Guess-and-Determine Rebound: Applications to Key Collisions on AES

Lingyue Qin[1,2,3] Wenquan Bi[2] Xiaoyang Dong[1,2,3](✉)

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

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

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

August 18, 2025

Outline

1. Background and Preliminaries

2. Guess-and-Determine Rebound Attack

3. Key Collision Attacks on Reduced AES

Outline

1. **Background and Preliminaries**

2. Guess-and-Determine Rebound Attack

3. Key Collision Attacks on Reduced AES

Key Commitment of Authenticated Encryption

- Key commitment of Authenticated Encryption:
  - A ciphertext chosen by an attacker does not decrypt into two different sets of key, nonce, and associated data
- [Albertini et al., 2022] analyzed the widely used AE schemes AES-GCM and ChaCha20-Poly1305
  - **Padding fix**: prepending a l-bit string X of 0's to the message M for each encryption as $\mathsf{Enc}(K, N, A, X \| M)$

Key Commitment of Authenticated Encryption

- Key commitment of Authenticated encryption:
  - A ciphertext chosen by an attacker does not decrypt into two different sets of key, nonce, and associated data
- [Albertini et al., 2022] analyzed the widely used AE schemes AES-GCM and ChaCha20-Poly1305
  - **Padding fix**: prepending a l-bit string X of 0's to the message M for each encryption as $\mathrm{Enc}(K, N, A, X \| M)$
  - Open problem: Is it possible to find two keys K_1 and K_2 such that $\mathrm{AES}_{K_1}(0) = \mathrm{AES}_{K_2}(0)$ in less than 2^{64} trials?

Key Collision Attack

Target-Plaintext Key Collision [Taiyama et al., 2024]

It is two distinct keys that generate the same ciphertext for a single target plaintext.

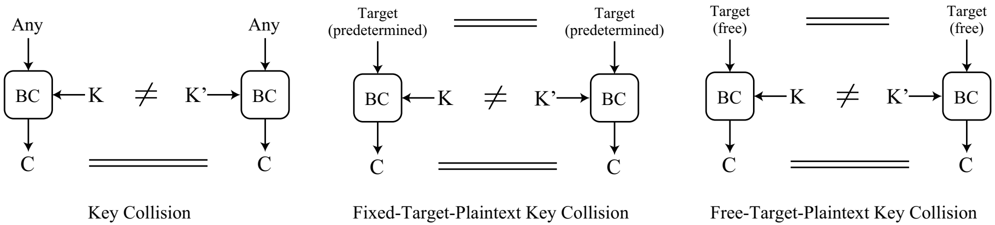
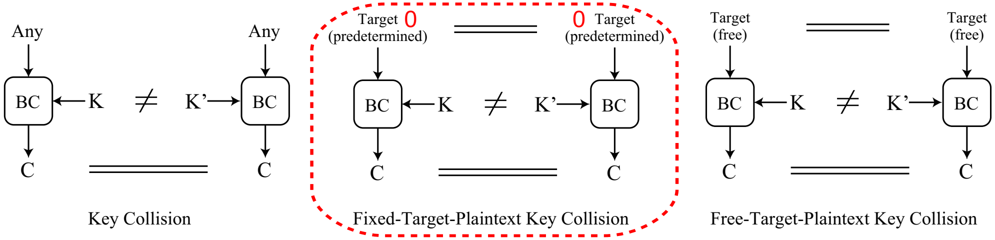


Figure: Variants of key collisions

Key Collision Attack

Target-Plaintext Key Collision [Taiyama et al., 2024]

It is two distinct keys that generate the same ciphertext for a single target plaintext.



