Security Analysis of PRINCE

Jérémy Jean, Ivica Nikolić, Thomas Peyrin, Lei Wang, Shuang Wu

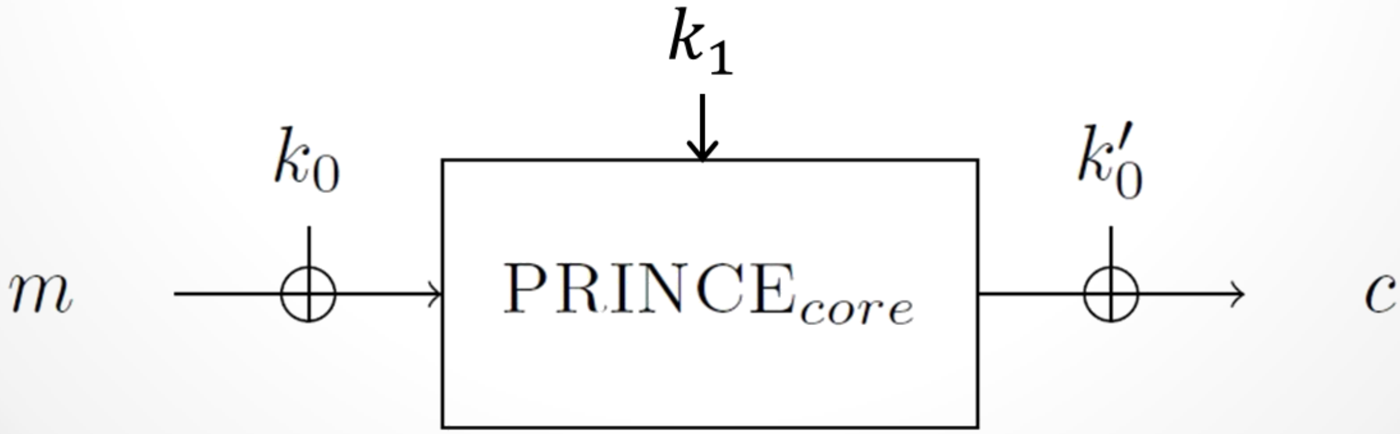
École Normale Superieure, France
Nanyang Technological University, Singapore

FSE 2013

Singapore – March 11, 2013

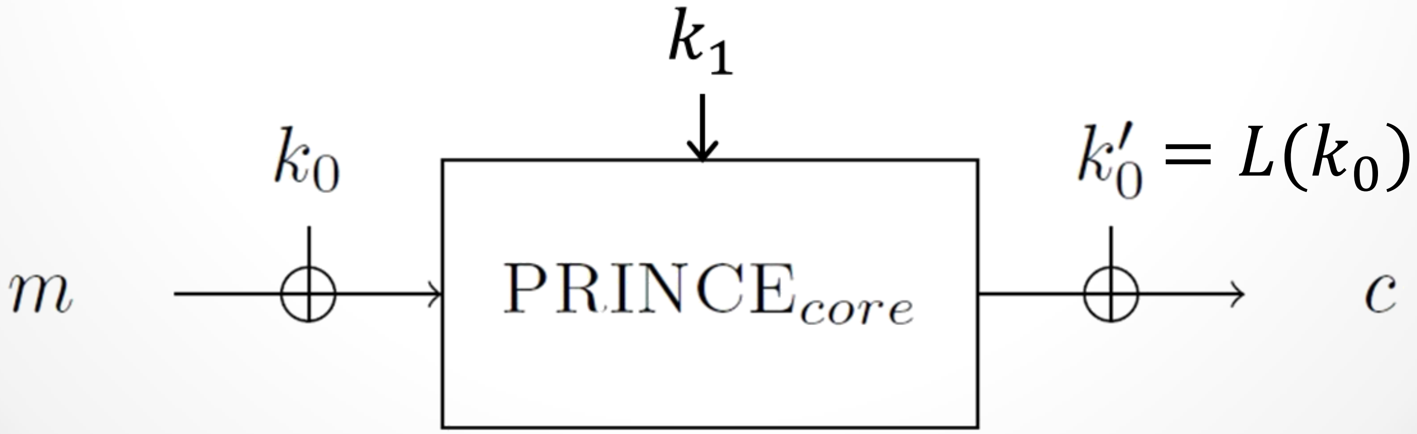
Introduction

- What is PRINCE
  - A lightweight block cipher published at ASIACRYPT 2012
  - Based on Even-Mansour-like and more importantly FX construction
  - 128-bit key, 64-bit data



Introduction

- Specification of PRINCE
  - Key expansion:
    - $k = (k_0||k_1) \to (k_0||k_0'||k_1),\ k_0' = L(k_0)$
    - $L(x) = (x \ggg 1) \oplus (x \gg 63)$



