Linear Cryptanalysis of PRINTcipher

Martin Ågren
Thomas Johansson

Department of Electrical and Information Technology
Lund University

Outline

Outline

1. **Introduction**
   - Contribution
   - PRINTCIPHER
   - Linear Cryptanalysis
2. **Linear Cryptanalysis of PRINTcipher**
3. **Guessing Bits for Encryption and Decryption**
4. **How to Find Many Samples**
5. **Conclusion**

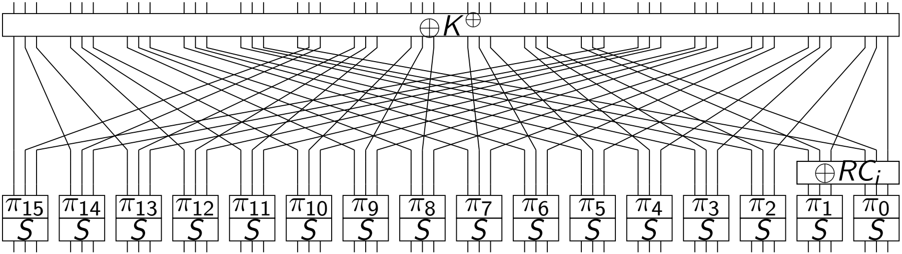
Contribution

Since PRINTcipher is made for burnt-in keys, it is "easy" to avoid weak keys, if there are any.

Previous work relates around weak keys:

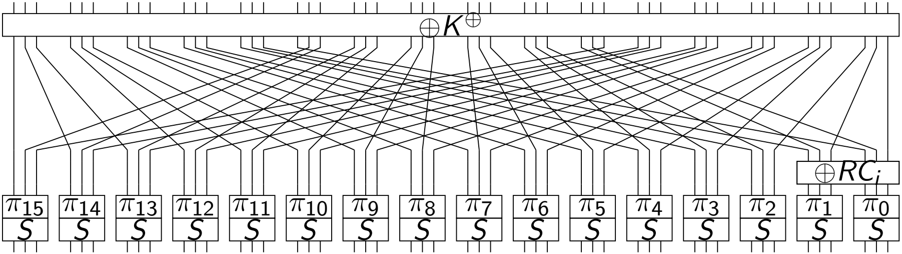
- Leander et al. at Crypto on > 0 rounds.
  Remaining keys: $2^{80} - 2^{52} \approx 2^{80}$.
- Karakoç et al. at SAC on 31 rounds.
  Remaining keys: $\approx 2^{79.8}$.
- This work on 29 rounds.
  Remaining keys: $\approx 2^{78}$.

PRINTcipher

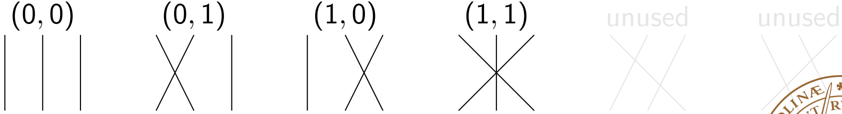


- 48-bit plaintext, ciphertext and state, 48 rounds.
- Same XOR key $K^{\oplus} = (k^{\oplus}_{47}, \ldots, k^{\oplus}_{0})$ in all rounds.
- Same permutation key $K^{\pi} = (k^{\pi}_{31}, \ldots, k^{\pi}_{0})$ in all rounds.

PRINTcipher



- We label bit positions using (b, c), $0 \le b < 16$, $0 \le c < 3$.
- $(k^{\pi}_{2b+1}, k^{\pi}_{2b})$ determines how permutation π_b acts on the bits at positions $(b, 2), (b, 1), (b, 0)$.



PRINTcipher

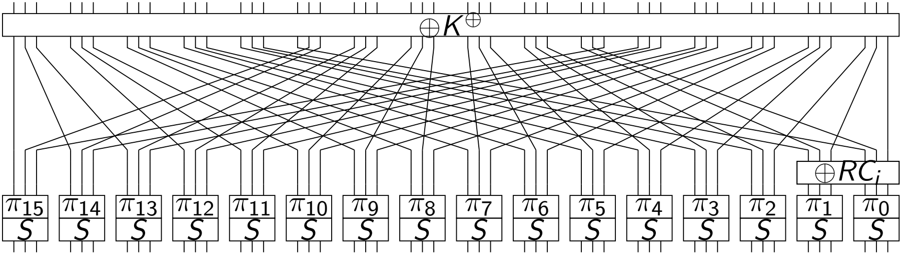


Table: $S(x_2, x_1, x_0) = (y_2, y_1, y_0)$.

x	000	001	010	011	100	101	110	111
$S(\mathbf{x})$	000	001	011	110	111	100	101	010

Linear Cryptanalysis

- We only use optimal characteristics.
- One-round characteristic holds with probability $\frac{1}{2} + 2^{-2}$.
- r-round characteristic holds with probability $\frac{1}{2} + 2^{-r-1}$.
- We call $\epsilon = \text{Prob}(\cdot) - \frac{1}{2} = 2^{-r-1}$ the *bias*.