AES

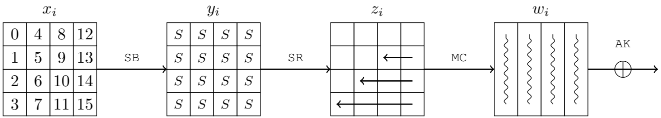


Figure: The round function of AES

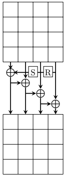


Figure: AES-128

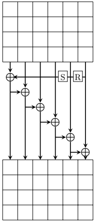


Figure: AES-192

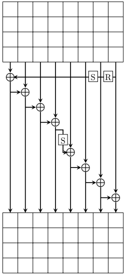
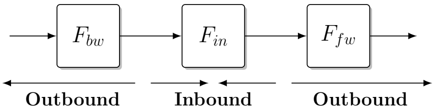


Figure: AES-256

Rebound Attack [Mendel et al., 2009]



- Split the internal block cipher or permutation F into $F = F_{fw} \circ F_{in} \circ F_{bw}$
  - **Inbound phase**: fulfill the low probability part of the differential with a meet-in-the-middle technique
  - **Outbound phase**: compute from the matched values backward and forward to satisfy the outbound differential trail in a brute-force fashion

Triangulating Rebound Attack [Dong et al., 2022]

- Connect multiple inbound phases with the available degrees of freedom both from the key schedule and the encryption path
- Solve a nonlinear system of the byte equations of AES with the help of triangulation algorithm

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

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

The Weaknesses of Dong et al.'s Triangulating Rebound

- **Weaknesses I**: Triangulation algorithm failed

$$\begin{cases} x \oplus y \oplus S(y) \oplus z \oplus S(z) \oplus t \oplus S(t) = 0, \\ S(x) \oplus y \oplus S(y) \oplus z \oplus S(z) \oplus t \oplus S(t) = 0, \\ x \oplus S(x) \oplus 2y \oplus S(y) \oplus 3z \oplus 3S(z) \oplus 2t \oplus 3S(t) = 0. \end{cases}$$

- [Bouillaguet et al., 2011] proposed the guess-and-determine method to solve the nonlinear system adopted the Gaussian elimination

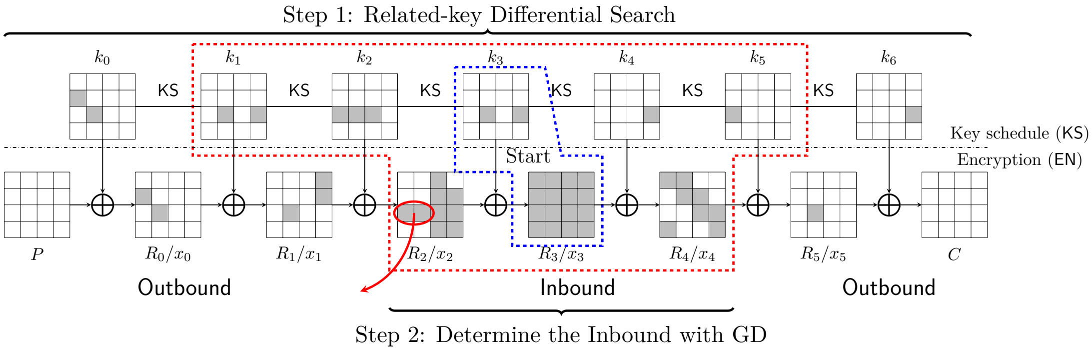
$$\begin{cases} z \oplus S(z) \oplus S(t) \oplus S(y) = 0, \\ t \oplus S(x) \oplus y \oplus 2S(y) = 0, \\ x \oplus S(x) \oplus 2S(y) = 0. \end{cases}$$

The Weaknesses of Dong et al.'s Triangulating Rebound

- **Weaknesses II**: Related-key differential unexplored on AES for triangulation rebound
  - Related-key differential may induce unexpected conflicts in the attack
  - The related-key differentials on 2-round AES-128 and 6-round AES-256 in [Taiyama et al., 2024] are invalid when searching $\mathrm{AES}_{K_1}(0) = \mathrm{AES}_{K_2}(0)$

