Differential-Linear Cryptanalysis on Xoodyak

Orr Dunkelman[1] Ariel Weizman[2]

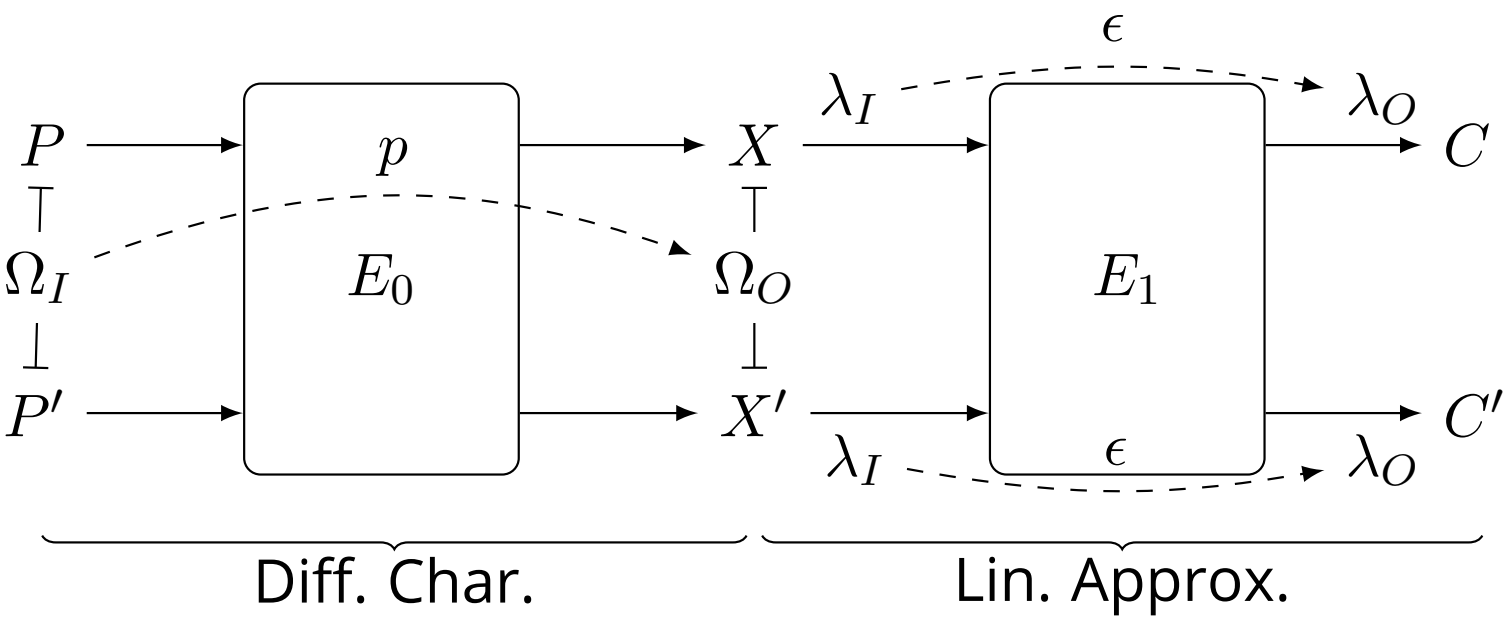
Lightweight Cryptography Workshop 2022

Differential-Linear (DL) Cryptanalysis [HL94]

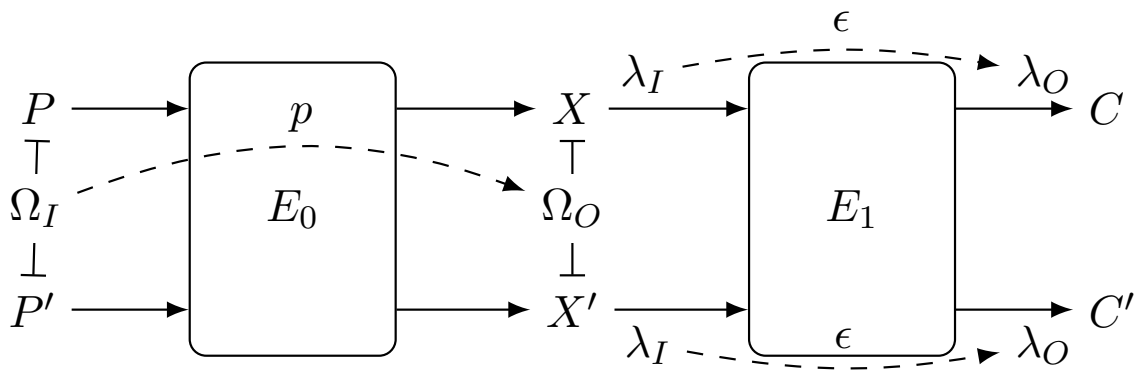
- Combining a differential characteristic for E_0 and a linear approximation for E_1 into an attack on the entire cipher $E = E_1 \circ E_0$.