Linear Cryptanalysis

- $\text{Prob}(\boldsymbol{\beta} \cdot C = \boldsymbol{\alpha} \cdot P) = \frac{1}{2} \pm 2^{-r-1}$.

Linear Cryptanalysis

- $\text{Prob}(\boldsymbol{\beta} \cdot C = \boldsymbol{\alpha} \cdot P) = \frac{1}{2} \pm 2^{-r-1}$.
- $\text{Prob}(c_{47} = p_{47}) = \frac{1}{2} + 2^{-r-1}$.

Finding Many Samples is Important

- To use a property with bias ϵ, we need ϵ^{-2} samples.
- $\epsilon = 2^{-r-1} \Rightarrow 2^{2r+2}$ samples.

Finding Many Samples is Important

- To use a property with bias ϵ, we need ϵ^{-2} samples.
- $\epsilon = 2^{-r-1} \Rightarrow 2^{2r+2}$ samples.
- One sample is most often one plaintext–ciphertext pair.
- 2^{48} plaintext–ciphertext pairs $\Rightarrow$ 23 rounds.
- 24 rounds $\Leftarrow 2^{50}$ samples "$\Leftrightarrow$" 2^2 samples per plaintext–ciphertext pair.

Outline

PRINTcipher Revisited

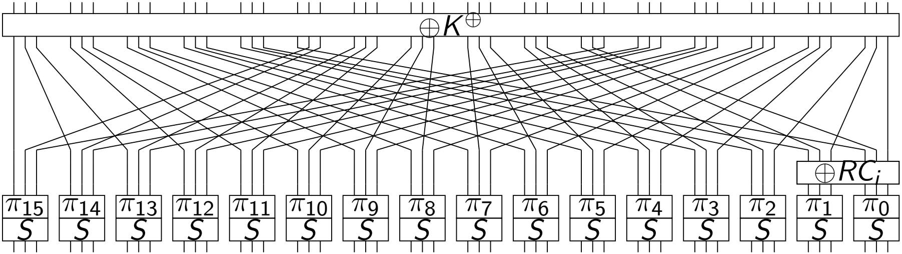


Table: $S(x_2, x_1, x_0) = (y_2, y_1, y_0)$.

x	000	001	010	011	100	101	110	111
$S(\mathbf{x})$	000	001	011	110	111	100	101	010

$\text{Prob}(y_2 = x_2) = \ldots$

PRINTCIPHER Revisited

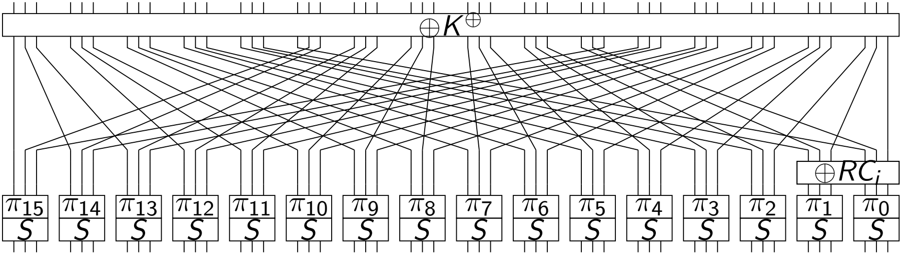


Table: $S(x_2, x_1, x_0) = (y_2, y_1, y_0)$.

x	000	001	010	011	100	101	110	111
$S(\mathbf{x})$	000	001	011	110	111	100	101	010

$$\text{Prob}(y_2 = x_2) = \frac{6}{8} = \frac{1}{2} + 2^{-2}$$

PRINTCIPHER Revisited

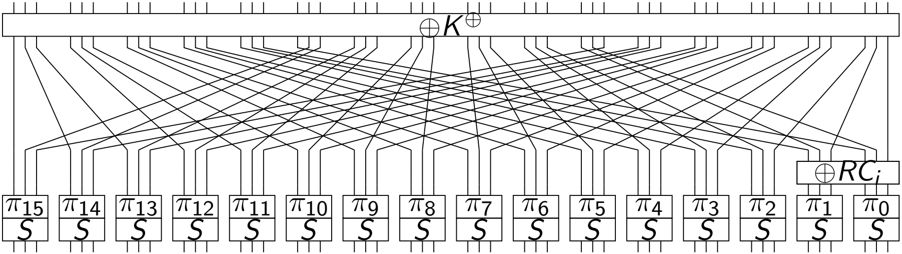


Table: $S(x_2, x_1, x_0) = (y_2, y_1, y_0)$.