Outline

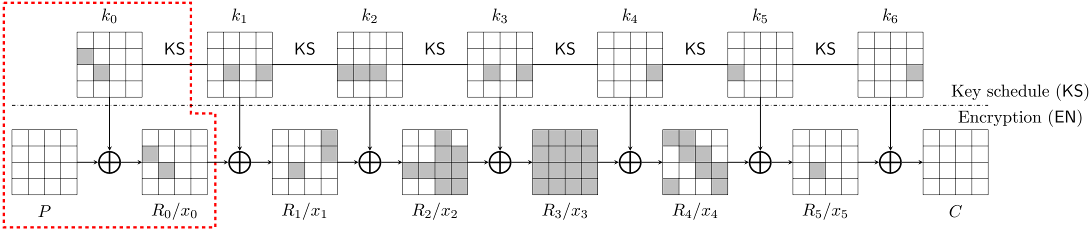
Guess-and-Determine Rebound Attack (GD rebound)



- **Step 1**: Search for related-key differentials suitable for key collisions on AES with [Gérault et al., 2020]'s model
- **Step 2**: Determine an efficient inbound phase by guess-and-determine

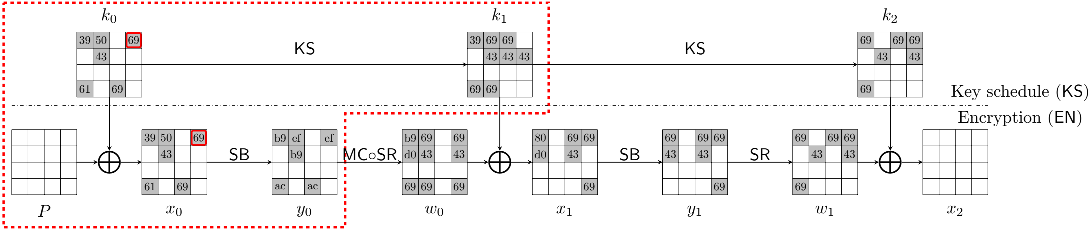
Step 1: Search for related-key differentials of AES

- **Collision condition**: $\Delta P = \Delta C = 0$
- **Degree of freedom (DoF)**: probability 2^{-p}
  - $p \leq |K|$ for fixed-target key collision
  - $p \leq n + |K|$ for free-target key collision
- **Restriction in round 0**: $\Delta x_0 = \Delta k_0$, $P = x_0 \oplus k_0$



Step 1: Search for related-key differentials of AES

- Key collision attack on 2-round AES-128 in [Taiyama et al., 2024]



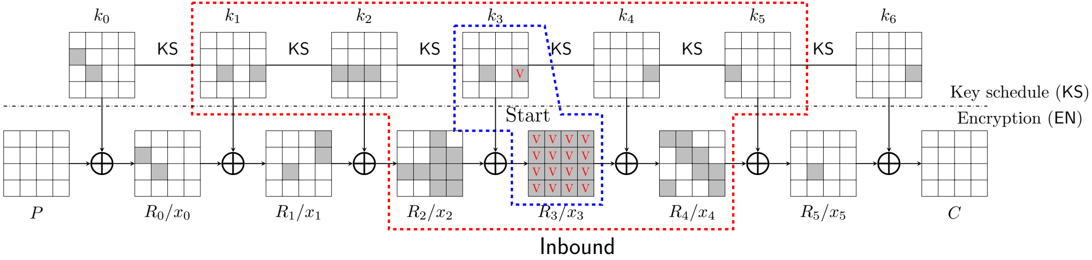
  - $(\Delta x_0[12], \Delta SB(x_0[12])) = (\texttt{0x69}, \texttt{0xef})$, $(\Delta k_0[12], \Delta SB(k_0[12])) = (\texttt{0x69}, \texttt{0x08})$
  - To fulfill the differential, $x_0[12] \in \{\texttt{0x1b}, \texttt{0x72}\}$, $k_0[12] \in \{\texttt{0x60}, \texttt{0x08}\}$
  - $P[12] = k_0[12] \oplus x_0[12] \neq 0$