Differential-Linear (DL) Cryptanalysis [HL94]

- Combining a differential characteristic for E_0 and a linear approximation for E_1 into an attack on the entire cipher $E = E_1 \circ E_0$.



Differential-Linear (DL) Cryptanalysis [HL94]



$$\mathbf{Pr}\left[C \cdot \lambda_O = C' \cdot \lambda_O | P \oplus P' = \Omega_I\right] = \frac{1}{2} + 2p\epsilon^2$$

DL with Partitioning [L16]

- Partitioning the data into s disjoint subsets

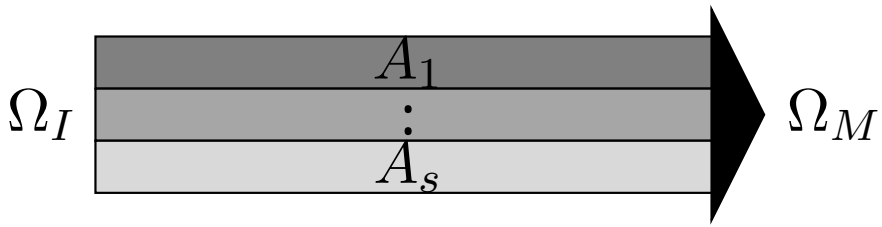
  $\mathcal{F} = \{A_1, A_2, \ldots, A_s\}$.

DL with Partitioning [L16]

- Partitioning the data into s disjoint subsets $\mathcal{F} = \{A_1, A_2, \ldots, A_s\}$.
- One right subset A_i satisfies the differential characteristic with significantly higher probability $p_i \gg p$, while $\forall j \neq i : p_j \approx 0$.

DL with Partitioning [L16]

- Partitioning the data into s disjoint subsets $\mathcal{F} = \{A_1, A_2, \ldots, A_s\}$.
- One right subset A_i satisfies the differential characteristic with significantly higher probability $p_i \gg p$, while $\forall j \neq i : p_j \approx 0$.



Neutral Bits [B+20]

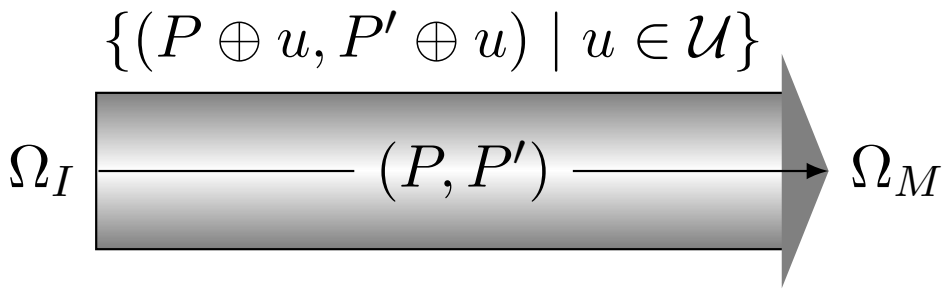
- Looking for a subspace $\mathcal{U} \subseteq \mathbb{F}_2^n$, s.t. given a right pair (P, P') (w.r.t. the differential part), then $\forall u \in \mathcal{U} : (P \oplus u, P' \oplus u)$ also right pairs.

Neutral Bits [B+20]

- Looking for a subspace $\mathcal{U} \subseteq \mathbb{F}_2^n$, s.t. given a right pair (P, P') (w.r.t. the differential part), then $\forall u \in \mathcal{U} : (P \oplus u, P' \oplus u)$ also right pairs.
- One right pair produces a (possibly large) set of right pairs, which have the same parity in the beginning of the linear part.