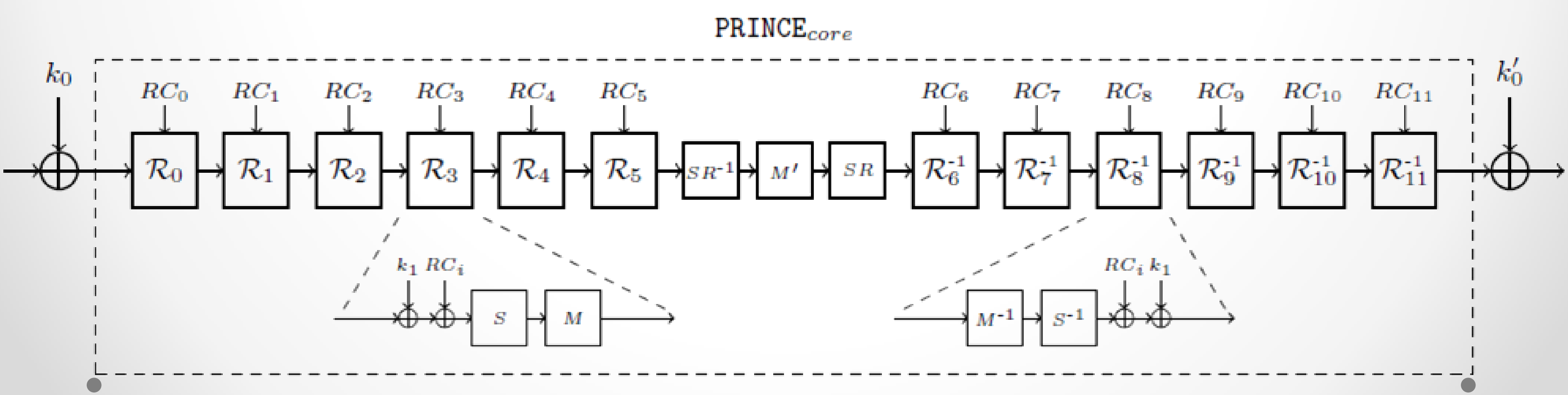
Introduction

- Specification of PRINCE
  - 12-round SPN structure in PRINCE$_{core}$
  - Symmetric construction
  - Round constants are related

$$RC_i \oplus RC_{11-i} = \alpha = 0xc0ac29b7c97c50dd$$

  - α-reflection property

$$D_{k_0||k_0'||k_1}(\cdot) = E_{k_0'||k_0||k_1 \oplus \alpha}(\cdot)$$



Introduction

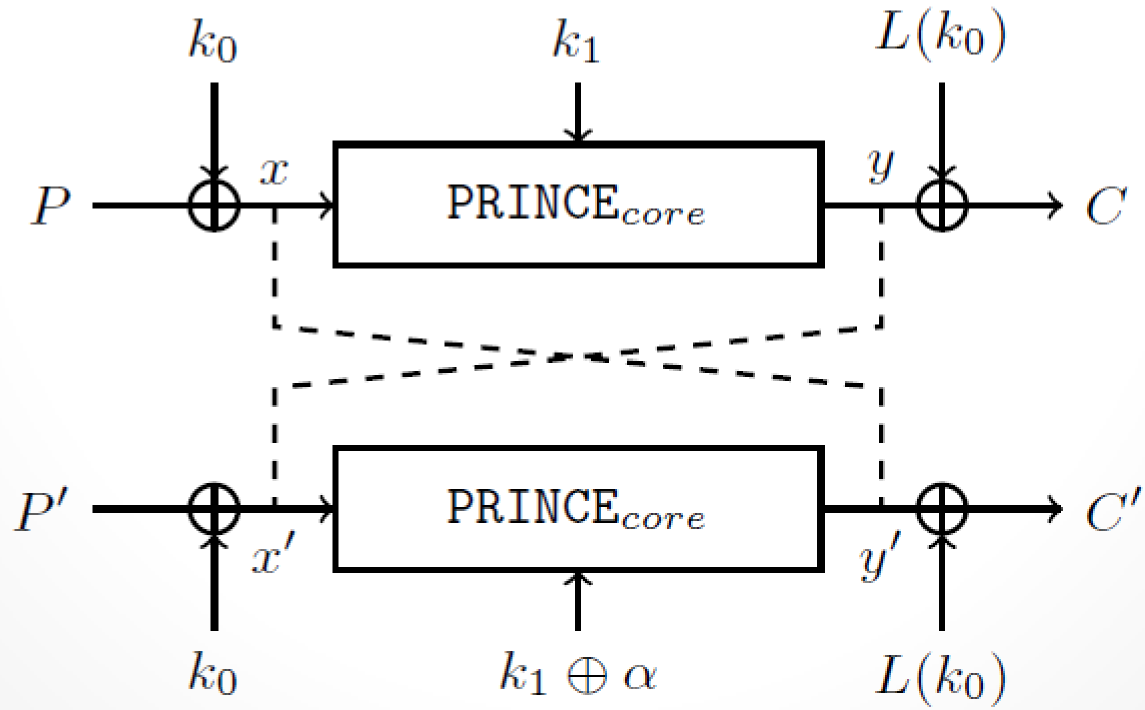
- Claimed Security of PRINCE
  - Single-key attack: 2^{127-n}
    - When 2^{n} queries are made
  - Related-key attack: No bound claimed
    - Only a trivial related-key distinguisher is given