Step 1: Search for related-key differentials of AES

Solve the incompatibility of KS and EN path in round 0

- Avoid activating Sbox in round 0 of the key schedule
  - $\Delta k_0[j] = 0$ ($j \in [12, 13, 14, 15]$) for AES-128
- Set the output differences of corresponding active Sbox in KS and EN path to be same
  - $\Delta k_0[j] = \Delta x_0[j]$ ($j \in [12, 13, 14, 15]$), $\Delta SB(k_0[j]) = \Delta SB(x_0[j])$ for AES-128
  - **Reconsideration of the probability**: Setting $k_0[j] = x_0[j]$, the probability only needs to be calculated once for two active Sboxes

Step 2: Determine the Inbound with guess-and-determine

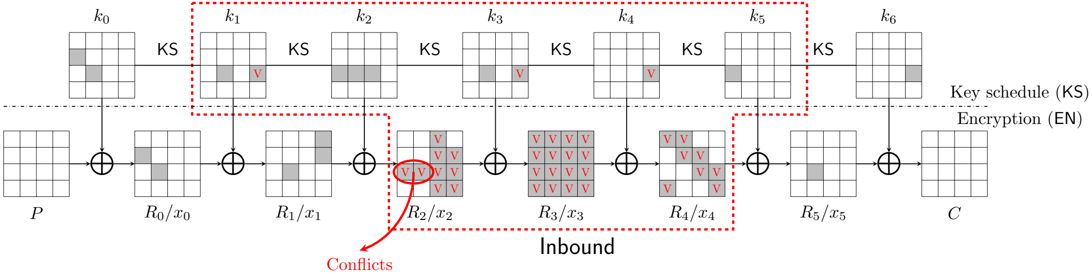


- Select the starting round as the initial Inbound
  - Fix all values of active Sboxes in KS and EN path of Inbound
  - Run Buillaguet et al.'s tool to get the guess-and-determine (GD) process of Inbound
  - c_{in} conflicts, $\mathcal{T}_{\text{GD}} = 2^{8c_{in}}$ to find one starting point

Step 2: Determine the Inbound with guess-and-determine

Conflicts in the guess-and-determine

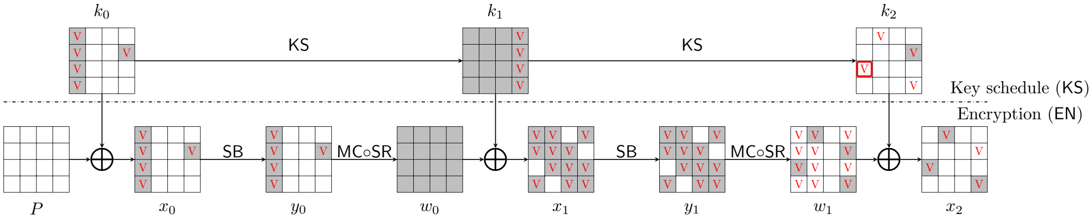
- **Type I**: Active sboxes falsely included in the Inbound



- Move c_1 **Type I** conflicts to the Outbound phase: $2^{8 \cdot c_1} \to 2^{(7 \text{ or } 6) \cdot c_1}$

Step 2: Determine the Inbound with guess-and-determine

- **Type II**: Conflict between KS and EN path



$$\begin{cases} k_2[2] = y_1[0] \oplus y_1[5] \oplus 02 \cdot y_1[10] \oplus 03 \cdot y_1[15] \oplus x_2[2], \\ k_2[2] = x_0[2] \oplus P[2] \oplus SB(k_1[15]). \end{cases}$$