Neutral Bits [B+20]

- Looking for a subspace $\mathcal{U} \subseteq \mathbb{F}_2^n$, s.t. given a right pair (P, P') (w.r.t. the differential part), then $\forall u \in \mathcal{U} : (P \oplus u, P' \oplus u)$ also right pairs.
- One right pair produces a (possibly large) set of right pairs, which have the same parity in the beginning of the linear part.



Our Results

DL Cryptanalysis on Xoodyak[D+19]:

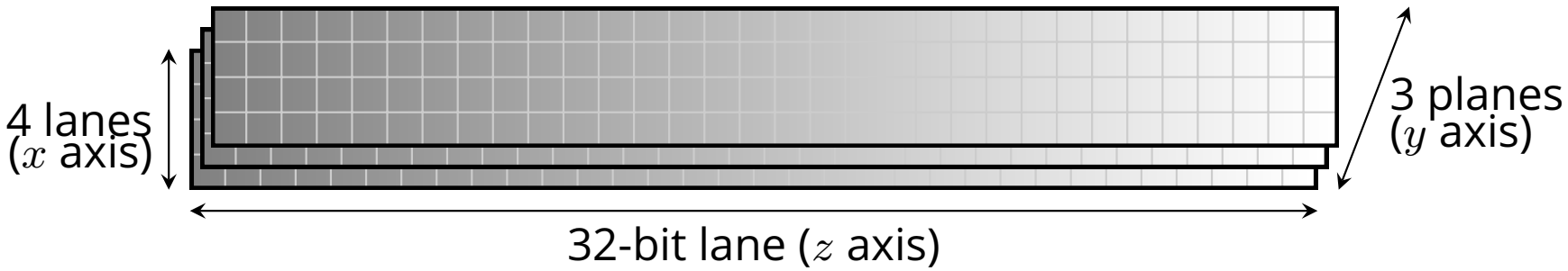
A permutation-based algorithm, relies on Xoodoo[D+18].

Our Results

1. 4-round DL attack, with $2^{23.34}$ data and times complexity.
2. 5-round related-key DL attack, with $2^{22.04}$ data and time complexity.

A Brief Description of Xoodoo

- Xoodoo: a 384-bit to 384- bit permutation.
- A 384-bit state is represented by three *planes*, each consists of four 32-bit *lanes*.
- The lanes within a plane are indexed by x, the planes are indexed by y, and the bits within a lane are indexed by z



The 5 Steps of each Xoodoo Round

(1) θ :

$P \leftarrow A_0 \oplus A_1 \oplus A_2$

$E \leftarrow P \lll (1,5) \oplus P \lll (1,14)$

$A_y \leftarrow A_y \oplus E, y \in \{0,1,2\}$

(2) ρ_{west} :

$A_1 \leftarrow A_1 \lll (1,0)$

$A_2 \leftarrow A_2 \lll (0,11)$

(3) ι :

$A_0 \leftarrow A_0 \oplus C_i$

(4) χ : (The S-box layer)

$B_0 \leftarrow \overline{A_1} \wedge A_2$

$B_1 \leftarrow \overline{A_2} \wedge A_0$

$B_2 \leftarrow \overline{A_0} \wedge A_1$

$A_y \leftarrow A_y \oplus B_y, y \in \{0,1,2\}$

(5) ρ_{east} :

