Generic Differential Key Recovery Attacks and Beyond

Ling Song, **Huimin Liu**, Qianqian Yang, Yincen Chen, Lei Hu, Jian Weng

ASIACRYPT 2024

中国科学院信息工程研究所
INSTITUTE OF INFORMATION ENGINEERING,CAS

暨南大學
JINAN UNIVERSITY

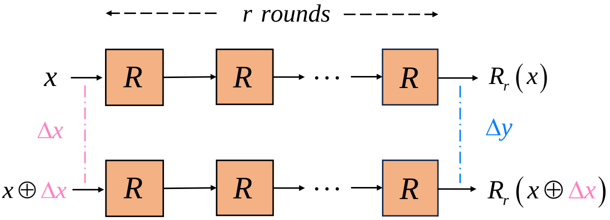
Outline

Outline

Background

Differential attack

- Differential cryptanalysis was introduced by Biham and Shamir in 1990. [BS90, BS91]
- Find a high-probability differential $(\Delta x, \Delta y)$ covering a large number of rounds

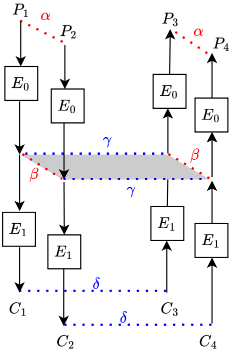


- the probability of $(\Delta x, \Delta y)$ should be higher than 2^{-n}, where n is the block size

Background

Boomerang attack

- Connect two short differentials of high probability to construct a long differential trail



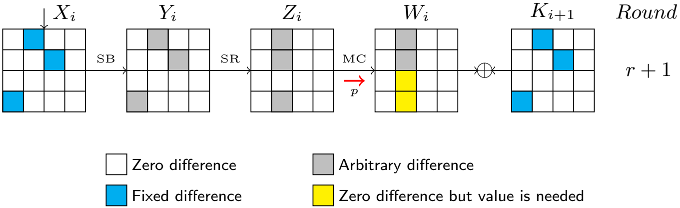
Rectangle attack (Chosen-plaintext variant of boomerang attack)

- More common for key recovery attacks

Background

Key recovery

- Structures of data [BS92]
  - ★ Enjoy the birthday effect and potentially attack more rounds without increasing the data complexity
- The probabilistic extensions [SYC+24]

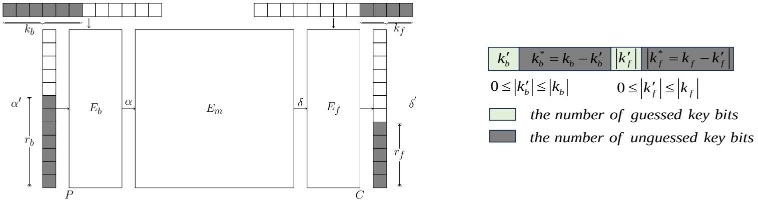


- Key guessing strategy
  - ★ The order of guessing key information
  - ★ The flexible guessing strategy

Outline

The generic classical rectangle attack (GCRA) [SZY$^+$22]

- Guess some key bits $|k'_b \cup k'_f|$ before any quartets are generated



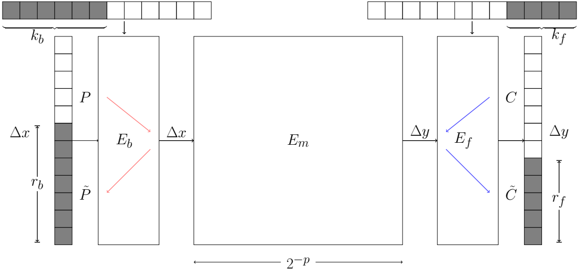
★ r'_b/r'_f: The condition can be verified under the guess of k'_b/k'_f;

★ $r^*_b = r_b - r'_b$; $r^*_f = r_f - r'_f$

- Select appropriate parameters $|k'_b|$, $|k'_f|$ to obtain optimal time complexity

The basic differential MITM attack(BDMA) [BDD+23]

- Guess **all** key information involved in the E_b and E_f parts, respectively



- More efficient when the key size of the cipher is bigger than the state size

New Generic Key Recovery Attacks

GCRA. [SZY+22] Guess some key bits in advance and adopt the flexible key-guessing strategy

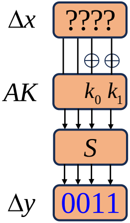
BDMA. [BDD+23] Employ a fixed key guessing strategy