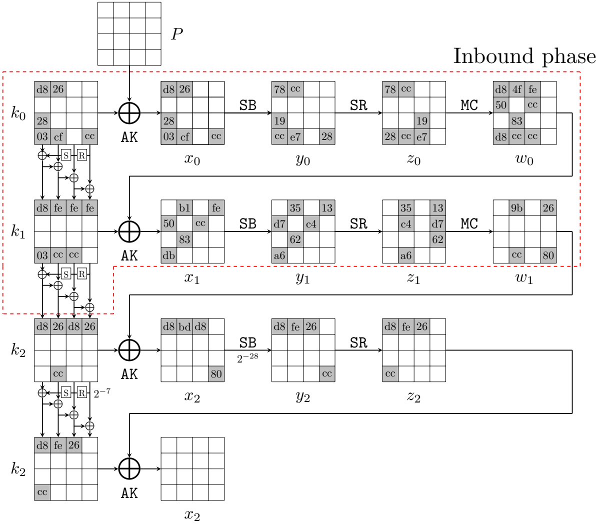
- **Type II** conflicts can be resolved by precomputation
- **Type III**: Internal conflict

Summary of the GD Rebound Attack

- **Time complexity**
  - Let the numbers of Type I/II/II conflicts be c_1, c_2, c_3
  - Time complexity of GD is $\mathcal{T}'_{\text{GD}} = \mathcal{T}_{\text{GD}}/2^{8(c_1+c_2)} = 2^{8c_3}$
  - Probability of the Outbound decreases to $2^{-p_{out}-(7 \text{ or } 6)\cdot c_1}$
  - Overall time complexity: $\mathcal{T} = 2^{8c_3} \cdot 2^{p_{out}+(7 \text{ or } 6)\cdot c_1}$
- Add more rounds of KS or EN into Inbound and update the probability of Outbound
  - Run the guess-and-determine tool to find a new GD and analyze the conflicts

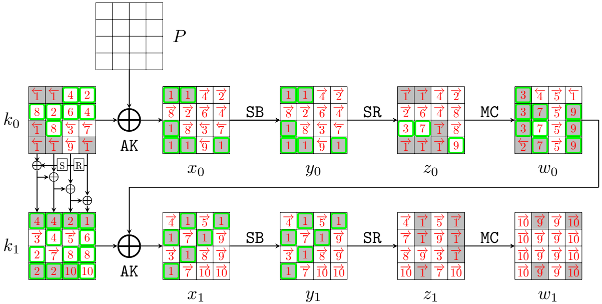
Outline

New Related-key Differential on 3-round AES-128



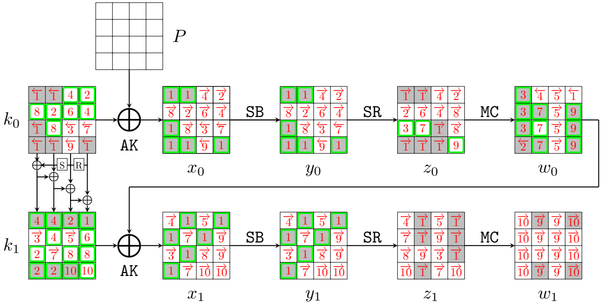
- $\Delta x_0[12] = \Delta k_0[12] =$ 0x69, $\Delta SB(x_0[12]) = \Delta SB(k_0[12]) =$ 0xef
- Keep $x_0[12] = k_0[12]$ for $P = 0$
- Probability $2^{-131} \rightarrow 2^{-125}$

The Practical Key Collision Attack on 3-round AES-128



1. Deduce $x_0[0, 2, 3, 4, 7, 15]$, $x_1[1, 3, 4, 6, 9, 12]$, $k_1[12]$ by the fixed differences $\boxed{1}$
   - Compute $k_0[0, 2, 3, 4, 7, 15] = (x_0 \oplus P)[0, 2, 3, 4, 7, 15]$ and $w_0[12] = k_1[12] \oplus x_1[12]$ ($\overleftarrow{1}$)
   - Deduce $z_0[0, 3, 4, 7, 10, 11]$ and $z_1[4, 5, 7, 12, 13, 14]$ ($\overrightarrow{1}$)