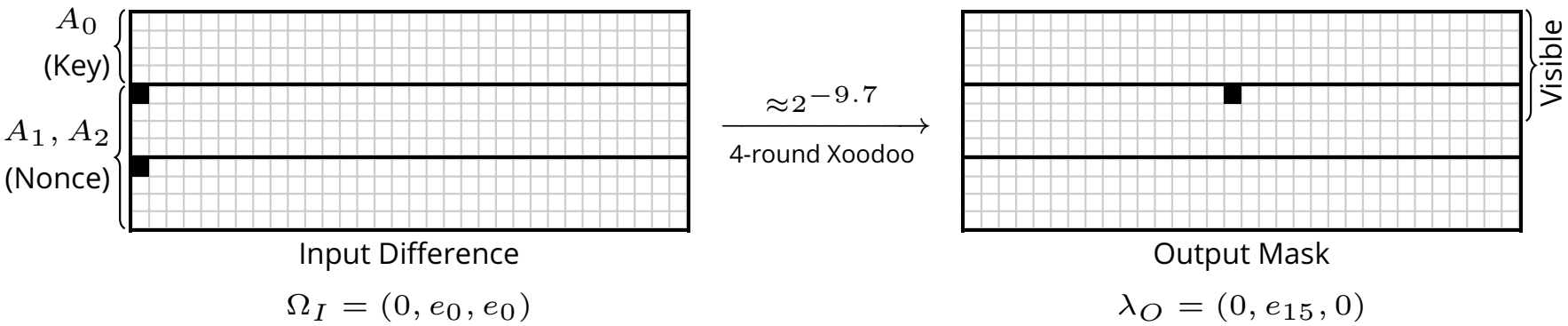
$A_1 \leftarrow A_1 \lll (0,1)$

$A_2 \leftarrow A_2 \lll (2,8)$

The Initialization Phase

1. The first plane is initialized by an 128-bit key, and the additional two planes by a 256-bit nonce.
2. Xoodoo is performed on the initialized state.
3. The first 192 bits are visible and XORed to the first block of the plaintext.

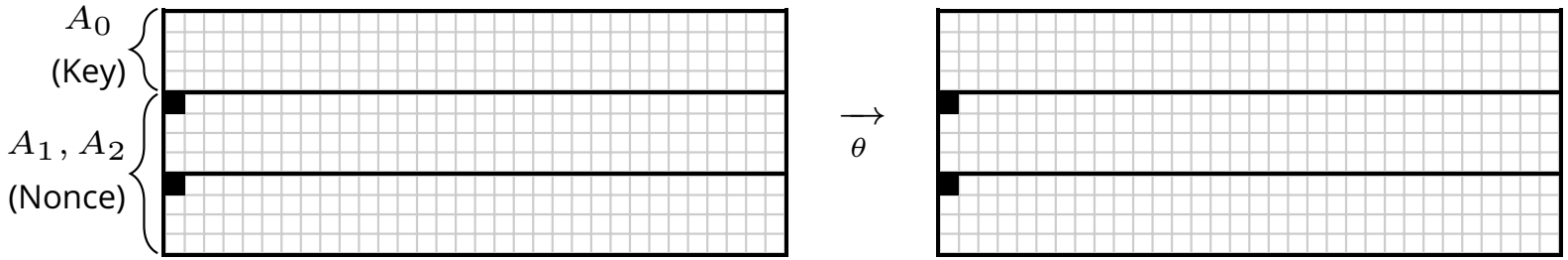
An Overview on the 4-round DL Characteristic



Note: Xoodoo's characteristics are rotation-invariant!

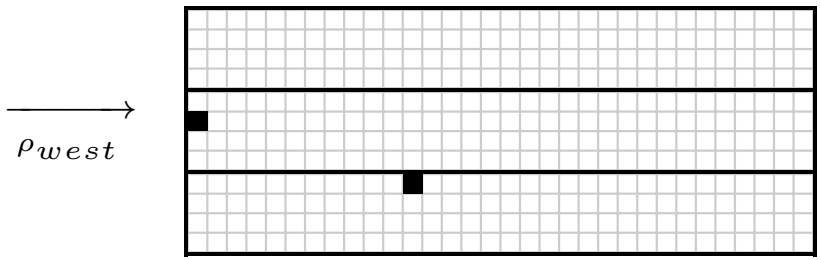
Behind the Choice of the Input Difference

Two active bits in the beginning lead to two active S-boxes.