Our Results

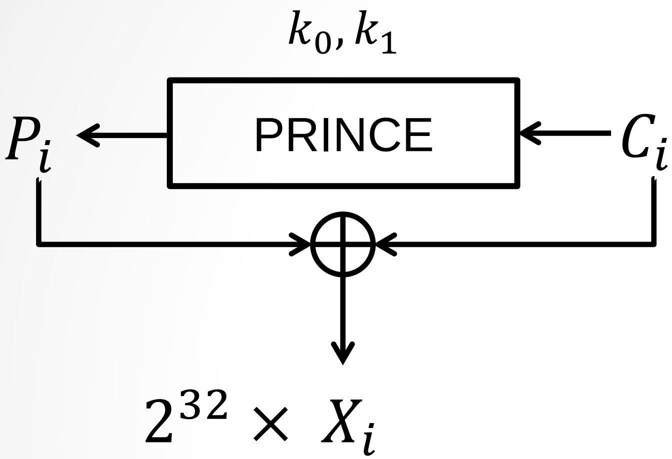
- Related-key Attacks on Full PRINCE
- Single-key Attack on $\text{PRINCE}_{\text{core}}$ with chosen-α
- Single-key Attack on Full PRINCE with $2^{126.47-n}$
- Integral Attack on 6 rounds
- Time-Memory-Data Tradeoffs

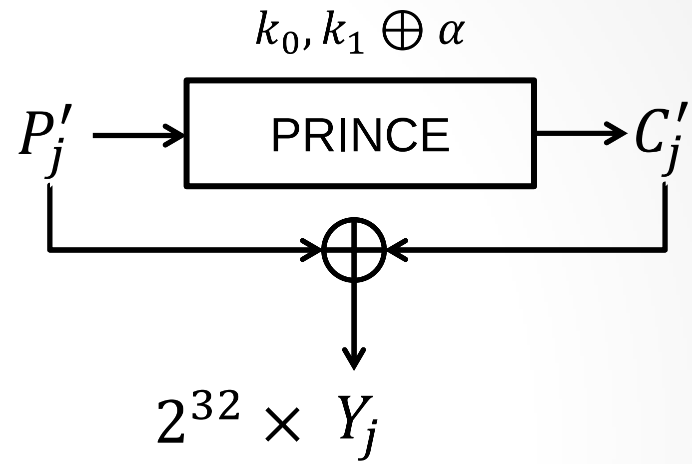
Related-key Attacks on full PRINCE

- $k = (k_0||k_1), k' = (k_0||k_1 \oplus \alpha)$
- **Property 1**. Let $C = PRINCE_k(P), C' = PRINCE_{k'}(P')$. $C \oplus P' = k_0 \oplus L(k_0) \Rightarrow C' \oplus P = k_0 \oplus L(k_0)$

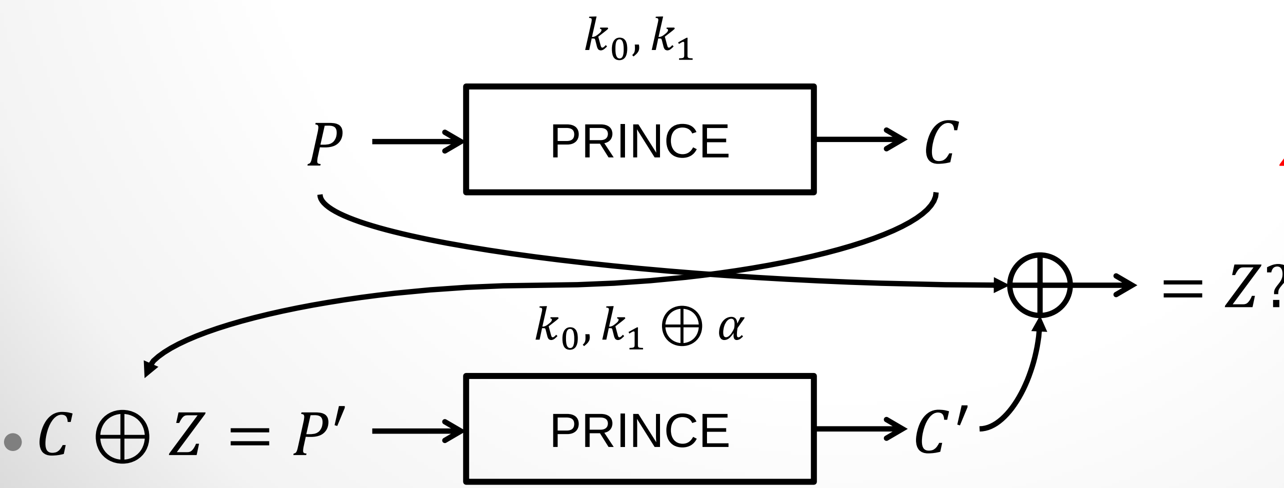


Related-key Attacks on full PRINCE





A collision $X_i = Y_j$ suggests that $Z = C_i \oplus P'_j$ is a possible candidate of $k_0 \oplus L(k_0)$