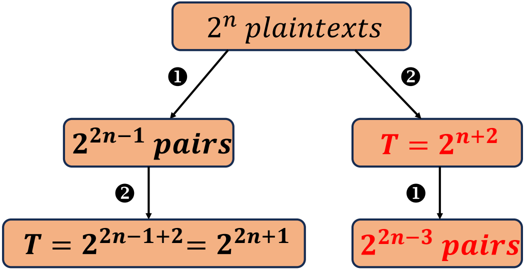
Questions:

- Can guessing some key bits in advance affect the time complexity of the differential attack? [**YES!** the generic classical differential attack(GCDA)]
- Can BDMA be generalized to support any key guessing strategy? [**YES!** the generic differential MITM attack(GDMA)]
- Can the MITM technique be integrated into GCRA? [**YES!** the generic rectangle MITM attack(GRMA)]

Outline

New Generic Key Recovery Attacks





❶: Generate pairs

❷: Guess 2-bit key

- **lower time complexity** ✔
- **reduce the number of pairs** ✔

New Generic Key Recovery Attacks

- Based on a distinguisher with probability 2^{-p}
- Data complexity: $D = 2^{p+1}$
- Steps:
  - Guess a part of key information k'_b, k'_f: $T_1 = 2^{|k'_b \cup k'_f|} \cdot D$
  - For each structure S_i of 2^{r_b} plaintexts, $0 \leq i \leq 2^{p-r_b+1} - 1$:
    - Generate $2^{2r_b-1+r_f-n-r'_b-r'_f}$ pairs;
      $T_2 = 2^{r_b-1+|k'_b \cup k'_f|+r_f-n-r'_b-r'_f} \cdot D$
    - Extract the extra key information k^*_b, k^*_f; $T_3 = 2^{|k_b \cup k_f|+p-n} \cdot \epsilon$
    - The exhaustive search. $T_4 = 2^{k+p-n}$

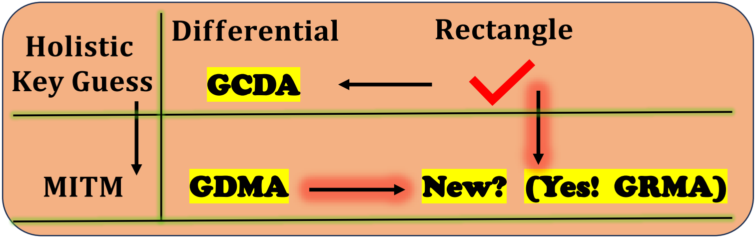
New Generic Key Recovery Attacks

- Combine the MITM technique with the flexible key guessing strategy
- Steps:
  - For each structure S_i of 2^{r_b} plaintexts, $0 \leq i \leq 2^{p-r_b+1}-1$:
  - Guess a part of key information k'_b: $T_{1,0} = 2^{|k'_b|} \cdot D$
    - Generate $2^{2r_b-1+r_f-n-r'_b}$ pairs; $T_{2,0} = 2^{r_b-1+|k'_b|+r_f-n-r'_b} \cdot D$
  - Guess a part of key information k'_f: $T_{1,1} = 2^{|k'_f|} \cdot D$
    - Generate $2^{2r_b-1+r_f-n-r'_f}$ pairs; $T_{2,1} = 2^{r_b-1+|k'_f|+r_f-n-r'_f} \cdot D$
    - Match Phase. Generate $2^{2r_b-1+r_f-n-r'_b-r'_f}$ pairs; $T_{2,2} = 2^{r_b-1+|k'_b \cup k'_f|+r_f-n-r'_b-r'_f} \cdot D$
    - Extract the extra key information k^*_b, k^*_f; $T_3 = 2^{|k_b \cup k_f|+p-n} \cdot \epsilon$
    - The exhaustive search. $T_4 = 2^{k+p-n}$

New Generic Key Recovery Attacks

Question:

- Can we combine the MITM technique with the rectangle attack?



Answer:

- Yes! The generic rectangle MITM attack (GRMA)

More effective when the ratio k/n is large

New Generic Key Recovery Attacks

- Based on a boomerang distinguisher with probability 2^{-2p}
- Construct y structures, each of 2^{r_b} plaintexts
- Data complexity: $D = 2^{n/2+p+1}$
- Steps:
  - Guess a part of key information k'_b: $T_{1,0} = 2^{|k'_b|} \cdot D$
    - Generate $D^2 \cdot 2^{2r_b^*-2}$ quartets; $T_{2,0} = 2^{2r_b^*-2+|k'_b|} \cdot D^2$
  - Guess a part of key information k'_f: $T_{1,1} = 2^{|k'_f|} \cdot D$
    - Generate $D^4 \cdot 2^{2r_f^*-2n-2} \cdot y^{-2}$ quartets; $T_{2,1} = 2^{|k'_f|+2r_f^*-2n-2 \cdot y^{-2}} \cdot D^4$
    - Extract the extra key information k_b^*, k_f^*; $T_3 = 2^{|k_b \cup k_f|} \cdot D^2 \cdot 2^{-2n-2} \cdot \epsilon$
    - The exhaustive search. $T_4 = 2^{k+p-n}$

Achieve a first 38-round attack on SKINNYe-64-256 v2

BDMA [BDD$^+$23] vs GDMA.