Input Difference

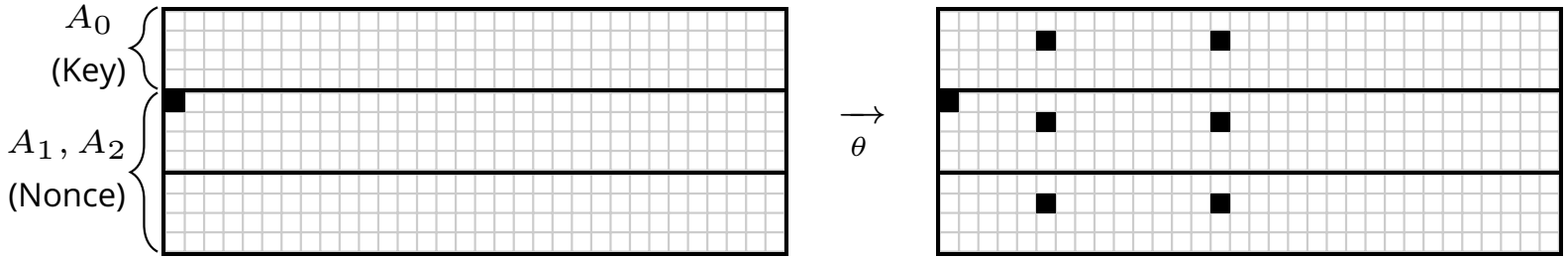
$\Omega_I = (0, e_0, e_0)$



Only 2 Active S-boxes

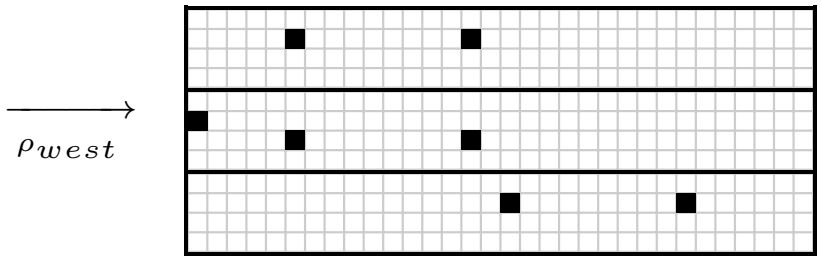
Behind the Choice of the Input Difference

One active bit in the beginning leads to seven active S-boxes.



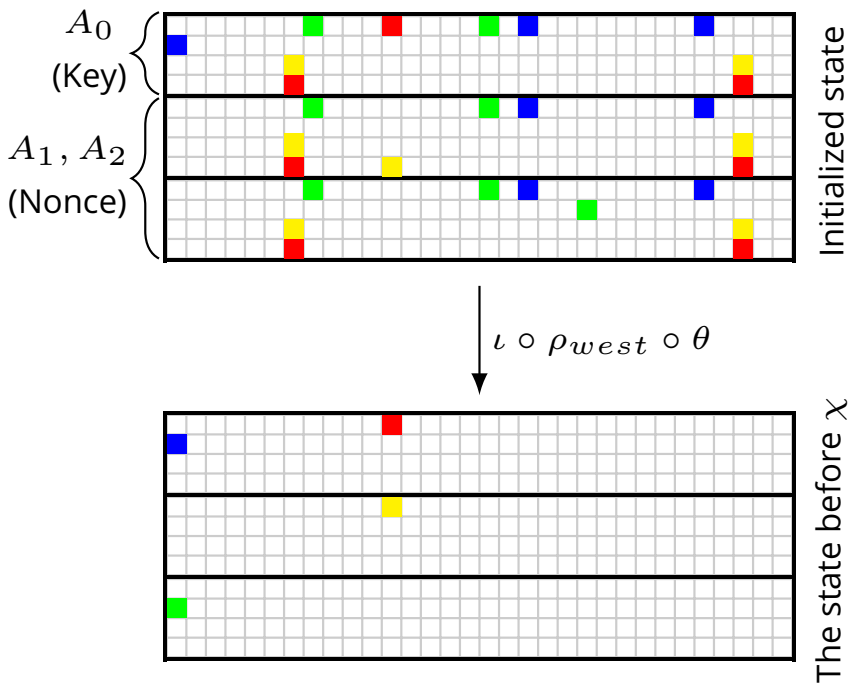
Input Difference

$\Omega_I = (0, e_0, 0)$



7 Active S-boxes

Using Neutral Bits



Using the Partitioning Technique

- The best input values to S-box 11 are 2 and 6. Thus:
  - The XOR of the red bits should be 0.
  - The XOR of the yellow bits should be 1.
- The best input values to S-box 32 are 1 and 3. Thus:
  - The XOR of the blue bits should be 1.
  - The XOR of the green bits should be 0.