The Practical Key Collision Attack on 3-round AES-128



2. Guess $k_0[5, 12]$ 2
   - Deduce $k_1[2, 3, 7, 8]$ by key relation 2
   - Compute $z_0[1, 12]$ and $w_0[3]$
3. For column 0 over the MC of round 0
   - Deduce $w_0[0, 1, 2]$ and $z_0[2]$ 3 from $z_0[0, 1, 3]$ and $w_0[3]$
   - Compute $k_0[10]$ and $k_1[1]$

The Practical Key Collision Attack on 3-round AES-128

1.	$k_0[0,2,3,4,7,15] = (x_0 \oplus P)[0,2,3,4,7,15]$	$w_0[12] = k_1[12] \oplus x_1[12]$
2.	$k_1[3] = k_0[3] \oplus SB(k_0[12])$	$k_1[7] = k_0[7] \oplus k_1[3]$
	$k_1[8] = k_1[12] \oplus k_0[12]$	$k_1[2] = k_0[2] \oplus SB(k_0[15])$
	$z_0[1] = SB(k_0[5] \oplus P[5])$	
3.	$w_0[0,1,2], z_0[2] = \texttt{MC}(z_0[0,1,3], w_0[3])$	$k_0[10] = P[10] \oplus SB^{-1}(z_0[2])$
	$k_1[1] = w_0[1] \oplus x_1[1]$	
4.	$k_1[0] = k_0[0] \oplus SB(k_0[13]) \oplus const$	$k_1[4] = k_0[4] \oplus k_1[0]$
	$k_0[8] = k_1[8] \oplus k_1[4]$	$k_1[5] = k_0[5] \oplus k_1[1]$
5.	$w_0[8,9,10,11] = \texttt{MC}(z_0[8,9,10,11])$	$k_1[9] = w_0[9] \oplus x_1[9]$
6.	$k_0[9] = k_1[9] \oplus k_1[5]$	$k_1[13] = k_1[9] \oplus k_0[13]$
7.	$w_0[5,6,7], z_0[6] = \texttt{MC}(z_0[4,5,7], w_0[4])$	$k_0[14] = P[14] \oplus SB^{-1}(z_0[6])$
	$k_1[6] = w_0[6] \oplus x_1[6]$	
8.	$k_0[1] = k_1[1] \oplus SB(k_0[14])$	$k_0[6] = k_1[6] \oplus k_1[2]$
	$k_1[10] = k_1[6] \oplus k_0[10]$	$k_1[14] = k_1[10] \oplus k_0[14]$
9.	$w_0[13,14,15], z_0[15] = \texttt{MC}(z_0[12,13,14], w_0[12])$	$k_0[11] = P[11] \oplus SB^{-1}(z_0[15])$
10.	$k_1[11] = k_0[11] \oplus k_1[7]$	$k_1[15] = k_1[11] \oplus k_0[15]$

Table: Equations in the GD steps for 3-round AES-128. Blue bytes are guessed.

The Practical Key Collision Attack on 3-round AES-128

Degree of freedom

- Step 1, deduce $2^{12+2}/2 = 2^{13}$ values for active bytes [1] from the differences
  - $s_1 = 12$ active Sboxes with 2^{-7} and $s_2 = 1$ active Sboxes with 2^{-6} probability
- Step 2 and 4, guess $k_0[5, 12, 13]$
- $2^{13+24} = 2^{37}$ states satisfying the inbound trial

Time complexity

- $c_{in} = 0$, $\mathcal{T}_{\mathrm{GD}} = 1$ for finding one starting point
- $2^{-p_{out}} = 2^{-35}$, collect 2^{35} starting points to expect one collision
- Overall time complexity $\mathcal{T} = 2^{35}$