x	000	001	010	011	100	101	110	111
$S(\mathbf{x})$	000	001	011	110	111	100	101	010

$$\text{Prob}(y_2 = x_2) = \frac{6}{8} = \frac{1}{2} + 2^{-2}$$
$$\text{Prob}(y_1 = x_1) = \frac{1}{2} + 2^{-2}$$

PRINTcipher Revisited

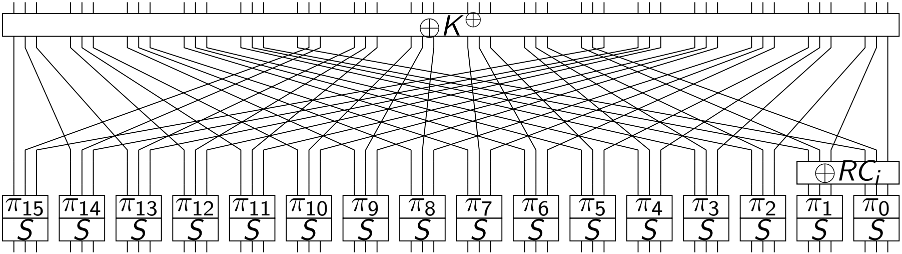
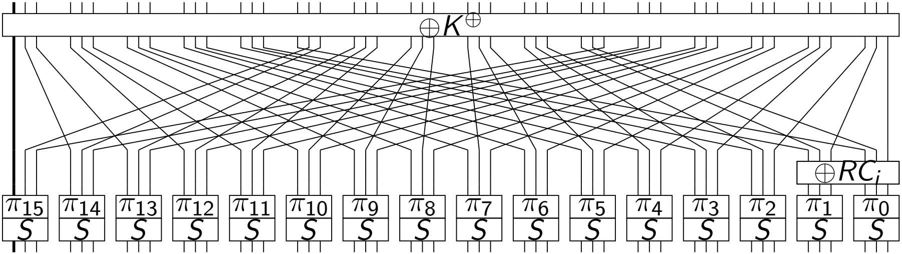


Table: $S(x_2, x_1, x_0) = (y_2, y_1, y_0)$.

x	000	001	010	011	100	101	110	111
$S(\mathbf{x})$	000	001	011	110	111	100	101	010

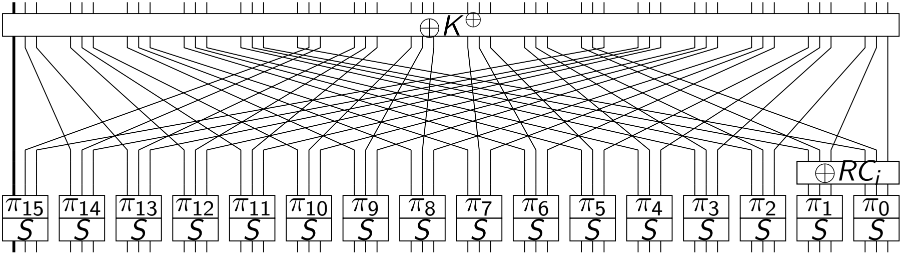
$$\text{Prob}(y_2 = x_2) = \frac{6}{8} = \frac{1}{2} + 2^{-2}$$
$$\text{Prob}(y_1 = x_1) = \frac{1}{2} + 2^{-2}$$
$$\text{Prob}(y_0 = x_0 \oplus 1) = \frac{1}{2} + 2^{-2}$$

A First Linear Characteristic



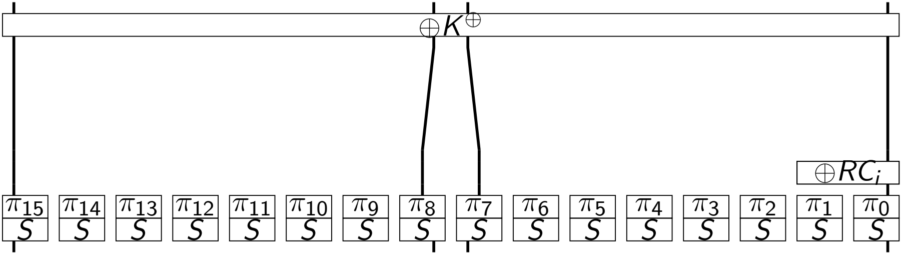
- $(15, 2)$ is permuted to $(15, 2)$ for half of the keys.
- Remember: $\text{Prob}(y_2 = x_2) = \frac{1}{2} + 2^{-2}$.

