Algebraic Attacks on Rasta and Dasta Using Low-degree Equations

Fukang Liu[1], Santanu Sarkar[4,5], Willi Meier[6], Takanori Isobe[1,2,3]

[1]University of Hyogo, Japan
[2]NICT, Japan,
[3]PRESTO, Japan
[4]Indian Institute of Technology Madras, India
[5]Ruhr-University Bochum, Germany
[6]FHNW, Switzerland

liufukangs@gmail.com

November 24, 2021

The Rasta Primitive

- Rasta was proposed at CRYPTO 2018.
- An FHE-friendly primitive (low AND-depth & #AND gates).
- The affine layers (linear layers & round constants) vary for each to-be-encrypted plaintext block, i.e. each keystream is generated with a different concrete Rasta instance.

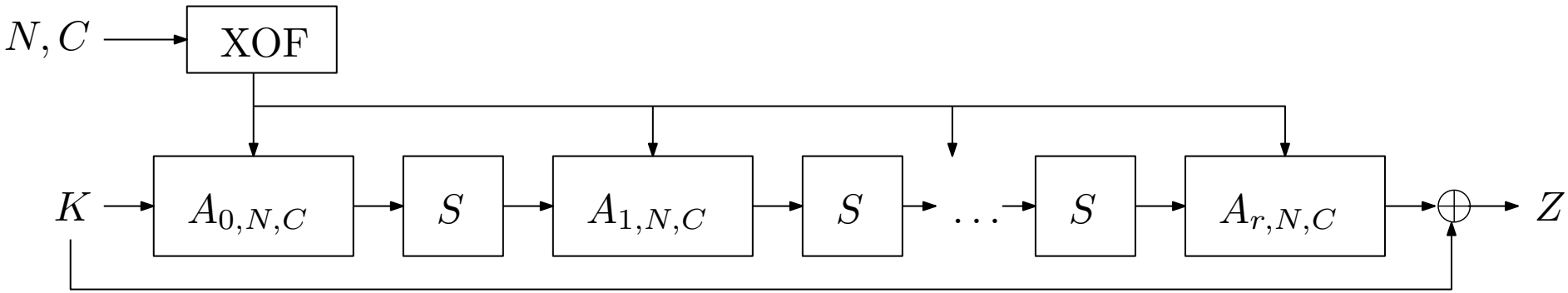


Figure: Illustration of r rounds of Rasta

The Rasta Round Function: Affine/Nonlinear Layers

- Generate the affine layer $u = A_{i,N,C}(v)$:

$$u \quad = \quad M_{i,N,C} \cdot v \oplus RC_{i,N,C}.$$

  - Use the plaintext block counter C and the nonce N as the input to an XOF (e.g. SHAKE-256).
  - Use the output of the XOF to construct a random full-rank linear transform matrix $M_{i,N,C}$ of size $n \times n$ and a random n-bit round constant $RC_{i,N,C}$ for each round.
- The fixed nonlinear layer $y = S(x)$, i.e. the n-bit χ operation:

$$y_i \quad = \quad x_i \oplus \overline{x_{i+1}} x_{i+2},$$

where $x = (x_0, x_1, \ldots, x_{n-1}) \in \mathbb{F}_2^n$ and $y = (y_0, y_1, \ldots, y_{n-1}) \in \mathbb{F}_2^n$.

$\star$ The 5-bit χ operation is used in the Keccak round function.

The Recommended Parameters for Rasta

Table: Parameters of Rasta

κ	n	r
80	327	4
	327	5
	219	6
128	1877	4
	525	5
	351	6
256	445939	4
	3545	5
	703	6

- The data limit for each n-bit key K: $\sqrt{2^{\kappa}}/n$

The Aggressive version of Rasta: Agrasta

Table: Parameters of Agrasta ($\kappa \approx n$)

κ	n	r
80	81	4
128	129	4
256	257	5

- The data limit for each n-bit key K: $\sqrt{2^{\kappa}}/n$

The Dasta Primitive

- Dasta was proposed at ToSC 2020.
- An FHE-friendly primitive (low AND-depth & #AND gates).
- The linear layer in each round is composed of a fixed linear transform L and an ever-changing bit permutation $P_{i,C}$.