The Practical Key Collision Attack on 3-round AES-128

Experiments on fixed-target-plaintext key collisions

- Intel Core i7-13700F @2.1 GHz and 16G RAM

Key Collisions on 3-round AES-128 **for** $P = 0$
K_1 : 0x0f6eef4eea138a1b60057a26d30bedfa
K_2 : 0xd76ec74dcc138ad460057a26d30bed36
C : 0x87c494f5d33621b65ad032992b8f6def
K_1 : 0x0f06c74eeae0f2d494b699656837a236
K_2 : 0xd706ef4dcce0f21b94b699656837a2fa
C : 0xa10740d59630c5a0e1ac2462fb79349d
K_1 : 0x0f42ef4eea32361b5938c173b43fd7cc
K_2 : 0xd742c74dcc3236d45938c173b43fd700
C : 0x04a426d2376e704c409b8409cb6f02d1

Summary

- We introduced the guess-and-determine rebound attack
  - Exploring and identifying valid related-key differentials for key collision attack
  - Determining the range of Inbound phase with the guess-and-determine technique and handling the conflicts flexibly
- Applied to AES-128/192/256 for fixed-target-plaintext key collision and free-target-plaintext key collision
  - The theoretical key collision attacks on AES in [Taiyama et al., 2024] are improved to practical ones
  - A new 3-round practical key collision attack on AES-128
  - Some quantum key collisions attacks and semi-free-start key collision attacks

Results

Target	Attack	Rounds	Time	C-Mem	qRAM	Setting	Ref.
AES-128	Key Collision	2/10	2^{49}	-	-	Classic	[Taiyama et al., 2024]
		2/10	Practical	2^{22}	-	Classic	[Ni et al., 2025]
		2/10	2^{6} Practical	-	-	Classic	Ours
		3/10	2^{35} Practical	-	-	Classic	Ours
	DM mode	5/10	2^{57}	-	-	Classic	[Taiyama et al., 2024]
	Semi-free-start	5/10	2^{54}	-	-	Classic	[Ni et al., 2025]
		5/10	2^{39}	-	-	Classic	Ours
AES-192	Key Collision	5/12	2^{61}	-	-	Classic	[Taiyama et al., 2024]
		5/12	Practical	2^{5}	-	Classic	[Ni et al., 2025]
		5/12	2^{21} Practical	-	-	Classic	Ours
		6/12	$2^{38.7}$		44	Quantum	Ours
	DM mode	7/12	2^{62}	-	-	Classic	[Taiyama et al., 2024]
	Semi-free-start	7/12	2^{56}	-	-	Classic	[Ni et al., 2025]
		7/12	2^{20} Practical	-	-	Classic	Ours
AES-256	Key Collision	6/14	2^{61}	-	-	Classic	[Taiyama et al., 2024]
		6/14	2^{60}	-	-	Classic	[Ni et al., 2025]
		6/14	2^{21} Practical	-	-	Classic	Ours
		7/14	$2^{36.7}$		60	Quantum	Ours

Thanks for your attention!

References I

Albertini, A., Duong, T., Gueron, S., Kölbl, S., Luykx, A., and Schmieg, S. (2022).
How to abuse and fix authenticated encryption without key commitment.
In *USENIX Security 2022*, pages 3291–3308.

Bouillaguet, C., Derbez, P., and Fouque, P. (2011).
Automatic search of attacks on round-reduced AES and applications.
In *CRYPTO 2011*, pages 169–187.

Dong, X., Guo, J., Li, S., and Pham, P. (2022).
Triangulating rebound attack on aes-like hashing.
In *CRYPTO 2022*, pages 94–124.

Gérault, D., Lafourcade, P., Minier, M., and Solnon, C. (2020).
Computing AES related-key differential characteristics with constraint programming.
Artif. Intell., 278.

References II

Mendel, F., Rechberger, C., Schläffer, M., and Thomsen, S. S. (2009).
The rebound attack: Cryptanalysis of reduced Whirlpool and Grøstl.
In *FSE 2009*, pages 260–276.

Ni, J., Li, Y., Liu, F., and Wang, G. (2025).
Practical key collision on AES and kiasu-bc.
IACR Cryptol. ePrint Arch., page 462.

Taiyama, K., Sakamoto, K., Ito, R., Taka, K., and Isobe, T. (2024).
Key collisions on AES and its applications.
In *ASIACRYPT 2024*, pages 267–300.