A First Linear Characteristic



- $(15, 2)$ is permuted to $(15, 2)$ for half of the keys.
- Remember: $\text{Prob}(y_2 = x_2) = \frac{1}{2} + 2^{-2}$.
- $\text{Prob}(c_{47} = p_{47} \oplus k^{\oplus}_{47}) = \frac{1}{2} + 2^{-2}$.
- More rounds: $\text{Prob}(c_{47} = p_{47} \oplus k^{\oplus}_{47} \cdot (r \bmod 2)) = \frac{1}{2} + 2^{-r-1}$.

All Single-Round Characteristics



- There are four different iterated single-round trails
- We can extend them to r rounds.
- Same bits of K^{π} — key classes do not shrink.

Outline

General Attack Idea

We want to use

$$\text{Prob}(c_{47} = p_{47} \oplus k_{47}^{\oplus}) = \frac{1}{2} + 2^{-24}$$

on 23 rounds, but attack more rounds.

General Attack Idea

We want to use

$$\text{Prob}(c_{47} = p_{47} \oplus k_{47}^{\oplus}) = \frac{1}{2} + 2^{-24}$$

on 23 rounds, but attack more rounds.

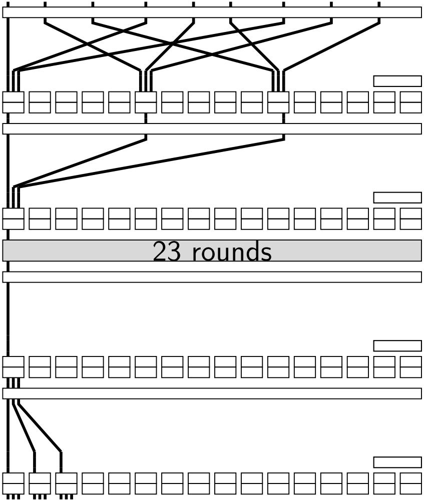
- Add some rounds of partial encryption/decryption.
- We need to guess the bits involved in these calculations.
- Good guess $\Rightarrow$ true "inner bits" $\Rightarrow$ we should observe a bias
- Bad guess $\Rightarrow$ we should not observe bias?!?

General Attack Formulation

$$\text{Prob}(c_{47}^{2} = c_{47}^{25} \oplus k_{47}^{\oplus}) = \frac{1}{2} + 2^{-24}$$

- Use several counters, initialized at zero.
- For each plaintext–ciphertext pair...
  - For each partial guess...
    - Do partial encryption/decryption.
    - If $c_{47}^{2} = c_{47}^{25} \oplus k_{47}^{\oplus}$, increase the counter for this guess.
- Now, the correct guess should have a high counter value.

27 Rounds



Improved General Attack Formulation

- For each plaintext–ciphertext pair...
  - categorize it according to the *active* bits

Improved General Attack Formulation

- For each plaintext–ciphertext pair...
  - categorize it according to the *active* bits
- For each "plaintext prototype"...
  - For each relevant partial guess...
    - Do partial encryption to access the inner bit c_{47}^2.

Improved General Attack Formulation

- For each plaintext–ciphertext pair...
  - categorize it according to the *active* bits
- For each "plaintext prototype"...
  - For each relevant partial guess...
    - Do partial encryption to access the inner bit c_{47}^{2}.
- For each "ciphertext prototype"...
  - For each relevant partial guess...
    - Do partial decryption to access the inner bit c_{47}^{25}.

Improved General Attack Formulation

- For each plaintext–ciphertext pair. . .
  - categorize it according to the *active* bits

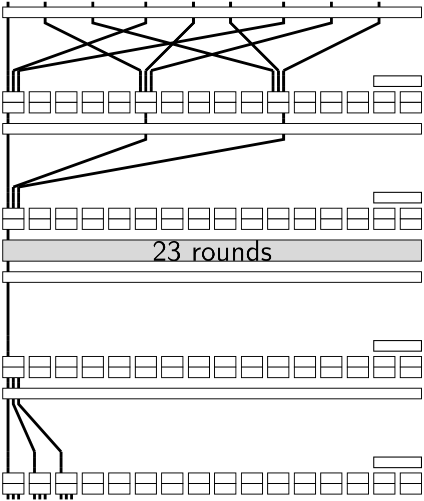
- For each "plaintext prototype". . .
  - For each relevant partial guess. . .
    - Do partial encryption to access the inner bit c_{47}^{2}.