$Z = k_0 \oplus L(k_0)$

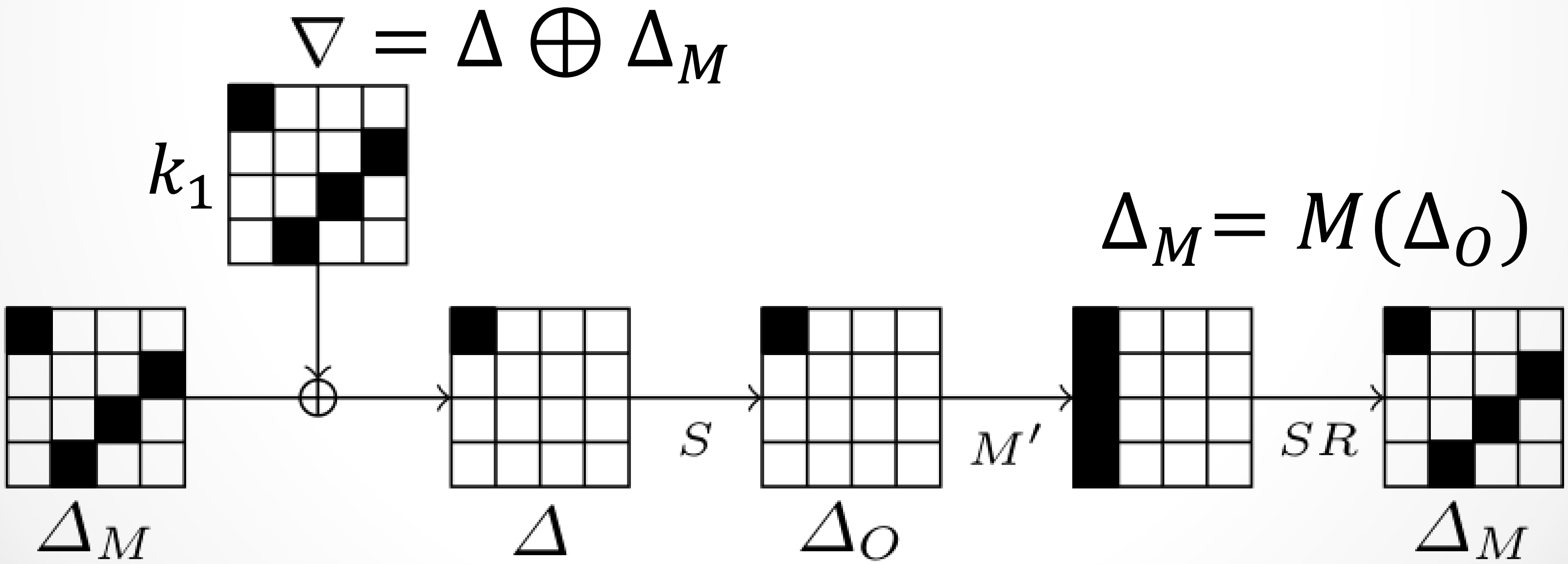
k_0		k_1		
2^{32}	$+$	2^{64}	$\approx$	2^{64}

Our Results

- Related-key Attacks on Full PRINCE
- Single-key Attack on $\mathrm{PRINCE}_{\mathrm{core}}$ with chosen-α
- Single-key Attack on Full PRINCE with $2^{126.47-n}$
- Integral Attack on 6 rounds
- Time-Memory-Data Tradeoffs

Related-key Boomerang Attack on PRINCE$_{core}$

- **Property 2**. For the S-box of PRINCE, optimal input-output differences holds with probability 2^{-2}