Table: Time Complexities Comparison of BDMA and GDMA

	BDMA		GDMA
T_0	D	$=$	D
T_1	$(2^{k_f} + 2^{k_b}) \cdot D$	$\geq$	$(2^{k'_f} + 2^{k'_b}) \cdot D$
T_2	–	$\leq$	$D \cdot 2^{\lvert k'_b \rvert} \cdot 2^{r_b - 1 + r_f - n - r'_b}$
	–		$D \cdot 2^{\lvert k'_f \rvert} \cdot 2^{r_b - 1 + r_f - n - r'_f}$
	–		$D \cdot 2^{\lvert k'_b \rvert \cup \lvert k'_f \rvert} \cdot 2^{r_b - 1 + r_f - n - r'_b - r'_f}$
T_3	$2^{\lvert k_b \cup k_f \rvert - n + p}$	$\leq$	$2^{\lvert k_b \cup k_f \rvert - n + p} \cdot \epsilon$
T_4	2^{k-n+p}	$=$	2^{k-n+p}

The GDMA can be seen as a generalization of BDMA.

GCDA vs GDMA.

Table: Time Complexities Comparison of GCDA and GDMA

	GCDA		GDMA
T_0	D	=	D
T_1	$2^{k'_f+k'_b} \cdot D$	$\geq$	$(2^{k'_f} + 2^{k'_b}) \cdot D$
T_2	–	$\leq$	$D \cdot 2^{\lvert k'_b \rvert} \cdot 2^{r_b-1+r_f-n-r'_b}$
	–		$D \cdot 2^{\lvert k'_f \rvert} \cdot 2^{r_b-1+r_f-n-r'_f}$
	$D \cdot 2^{\lvert k'_b \rvert \cup \lvert k'_f \rvert} \cdot 2^{r_b-1+r_f-n-r'_b-r'_f}$		$D \cdot 2^{\lvert k'_b \rvert \cup \lvert k'_f \rvert} \cdot 2^{r_b-1+r_f-n-r'_b-r'_f}$
T_3	$2^{\lvert k_b \cup k_f \rvert - n+p} \cdot \epsilon$	=	$2^{\lvert k_b \cup k_f \rvert - n+p} \cdot \epsilon$
T_4	2^{k-n+p}	=	2^{k-n+p}

- If T_1 is dominant, GDMA outperforms GCDA.
- If $r'_b \leq \lvert k'_b \rvert$ and $r'_f \leq \lvert k'_f \rvert$, GDMA will not be worse than GCDA.

BDMA, GCDA, and GDMA.

When the overall time complexity reaches $2^{|k_b \cup k_f|+p-n}$, there are ways to balance.

- If the exhaustive search time complexity is high, **the counting method** can be used to select the most likely candidates to test.
- The holistic key guessing strategy can balance T_1 and T_2.
- If T_3 is large due to a large ϵ, precomputed tables may help to reduce ϵ.

New Generic Key Recovery Attacks

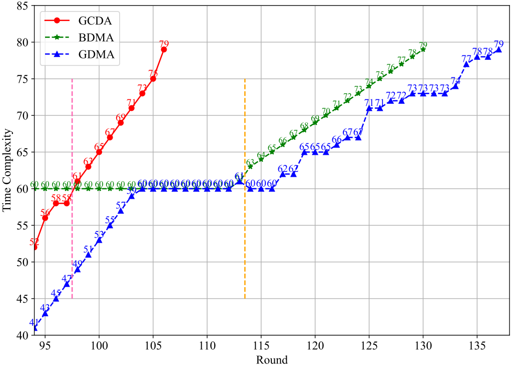
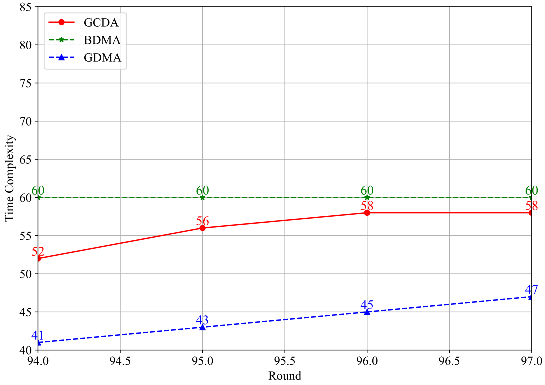