- For each "ciphertext prototype". . .
  - For each relevant partial guess. . .
    - Do partial decryption to access the inner bit c_{47}^{25}.

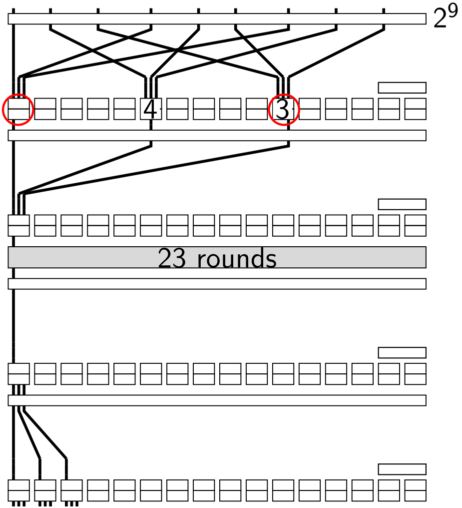
- For each partial guess. . .
  - For each "plaintext–ciphertext prototype". . .
    - If $c_{47}^{2} = c_{47}^{25} \oplus k_{47}^{\oplus}$, increase the counter for this guess.
    - The increase depends on how many such pairs we saw.

- Now, the correct guess should have a high counter value.

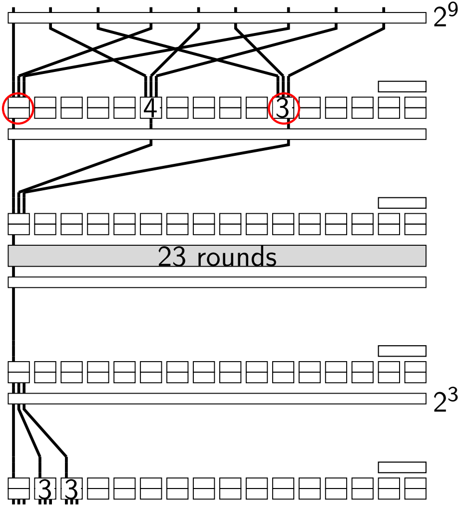
27 Rounds



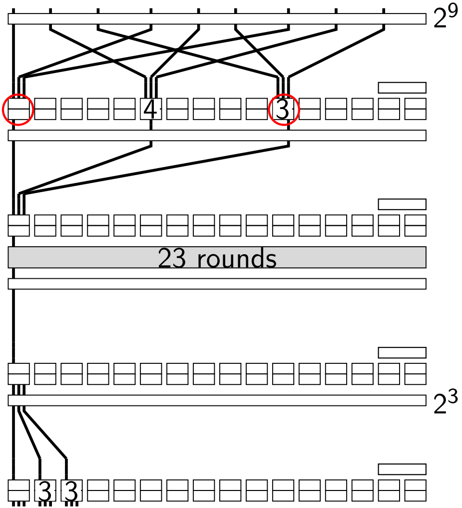
27 Rounds



27 Rounds



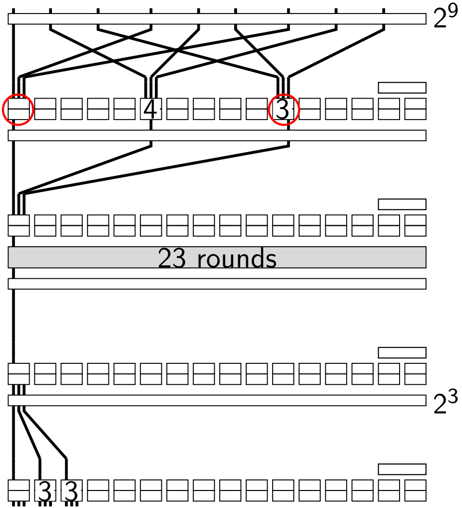
27 Rounds



Total guesswork:
$N = 2^{13} \cdot 3^3 \approx 2^{17.75}$

Encryption: $2^{11} \cdot 3 \approx 2^{12.6}$
Decryption: $2^3 \cdot 3^2 \approx 2^{6.2}$

27 Rounds

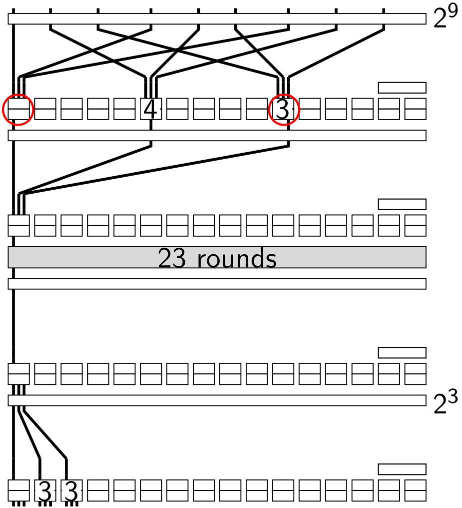


Total guesswork:
$N = 2^{13} \cdot 3^3 \approx 2^{17.75}$

Encryption: $2^{11} \cdot 3 \approx 2^{12.6}$
Decryption: $2^3 \cdot 3^2 \approx 2^{6.2}$