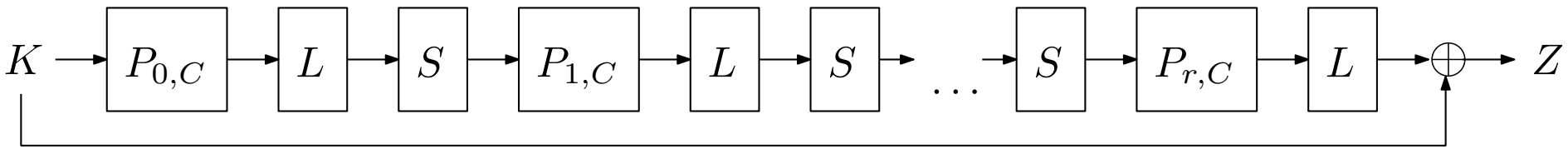


Figure: Illustration of r rounds of Dasta

■ Main feature:

- No PRNG is used.
- No need to generate random full-rank matrices.

The Recommended Parameters for Dasta

Table: Parameters of Dasta

κ	n	r
80	327	4
	327	5
	219	6
128	1877	4
	525	5
	351	6
256	~~445939~~	~~4~~
	3545	5
	703	6

- The data limit for each n-bit key K: $\sqrt{2^{\kappa}}/n$

How to Analyze Rasta

- The most challenging problems:
  - It is a moving target.
  - Traditional techniques like differential/linear/cube/higher-order differential attacks all fail because they require to collect many plaintext-ciphertext pairs under a fixed encryption instance.
- Some exploitable features:
  - The degree is 2 of the χ operation in the forward direction.
  - The number of rounds is small.
  - There is a feed-forward operation.

!!! The algebraic attack seems potential for the low degree of the keystream.

Trivial Linearization Attacks

Linearization attack

It is the simplest algebraic attack. First, the attacker collects t equations in terms of m variables and the degree of these equations is upper bounded by d. If $t \geq \sum_{i=1}^{d} \binom{m}{i}$, he can rename all the terms of degree larger than 1 with new variables. Finally, the problem is equivalent to solving t linear equations in terms of $\sum_{i=1}^{d} \binom{m}{i}$ variables, which can be easily solved by Gaussian elimination.

■ The degree d dominates the time complexity of the linearization attack when m is fixed. The smaller d, the lower the time complexity of the Gaussian elimination and the attack.

Trivial Linearization Attacks

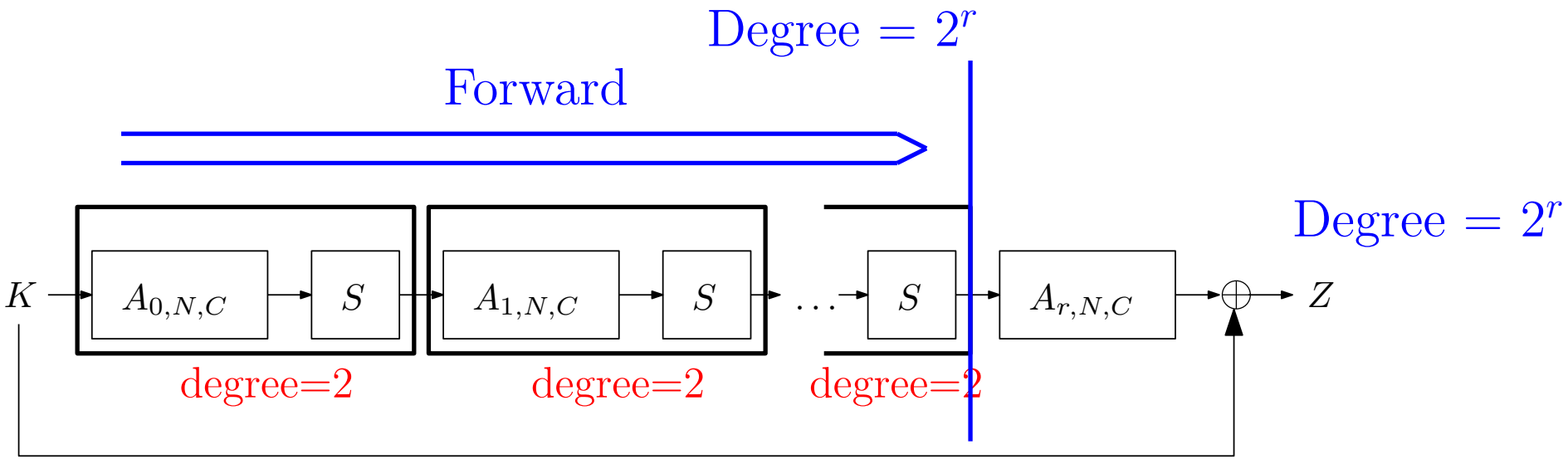


Figure: The trivial linearization attack on r-round Rasta

Trivial Linearization Attacks

- Can we consider the backward direction?

