyal Ronen, and Adi Shamir.
Improved key recovery attacks on reduced-round AES with practical data and memory complexities.
In Hovav Shacham and Alexandra Boldyreva, editors, Advances in Cryptology - CRYPTO 2018 - 38th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 19-23, 2018, Proceedings, Part II, volume 10992 of Lecture Notes in Computer Science, pages 185–212. Springer, 2018.

[Bou11] Charles Bouillaguet.
Etudes dhypotheses algorithmiques et attaques de primitives cryptographiques.
PhD thesis, Université Paris-Diderot–École Normale Supérieure, 2011.

Reference II

[Der13] Patrick Derbez.
Meet-in-the-middle attacks on AES.
PhD thesis, Ecole Normale Supérieure de Paris-ENS Paris, 2013.

[DH77] Whitfield Diffie and Martin E. Hellman.
Special feature exhaustive cryptanalysis of the NBS data encryption standard.
Computer, 10(6):74–84, 1977.

[DHS+21] Xiaoyang Dong, Jialiang Hua, Siwei Sun, Zheng Li, Xiaoyun Wang, and Lei Hu.
Meet-in-the-middle attacks revisited: Key-recovery, collision, and preimage attacks.
In CRYPTO 2021, Proceedings, Part III, volume 12827, pages 278–308. Springer, 2021.

[DKRS24] Orr Dunkelman, Nathan Keller, Eyal Ronen, and Adi Shamir.
The retracing boomerang attack, with application to reduced-round AES.
J. Cryptol., 37(3):32, 2024.

[DR02] Joan Daemen and Vincent Rijmen.
The Design of Rijndael: AES - The Advanced Encryption Standard.
Information Security and Cryptography. Springer, 2002.

Reference III

[KBN09] Dmitry Khovratovich, Alex Biryukov, and Ivica Nikolic.
Speeding up collision search for byte-oriented hash functions.
In Marc Fischlin, editor, Topics in Cryptology - CT-RSA 2009, The Cryptographers' Track at the RSA Conference 2009, San Francisco, CA, USA, April 20-24, 2009. Proceedings, volume 5473 of Lecture Notes in Computer Science, pages 164–181. Springer, 2009.

[LO90] Brian A. LaMacchia and Andrew M. Odlyzko.
Solving large sparse linear systems over finite fields.
In Alfred Menezes and Scott A. Vanstone, editors, Advances in Cryptology - CRYPTO '90, 10th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1990, Proceedings, volume 537 of Lecture Notes in Computer Science, pages 109–133. Springer, 1990.

[RBH17] Sondre Rønjom, Navid Ghaedi Bardeh, and Tor Helleseth.
Yoyo tricks with AES.
In Tsuyoshi Takagi and Thomas Peyrin, editors, Advances in Cryptology - ASIACRYPT 2017 - 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Hong Kong, China, December 3-7, 2017, Proceedings, Part I, volume 10624 of Lecture Notes in Computer Science, pages 217–243. Springer, 2017.

Reference IV

[Sas11] Yu Sasaki.
Meet-in-the-middle preimage attacks on AES hashing modes and an application to whirlpool.
In FSE 2011, pages 378–396. Springer, 2011.

[Tun12] Michael Tunstall.
Improved "partial sums"-based square attack on AES.
In Pierangela Samarati, Wenjing Lou, and Jianying Zhou, editors, SECRYPT 2012 - Proceedings of the International Conference on Security and Cryptography, Rome, Italy, 24-27 July, 2012, SECRYPT is part of ICETE - The International Joint Conference on e-Business and Telecommunications, pages 25–34. SciTePress, 2012.