Total calculations:
$2^9 \cdot 2^{11} \cdot 3 + 2^9 \cdot 2^3 \cdot 3^2 \approx 2^{21.6}$

27 Rounds

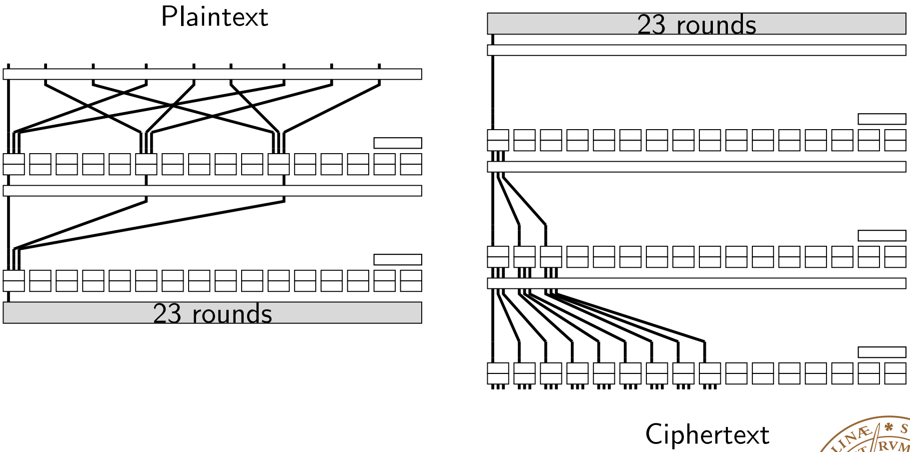


Categorizing the data:
2^{48}

Preparing the counters:
2^{22}

Combining the counters:
$2^{9+9} \cdot N \approx 2^{36}$

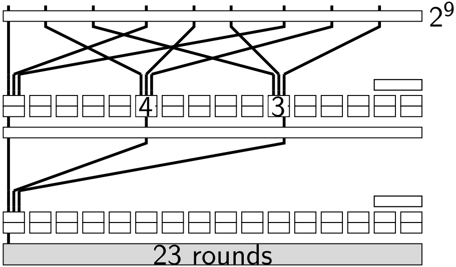
28 Rounds

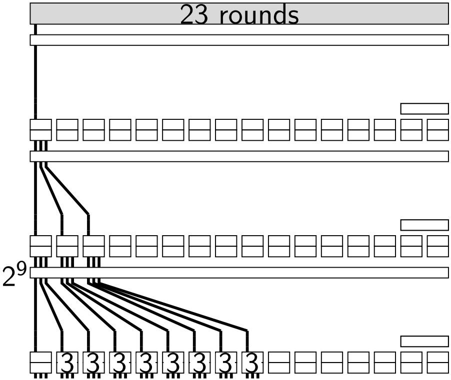


M. Ågren, T. Johansson, Dept. of Electrical and Information Technology, Lund University, Sweden

28 Rounds

Plaintext





Ciphertext

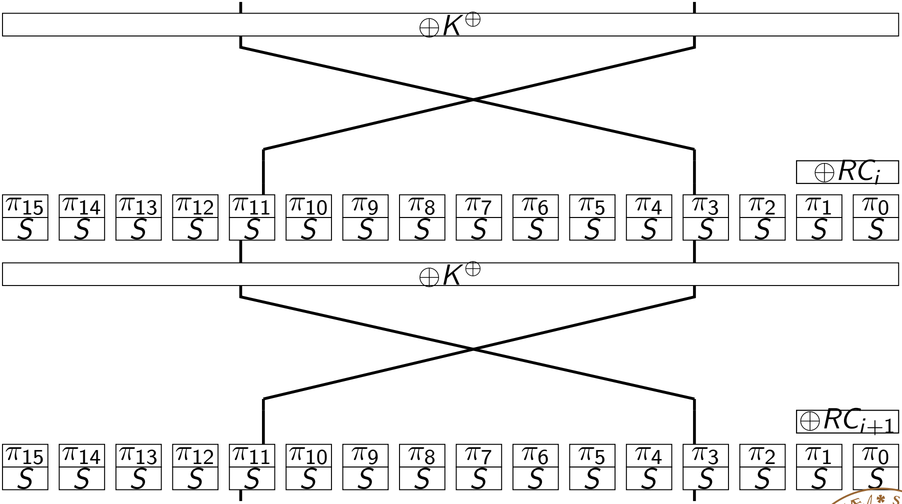
$N = 2^{18} \cdot 3^{8} \approx 2^{30.7}$