$\Pr[\Delta \rightarrow \Delta_O] = 2^{-2}$

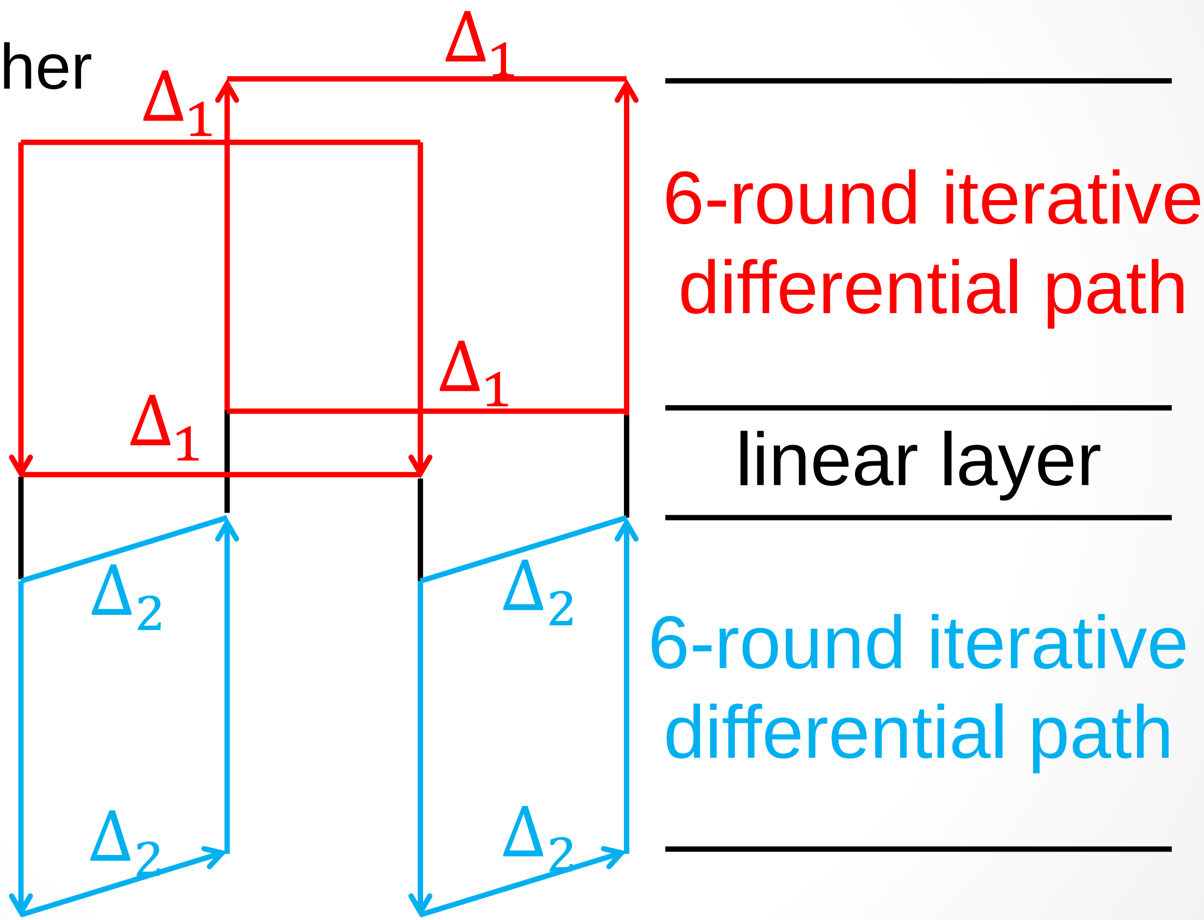
Related-key Boomerang Attack on $\text{PRINCE}_{\text{core}}$