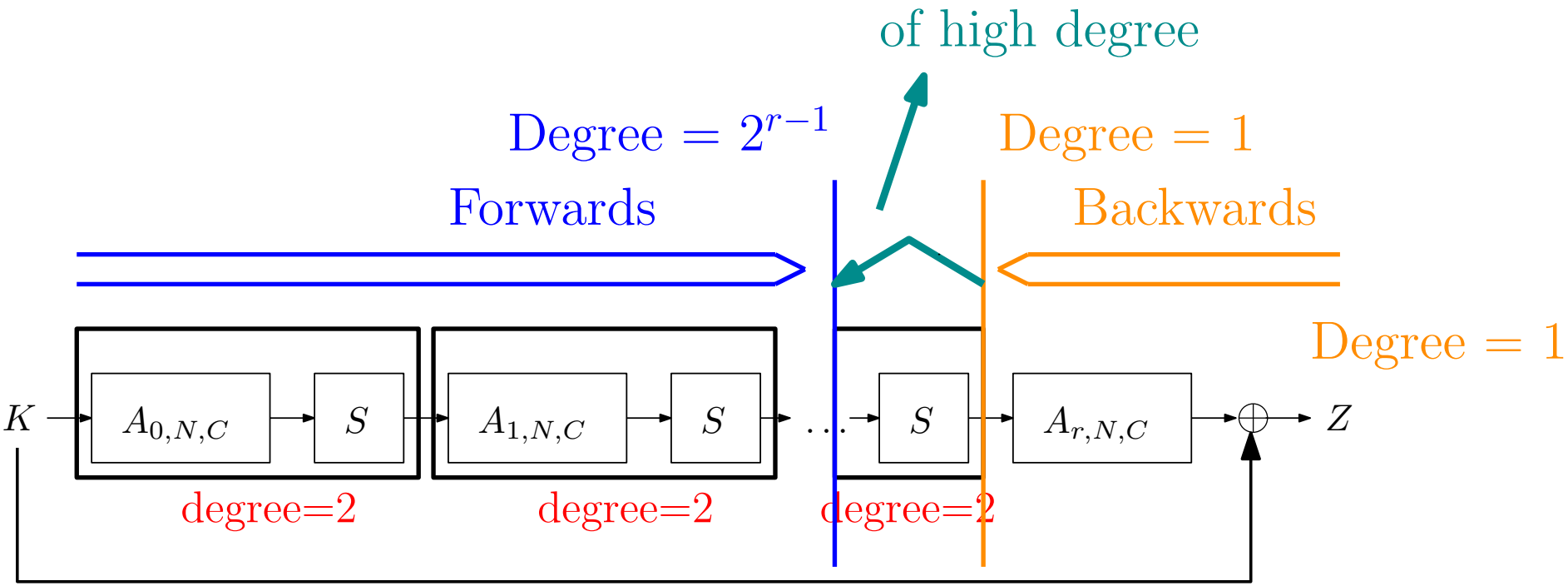
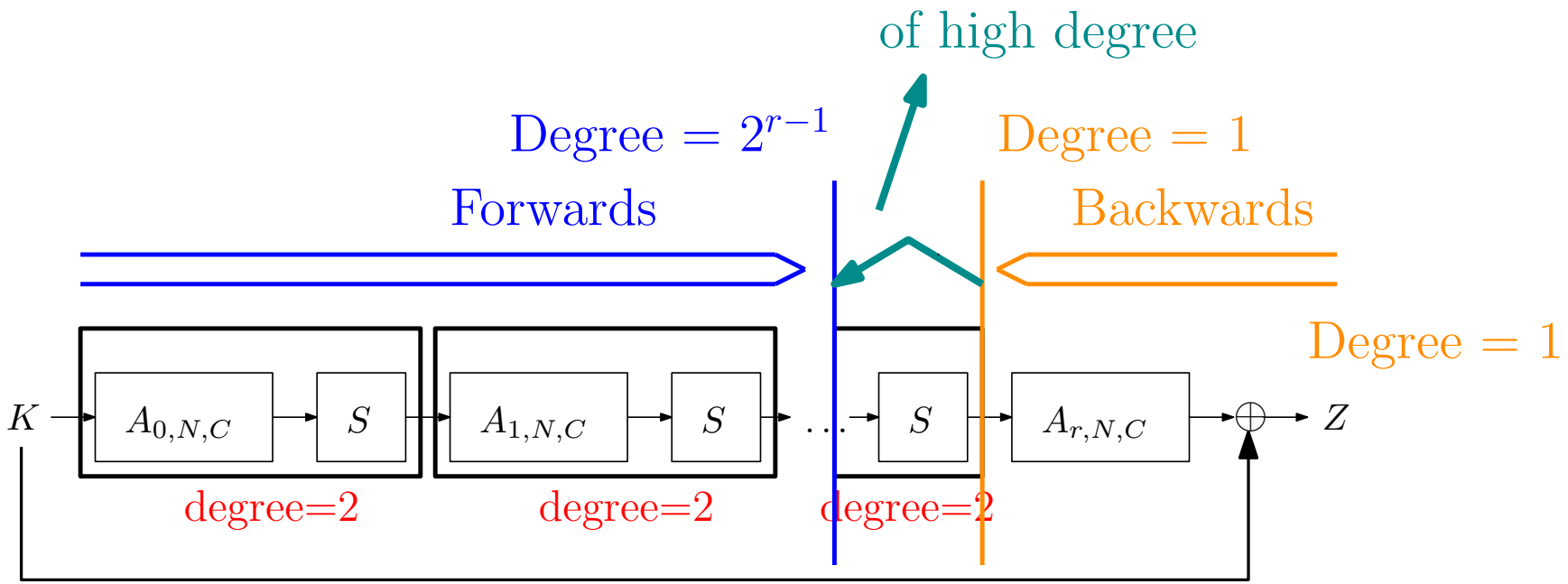