Preparing the counters: $\approx 2^{51}$

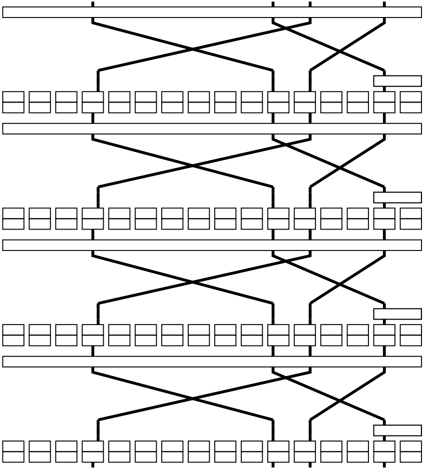
Combining the counters: $\approx 2^{67}$

Outline

Two Rounds of PRINTcipher



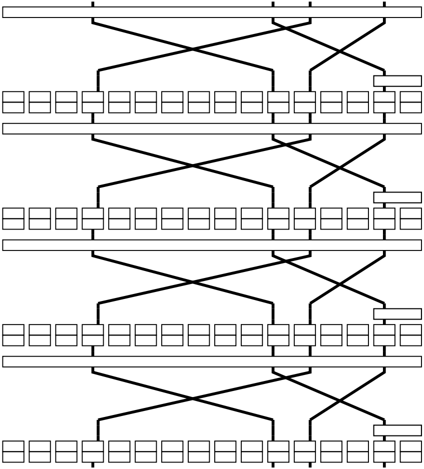
Four Rounds of PRINTcipher



$(k^\pi_{25}, k^\pi_{24}, k^\pi_{10}, k^\pi_{9}, k^\pi_{3}) = (1, 0, 0, 0, k^\pi_{2})$

$\text{Prob}(c_4 = p_4) = \frac{1}{2} + 2^{-r-1}$

Four Rounds of PRINTcipher

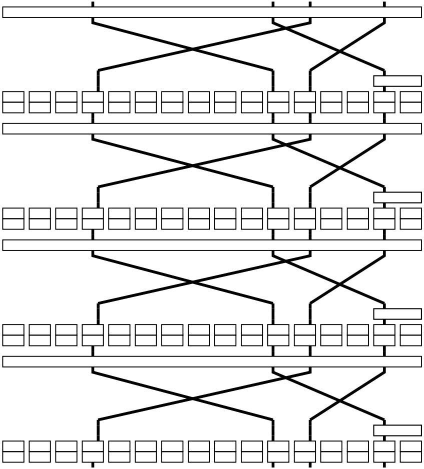


$(k_{25}^{\pi}, k_{24}^{\pi}, k_{10}^{\pi}, k_{9}^{\pi}, k_{3}^{\pi}) = (1, 0, 0, 0, k_{2}^{\pi})$

$\text{Prob}(c_4 = p_4) = \frac{1}{2} + 2^{-r-1}$

$\text{Prob}(c_{12} = p_{12}) = \frac{1}{2} + 2^{-r-1}$

Four Rounds of PRINTcipher



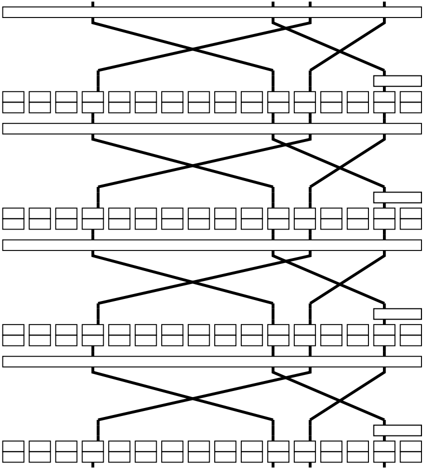
$(k^{\pi}_{25}, k^{\pi}_{24}, k^{\pi}_{10}, k^{\pi}_{9}, k^{\pi}_{3}) = (1, 0, 0, 0, k^{\pi}_{2})$

$\text{Prob}(c_4 = p_4) = \frac{1}{2} + 2^{-r-1}$

$\text{Prob}(c_{12} = p_{12}) = \frac{1}{2} + 2^{-r-1}$

$\text{Prob}(c_{17} = p_{17}) = \frac{1}{2} + 2^{-r-1}$

Four Rounds of PRINTcipher



$(k^{\pi}_{25}, k^{\pi}_{24}, k^{\pi}_{10}, k^{\pi}_{9}, k^{\pi}_{3}) = (1, 0, 0, 0, k^{\pi}_{2})$