- The distinguisher

$p = (2^{-2})^6 = 2^{-12}$

$(pq)^2 = 2^{-48}$

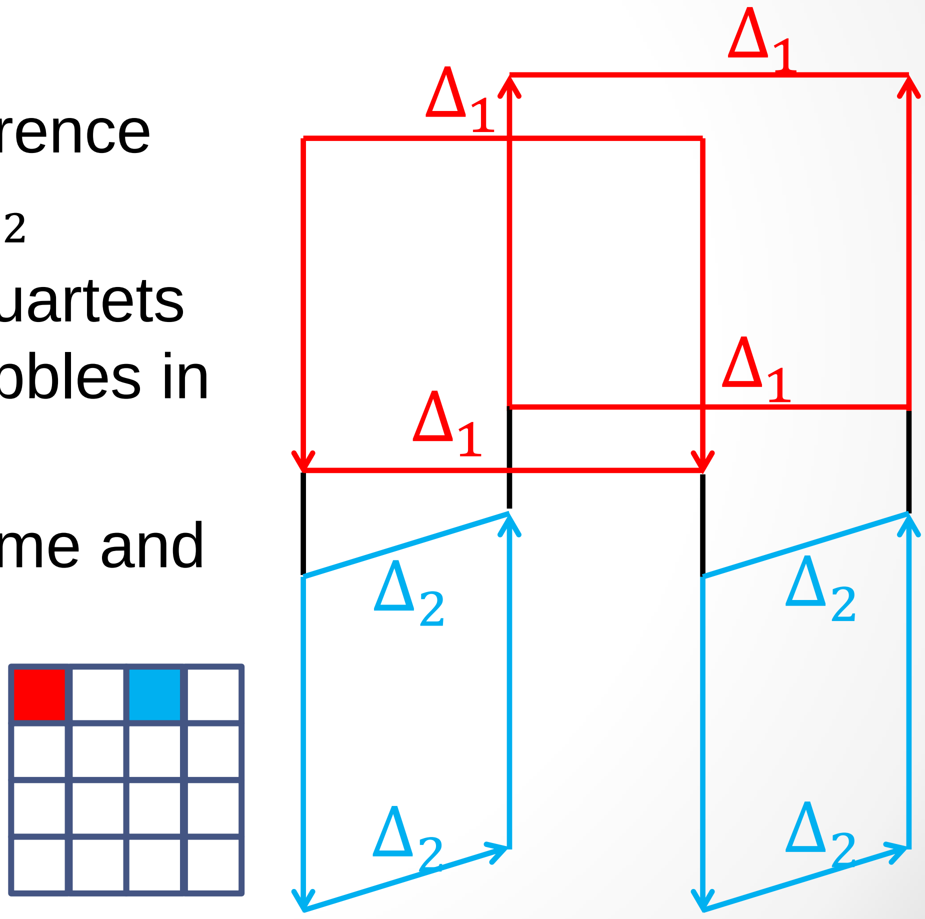
$q = (2^{-2})^6 = 2^{-12}$



Experimental probability (amplified) $\approx 2^{-36}$

Related-key Boomerang Attack on PRINCE_{core}

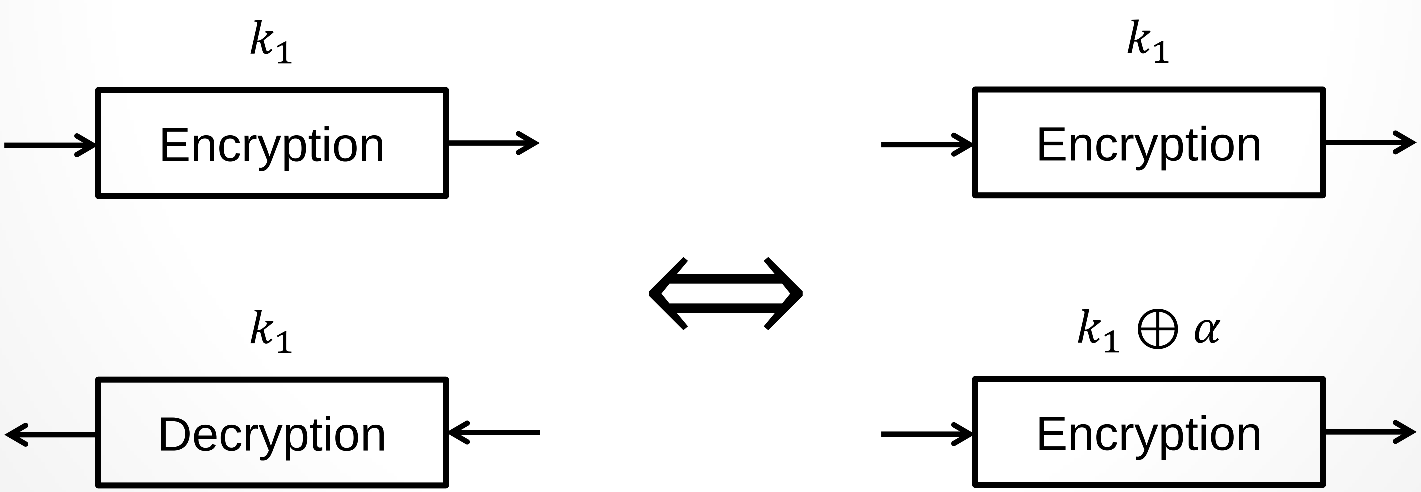
- Key recovery
  - Choose distinct difference positions in Δ_1 and Δ_2
  - Find 8 boomerang quartets to cover all the 16 nibbles in the key
  - Complexity: $8 \cdot 2^{36}$ time and chosen data



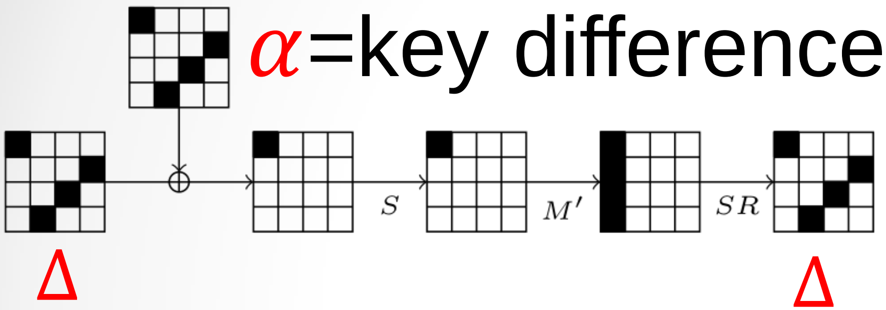
Single-key Attack on $\text{PRINCE}_{\text{core}}$ with chosen-α

- The α-reflection property
  - In single-key attack, the decryption oracle can be used as related-key encryption oracle