Figure: The trivial linearization attack on r-round Rasta by considering the backward direction for 1 round

However, $Deg(\chi^{-1}) = (n-1)/2 + 1$ when χ works on n bits.

Improved Linearization Attacks

- Some facts:
  - In the backward direction, the degree of the output of the last χ operation is 1.
  - In the forward direction, the degree of the input of the last χ operation is 2^{r-1} if we consider an r-round attack.
  - The inverse of the large χ operation is of very high degree.
  - We should never consider the full inverse of the χ operation.



Improved Linearization Attacks

- How do we find the improved attack?
  - The study [1] on the 3-bit LowMC S-box which is defined as below:

$$\begin{aligned} y_0 &= x_0 \oplus x_1 x_2, \\ y_1 &= x_0 \oplus x_1 \oplus x_0 x_2, \\ y_2 &= x_0 \oplus x_1 \oplus x_2 \oplus x_0 x_1. \end{aligned}$$

[1] Fukang Liu, Takanori Isobe, Willi Meier: A Simple Algebraic Attack on 3-Round LowMC. https://eprint.iacr.org/2021/255.

Improved Linearization Attacks

- How do we find the improved attack?
  - 8 More linearly independent quadratic equations:

$$
\begin{aligned}
y_0x_1 &= x_0x_1 \oplus x_1x_2, \\
y_0x_2 &= x_0x_2 \oplus x_1x_2, \\
y_1x_0 &= x_0 \oplus x_1x_0 \oplus x_0x_2, \\
y_1x_2 &= x_1x_2, \\
y_2x_0 &= x_0 \oplus x_1x_0 \oplus x_2x_0 \oplus x_0x_1, \\
y_2x_1 &= x_0x_1 \oplus x_1 \oplus x_2x_1 \oplus x_0x_1, \\
y_0x_0 \oplus x_0 &= y_1x_1 \oplus x_0x_1 \oplus x_1, \\
y_1x_1 \oplus x_0x_1 \oplus x_1 &= y_2x_2 \oplus x_0x_2 \oplus x_1x_2 \oplus x_2
\end{aligned}
$$

The inverse of the LowMC S-box is also quadratic, thus resulting in totally 14 linearly independent quadratic equations.