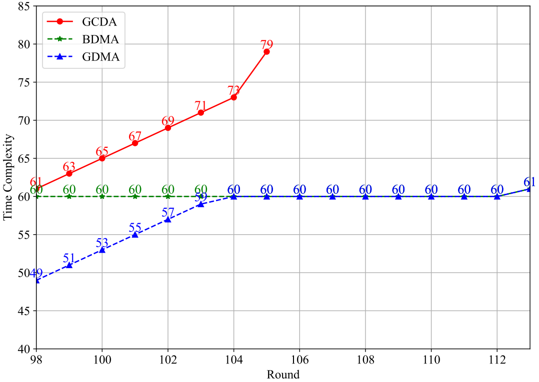
Figure: The time complexity of three attacks on KATAN-32.

- GDMA **always** performs better than GCDA on KATAN-32.

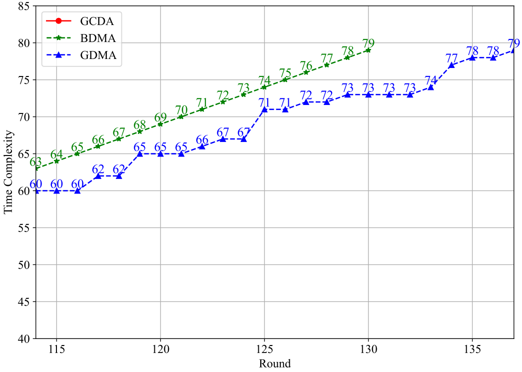


- The last part 2^{k-n+p} of BDMA's time complexity is dominant, while GCDA and GDMA can use **the counting method** to reduce it.

New Generic Key Recovery Attacks



- GCDA is worse than BDMA and GDMA when T_1 dominants;
- GDMA outperforms BDMA, when $k_b \cup k_f$ is not full key space;
- When $k_b \cup k_f$ reaches full key space, the time complexities of BDMA and GDMA are the same.

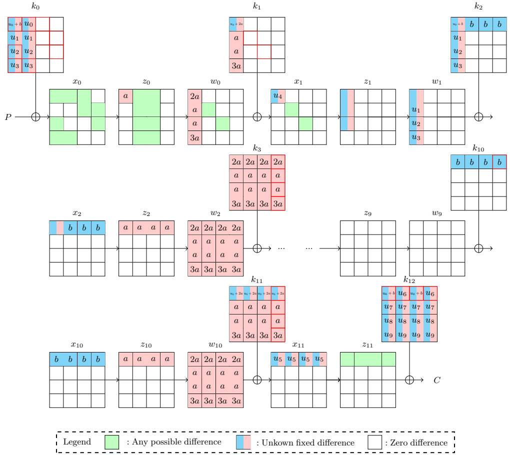


- $T_1^{BDMA} = 2^{|k_b|+|k_f|} \cdot 2^p$;
- $T_1^{GDMA} = 2^{|k'_b|+|k'_f|} \cdot 2^p$;
- GDMA has a lower time complexity than BDMA [BDD+23];
- GDMA adopts **flexible** key guessing strategy.

Outline

Attacks on 12-round AES-256

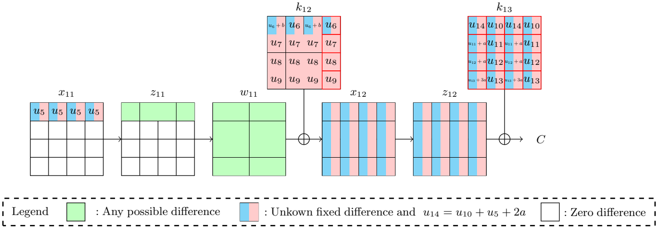
- Based on a 9-round distinguisher with probability $p = 2^{-86}$



- $|k_b| = 120, |k_f| = 64;$ $|r_b| = 88, |r_f| = 56;$
- $|k'_b| = 32, |r'_b| = 16;$ $|k'_f| = 24, |r'_f| = 16;$
- $T_{BDMA} = 2^{206}$ [BDD+23]
- $\boldsymbol{T_{GCDA} = 2^{145}}$
- $\boldsymbol{T_{GDMA} = 2^{144}}$

Attacks on 13-round AES-256

- Based on a 9-round distinguisher with probability $p = 2^{-86}$



- $|k_b| = 120, |k_f| = 224; |r_b| = 88, |r_f| = 128;$
- $|k'_b| = 16, |r'_b| = 16; |k'_f| = 72, |r'_f| = 8;$
- $T_{BDMA} = 2^{342}$ ✗
- $\boldsymbol{T_{GCDA} = 2^{240}}$

Applications

Table 1: Summary of the cryptanalytic results. RK: related-key. SK: single-key.