$$D_{k_1}(X) = E_{k_1 \oplus \alpha}(X)$$



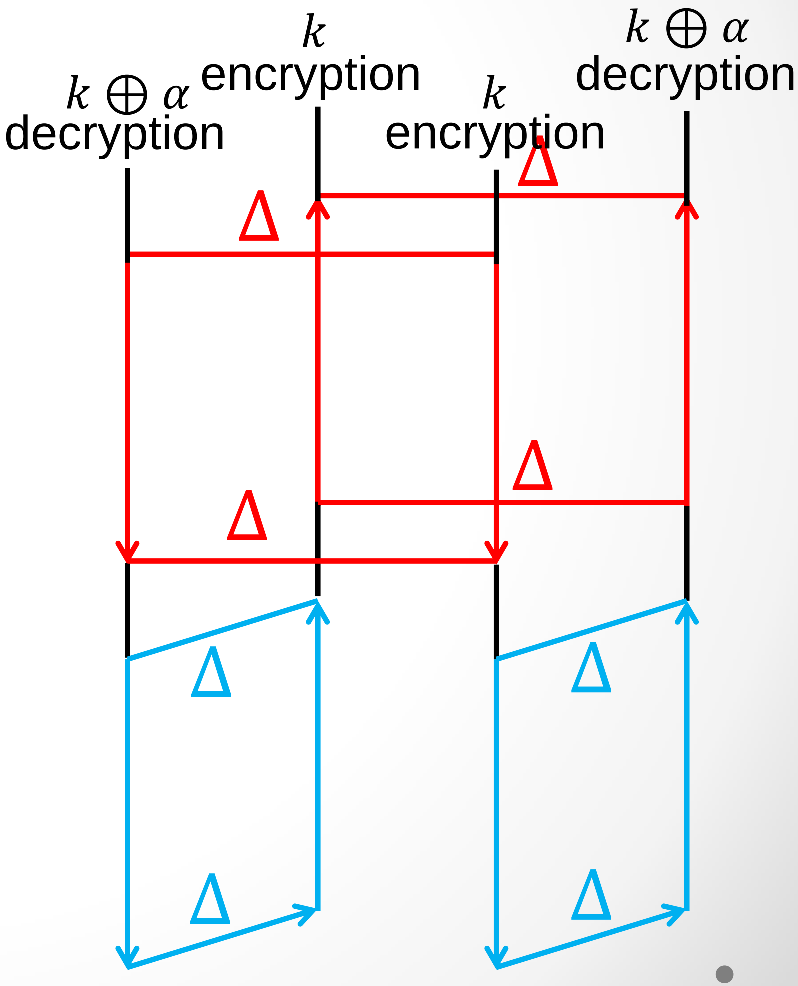
Single-key Attack on PRINCE$_{core}$ with chosen-α



Related-key boomerang attack

↓ chosen α

Single-key attack



Single-key Attack on $\text{PRINCE}_{\text{core}}$ with chosen-α

- Key differences have to be the same in the top and bottom paths
  - Amplified probability becomes 2^{-40}
- Cannot choose position of the active nibble
  - Fixed by the chosen value of α
  - Can only recover a single nibble of the key
- Need 2 boomerang quartets to determine the value of the key nibble
  - Complexity $2 \cdot 2^{40}$ to recover one nibble
- There are 240 possible choices for α
  - The α chosen by the designers is not in the 240 values

Our Results

- Related-key Attacks on Full PRINCE
- Single-key Attack on $\text{PRINCE}_{\text{core}}$ with chosen-α
- Single-key Attack on Full PRINCE with $2^{126.47-n}$
- Integral Attack on 6 rounds
- Time-Memory-Data Tradeoffs

Single-key Attack on Full PRINCE with $2^{126.4-n}$

- Linear relations with probability of 1
  - From FX construction

$$E_{k_0||k_1}(P) = E_{k_0 \oplus \Delta||k_1}(P \oplus \Delta) \oplus L(\Delta)$$

or $D_{k_0||k_1}(C) = D_{k_0 \oplus \Delta||k_1}\left(C \oplus L(\Delta)\right) \oplus \Delta$

  - From the α-reflection property

$$D_{k_0||k_1}(C) = E_{k_0||k_1 \oplus \alpha}\left(C \oplus k_0 \oplus L(k_0)\right) \oplus k_0 \oplus L(k_0)$$

Single-key Attack on Full PRINCE with $2^{126.4-n}$

- (P, C) is a known plaintext-ciphertext pair
- One offline computation to test 4 keys:
  - $E_{k_0||k_1}(P) = C'$
  - If $\delta = C' \oplus C \neq 0$, let

$$X = L^{-1}(P \oplus C \oplus k_0),\ Y = P \oplus C' \oplus L(k_0),$$

obtain the other three equations:

$$E_{k_0 \oplus L^{-1}(\delta)||k_1}\big(P \oplus L^{-1}(\delta)\big) = C$$

$$D_{X||k_1 \oplus \alpha}(C) = C' \oplus L(k_0) \oplus L^{-1}(P \oplus C \oplus k_0) = P?$$

$$E_{Y||k_1 \oplus \alpha}(P) = P \oplus k_0 \oplus L\big(P \oplus C' \oplus L(k_0)\big) = C?$$

Single-key Attack on Full PRINCE with $2^{126.4-n}$

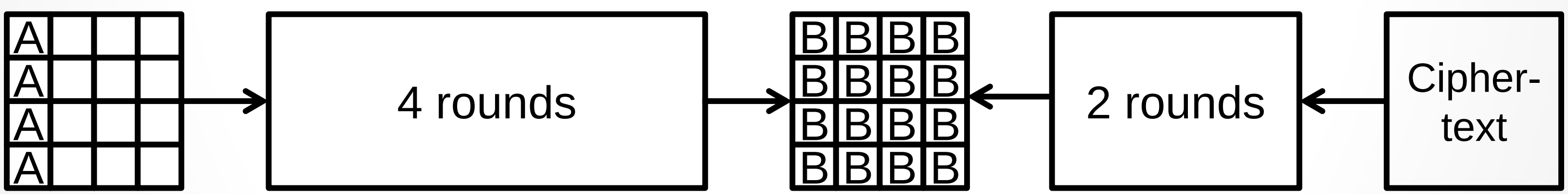
- Speeding up the key recovery
  - One query: Time complexity $2^{126.47}$, Claimed bound 2^{127}
  - Two queries: Time complexity $2^{125.47}$, Claimed bound 2^{126}
- A proven new bound
  - With 2^n data, the bound is $2^{126.47-n}$