Improved Linearization Attacks

- How do we find the improved attack?
  - Perform similar analysis for the n-bit χ operation:

$$\begin{aligned} y_0 &= x_0 \oplus \overline{x_1} x_2, \\ y_1 &= x_1 \oplus \overline{x_2} x_3, \\ &\cdots \\ y_{n-1} &= x_{n-1} \oplus \overline{x_0} x_1 \end{aligned}$$

  - Some simply derived equations:

$$\begin{aligned} y_i x_{i+1} &= x_i x_{i+1}, \\ y_i x_{i+2} &= x_i x_{i+2} \oplus \overline{x_{i+1}} x_{i+2}. \end{aligned}$$

Improved Linearization Attacks

- How do we find the improved attack?
  - Perform similar analysis for the n-bit χ operation:

$$\begin{aligned} y_0 &= x_0 \oplus \overline{x_1} x_2, \\ y_1 &= x_1 \oplus \overline{x_2} x_3, \\ &\cdots \\ y_{n-1} &= x_{n-1} \oplus \overline{x_0} x_1. \end{aligned}$$

  - Can we have equations in other forms?

$$y_i = x_i \oplus \overline{x_{i+1}} x_{i+2} \text{ and } y_{i+1} = x_{i+1} \oplus \overline{x_{i+2}} x_{i+3},$$

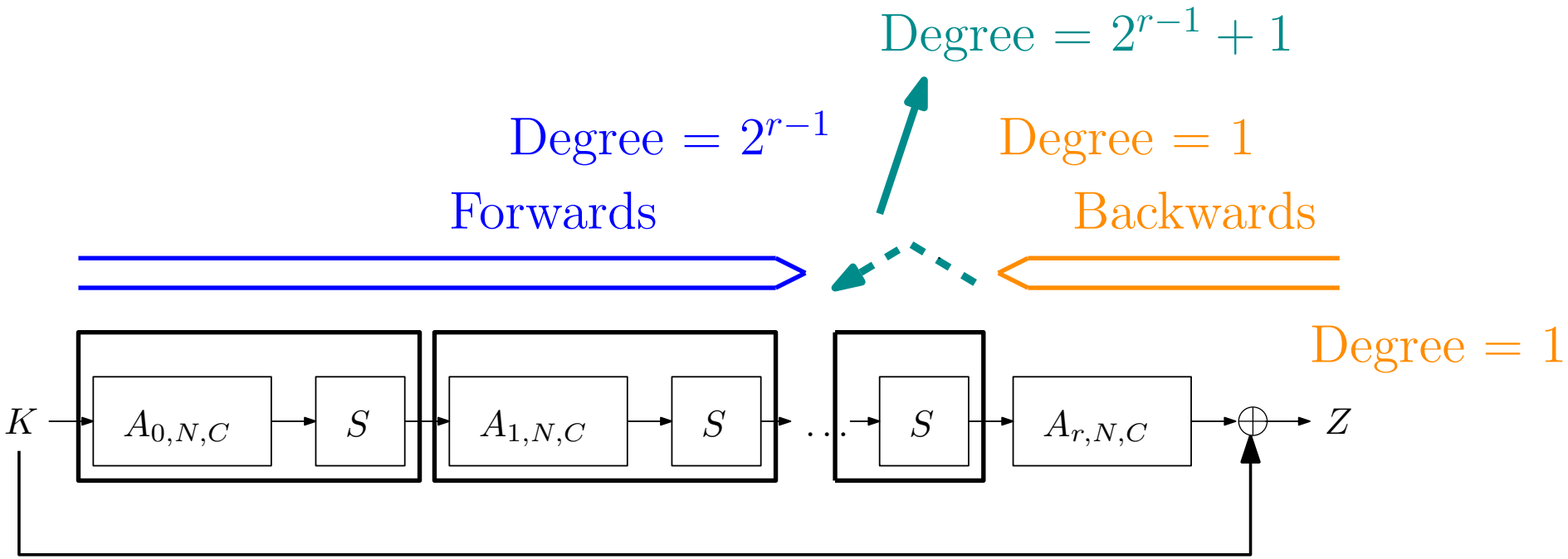
$$\Rightarrow (y_i \oplus x_i) y_{i+1} = \overline{x_{i+1}} x_{i+2} (x_{i+1} \oplus \overline{x_{i+2}} x_{i+3}) = 0.$$

Improved Linearization Attacks

- How do we find the improved attack?
  - What does $(y_i \oplus x_i)y_{i+1} = 0$ imply?
- Note that x_i is the input bit of the χ operation, while y_i is the output bit.
- Note that the expression of x_i is of degree 2^{r-1}, while the the expression of y_i is of degree 1.
- Although the large-scale χ operation is not fully inverted, we obtain an equation in terms of the key bits whose degree is upper bounded by $2^{r-1} + 1$, which is smaller than 2^r and $(n-1)/2 + 1$.