Cipher	Rounds	Data	Time	Memory	Setting	Type
AES-256	12	2^{89}	2^{214}	2^{89}	RK	BDMA [BDD+23]
			2^{206}	2^{184}	RK	BDMA [BDD+23]
			$\mathbf{2^{185}}$	$\mathbf{2^{89}}$	RK	GCDA (Section 4.1)
			$\mathbf{2^{144}}$	$\mathbf{2^{184}}$	RK	GDMA (Section 4.1)
			$\mathbf{2^{145}}$	$\mathbf{2^{128}}$	RK	GCDA (Section 4.1)
	13	2^{126}	2^{253}	2^{89}	RK	BDMA [BDF23]
		2^{126}	2^{250}	2^{231}	RK	BDMA [BDF23]
		$\mathbf{2^{89}}$	$\mathbf{2^{248}}$	$\mathbf{2^{89}}$	RK	GCDA (Section 4.1)
		$\mathbf{2^{89}}$	$\mathbf{2^{240}}$	$\mathbf{2^{144}}$	RK	GCDA (App. A.3)
KATAN-32	115	2^{32}	$2^{79.98}$	–	SK	Differential [AL13]
	151		$2^{79.98}$	2^{38}	SK	BDMA (Section 4.2)
SKINNYe-64-256 v2	37	$2^{62.8}$	$2^{240.03}$	$2^{62.8}$	RK	Rectangle [QDW+22]
	38	$\mathbf{2^{65.4}}$	$\mathbf{2^{251.07}}$	$\mathbf{2^{254.8}}$	RK	GRMA (Section 4.3)

Outline

Summary

Three generic key recovery attacks

- ★ GCDA: encompassing the previous differential attack with any key guessing strategies
- ★ GDMA: introducing the flexible key guessing strategy into the BDMA
- ★ GRMA: employing the MITM technique into GCRA

$\hookrightarrow$ A series of improved results

Thank you!

Q & A

References I

Christina Boura, Nicolas David, Patrick Derbez, Gregor Leander, and María Naya-Plasencia, Differential meet-in-the-middle cryptanalysis, Advances in Cryptology - CRYPTO 2023 - 43rd Annual International Cryptology Conference, CRYPTO 2023, Santa Barbara, CA, USA, August 20-24, 2023, Proceedings, Part III (Helena Handschuh and Anna Lysyanskaya, eds.), Lecture Notes in Computer Science, vol. 14083, Springer, 2023, pp. 240–272.

Eli Biham and Adi Shamir, Differential cryptanalysis of DES-like cryptosystems, Advances in Cryptology - CRYPTO '90, 10th Annual International Cryptology Conference, Santa Barbara, California, USA, August 11-15, 1990, Proceedings (Alfred Menezes and Scott A. Vanstone, eds.), Lecture Notes in Computer Science, vol. 537, Springer, 1990, pp. 2–21.

Eli Biham and Adi Shamir, Differential cryptanalysis of des-like cryptosystems, Journal of CRYPTOLOGY **4** (1991), 3–72.

References II

- Eli Biham and Adi Shamir, Differential cryptanalysis of the full 16-round DES, Advances in Cryptology - CRYPTO '92, 12th Annual International Cryptology Conference, Santa Barbara, California, USA, August 16-20, 1992, Proceedings (Ernest F. Brickell, ed.), Lecture Notes in Computer Science, vol. 740, Springer, 1992, pp. 487–496.
- Ling Song, Qianqian Yang, Yincen Chen, Lei Hu, and Jian Weng, Probabilistic extensions: a one-step framework for finding rectangle attacks and beyond, Annual International Conference on the Theory and Applications of Cryptographic Techniques, Springer, 2024, pp. 339–367.
- Ling Song, Nana Zhang, Qianqian Yang, Danping Shi, Jiahao Zhao, Lei Hu, and Jian Weng, Optimizing rectangle attacks: A unified and generic framework for key recovery, ASIACRYPT (2022).