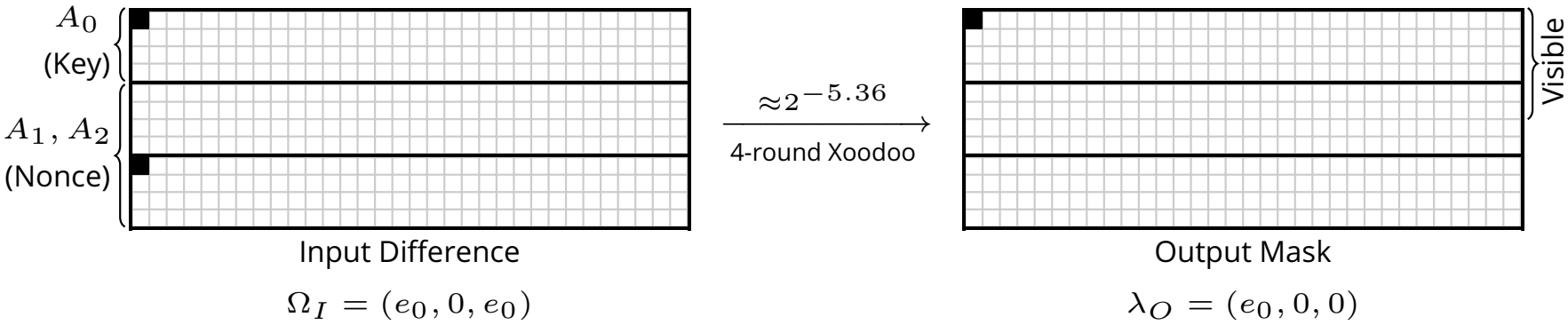
Using the Partitioning Technique

$$
\begin{aligned}
K_{11} \oplus K_{102} \oplus K_{125} &= N_{230} \oplus N_{253} \oplus N_{358} \oplus N_{381}, \\
K_{70} \oplus K_{93} &= N_{198} \oplus N_{221} \oplus N_{235} \oplus N_{326} \oplus N_{349} \oplus 1, \\
K_{18} \oplus K_{27} \oplus K_{32} &= N_{146} \oplus N_{155} \oplus N_{274} \oplus N_{283} \oplus 1, \\
K_{7} \oplus K_{16} &= N_{135} \oplus N_{144} \oplus N_{263} \oplus N_{272} \oplus N_{309},
\end{aligned}
$$

(Where the key bits are indexed by $0 \leq i < 128$ and the nonce bits are indexed by $128 \leq i < 383$.)

Adjustments for Attacking 5-Round Xoodyak

1. Use another input difference (and thus also another output mask).
   1. A better bias of $2^{-5.36}$ instead of $2^{-9.7}$.
   2. Since there is an active key bit, we need related keys.



Adjustments for Attacking 5-Round Xoodyak

2. Add one round preceding:

$$(\Omega A_0, \Omega A_1, \Omega A_2) \xrightarrow[\text{1-round Xoodoo}]{p=2^{-4}} (e_0, 0, e_0),$$

where:

$$\begin{aligned} \Omega A_0 &= a8b23b19\ 98810919\ 52674513\ 95a876f3_x \\ \Omega A_1 &= a8b23b18\ 98810919\ 52674513\ 95a876f3_x \\ \Omega A_2 &= a8b23b18\ 98810919\ 52676513\ 95a876f3_x. \end{aligned}$$

Adjustments for Attacking 5-Round Xoodyak

3. The entire DL characteristic is:

$$(\Omega A_0, \Omega A_1, \Omega A_2) \xrightarrow[\text{5-round Xoodoo}]{p \approx 2^{-9.36}} (e_0, 0, 0),$$

4. Use neutral bits and the partitioning technique as before.

Summary

The first DL cryptanalysis on Xoodyak:

1. 4-round DL attack: revealing the entire key with complexity of $2^{23.34}$.
2. 5-round RK DL attack: revealing the entire key with complexity of $2^{22.04}$.

Thank you for your attention!

Questions?