Our Results

- Related-key Attacks on Full PRINCE
- Single-key Attack on $\text{PRINCE}_{\text{core}}$ with chosen-α
- Single-key Attack on Full PRINCE with $2^{126.47-n}$
- Integral Attack on 6 rounds
- Time-Memory-Data Tradeoffs

Integral Attack on 6 rounds

- 6-round integral attack
  - Similar technique as in original SQUARE attack
  - 4-round integral path
  - 2-round guess of key nibbles

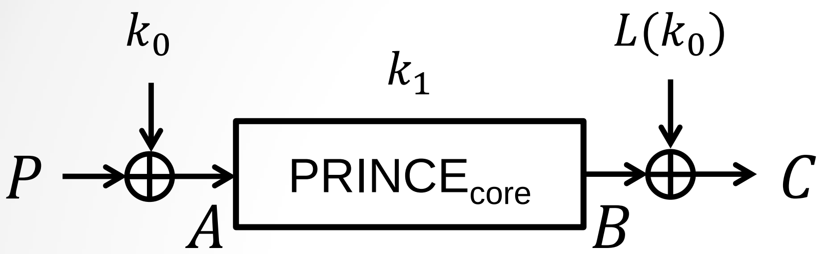


Guess part of the key

Our Results

- Related-key Attacks on Full PRINCE
- Single-key Attack on $\text{PRINCE}_{\text{core}}$ with chosen-α
- Single-key Attack on Full PRINCE with $2^{126.47-n}$
- Integral Attack on 6 rounds
- Time-Memory-Data Tradeoffs

A Memory-Data Trade-off



$$P \oplus k_0 = A \qquad\qquad L(P) \oplus L(A) = L(k_0)$$
$$B \oplus L(k_0) = C \quad \Rightarrow \quad B \oplus C = L(k_0)$$

$$\Rightarrow \quad L(P) \oplus C = L(A) \oplus B$$

online | offline

2^d known plaintext-ciphertext pairs

For 2^{64-d} values of A and 2^{64} k_1, build a table (size 2^{128-d})

$$N = 2^{128}, P = 2^{128-d}, M = 2^{128-d}, T = 2^{64}, D = 2^d$$

$$DM = N, T = N^{1/2}, M > N^{1/2}$$

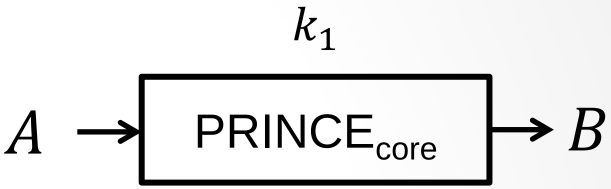
Time-Memory-Data Trade-offs

- Hellman's trade-off
  - t tables with $m \times t$ sizes

$$N = 2^n, T = t^2, M = mt$$

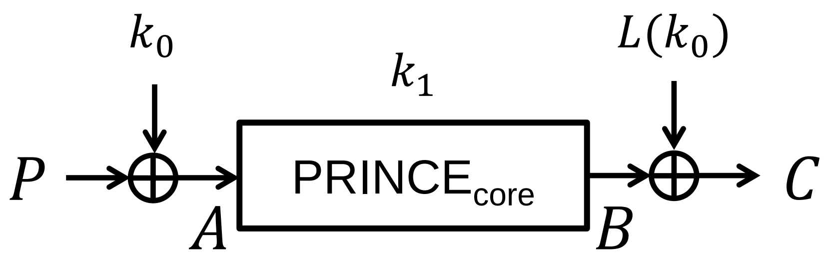
$$TM^2 = N^2$$

  - Built for given plaintext A



Time-Memory-Data Trade-offs

- Build Hellman's table for chosen values of A



$$T(MD)^2 = N^2N^{1/2}$$ *better than Hellman's TO when* $D > N^{1/4}$

- Hellman's single table trade-off

$$TMD = NN^{1/2}$$ *better than Hellman's TO when* $D > M/N^{1/2}$

Summary

Cipher	Rounds	Data	Time	Memory	Technique
PRINCE	4	2^4	2^{64}	2^4	Integral
	5	$5 \cdot 2^4$	2^{64}	2^8	Integral
	6	2^{16}	2^{64}	2^{16}	Integral
	12	2^1	$2^{125.47}$	negl.	Single-Key
	12	2^{33}	2^{64}	2^{33}	Related-Key
	12	$MD = N, T = N^{1/2}$			Memory-Data Trade-off
	12	$T(MD)^2 = N^2 N^{1/2}$			Time-Memory-Data Trade-off
	12	$TMD = NN^{1/2}$			Time-Memory-Data Trade-off
$\text{PRINCE}_{\text{core}}$	4	2^4	2^8	2^4	Integral
	5	$5 \cdot 2^4$	2^{64}	2^8	Integral
	6	2^{16}	2^{64}	2^{16}	Integral
	12	2^{39}	2^{39}	2^{39}	Related-Key Boomerang
	12	2^{41}	2^{41}	negl.	Single-Key Boomerang, Chosen α

Thank you for your attention!