$\text{Prob}(c_4 = p_4) = \frac{1}{2} + 2^{-r-1}$

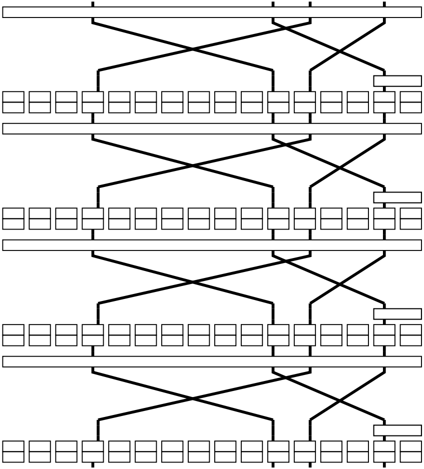
$\text{Prob}(c_{12} = p_{12}) = \frac{1}{2} + 2^{-r-1}$

$\text{Prob}(c_{17} = p_{17}) = \frac{1}{2} + 2^{-r-1}$

$\text{Prob}(c_{37} = p_{37}) = \frac{1}{2} + 2^{-r-1}$

Four samples for the same basic property!

Four Rounds of PRINTcipher



$(k^{\pi}_{25}, k^{\pi}_{24}, k^{\pi}_{10}, k^{\pi}_{9}, k^{\pi}_{3}) = (1, 0, 0, 0, k^{\pi}_{2})$

$\text{Prob}(c_4 = p_4) = \frac{1}{2} + 2^{-r-1}$

$\text{Prob}(c_{12} = p_{12}) = \frac{1}{2} + 2^{-r-1}$

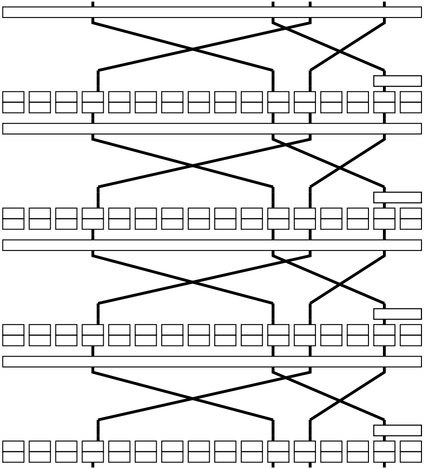
$\text{Prob}(c_{17} = p_{17}) = \frac{1}{2} + 2^{-r-1}$

$\text{Prob}(c_{37} = p_{37}) = \frac{1}{2} + 2^{-r-1}$

I have cheated: round constants and bits of $K^{\oplus}$.

Four samples for the same basic property!

Four Rounds of PRINTcipher

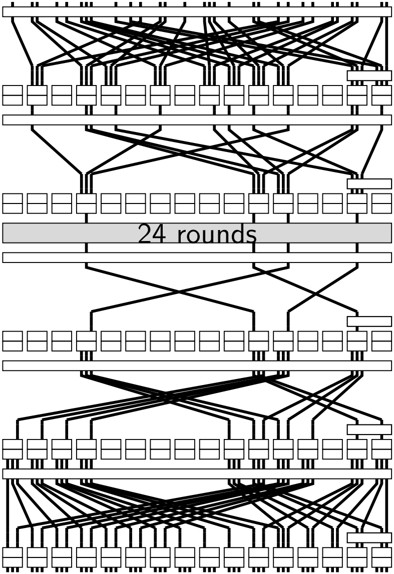


We can control the round constants.
Pile to eight rounds
$\Rightarrow$ bits of $K^{\oplus}$ cancel.

We have created eight-round trails with bias 2^{-r-1} that allow four samples per plaintext–ciphertext pair.
$\Rightarrow$
We can construct a 24-round characteristic that we can actually distinguish!

Four samples for the same basic property!

29 Rounds



$N = 2^{63} \cdot 3^3 \approx 2^{67}$

Preparing the counters:
$\approx 2^{55}$

Combining the counters:
$\approx 2^{76}$

Finalizing the counters:
$N \approx 2^{67}$

Brute force: 2^{75}!?!

Outline

Conclusion

- There are several large class of weak keys.
- We can find several samples per plaintext–ciphertext pair.
- We reach 29 rounds.

Open problems

- Reach more rounds (e.g., all 48).
- Use large key classes (e.g. $2^8$0 or at least $> 2^{51}$).
- We probably need to do something quite different.

Conclusion

Thank you!