Improved Linearization Attacks

- How do we find the improved attack?
  - What does $(y_1 \oplus x_i)y_{i+1} = 0$ imply?



Improved Linearization Attacks

Implication of the discovered quadratic equation

The trivial linearization attack will be improved by one more round because attacking r-round Rasta with the new quadratic equation is now almost equivalent to attacking $(r-1)$-round Rasta with the trivial linearization attack, i.e. solving a system of nonlinear equations of degree $2^{r-1}+1$ in terms of n variables.

Improved Linearization Attacks

A natural question

Can we have other similar useful equations? If so, how to find them?

To answer this question, we should first understand what kind of equations are useful to improve the attack.

Exploitable equation

An exploitable equation is defined as an equation where the input bits of the χ operation are only allowed to form linear terms or quadratic terms with the output bits.

Improved Linearization Attacks

- How to find exploitable equations?
  1. Consider a small-scale χ operation, e.g. $n \in \{7, 9, 11, 13\}$.
  2. Use similar techniques to find quadratic equations for an S-box to find exploitable equations for the small-scale χ operation.
  3. Check whether the found exploitable equations also hold for the χ operation of any size.

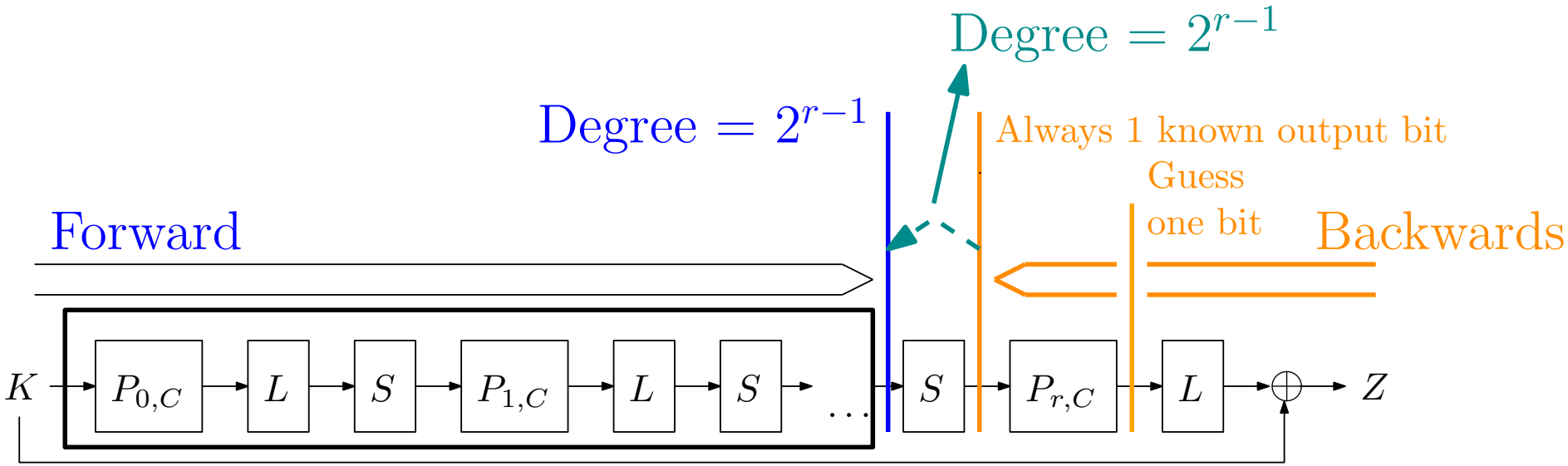
Improved Linearization Attacks

- The 5 exploitable equations used in this paper:

$$
\begin{aligned}
y_{i+1}(y_i \oplus x_i) &= 0, && (1)\\
y_i \oplus x_i \oplus (y_{i+1} \oplus 1)x_{i+2} &= 0, && (2)\\
y_{i+3}(y_{i+2}y_{i+1} \oplus y_{i+2} \oplus y_i \oplus x_i) &= 0, && (3)\\
y_{i+5}\left(x_i \oplus x_{i+2} \oplus y_i \oplus y_{i+1}y_{i+2} \oplus y_{i+1}\overline{y_{i+3}}y_{i+4}\right) &= 0, && (4)\\
y_{i+7}\left(x_i \oplus y_i \oplus \overline{y_{i+1}}y_{i+2} \oplus \overline{y_{i+1}}(y_{i+4} \oplus \overline{y_{i+5}}y_{i+6})\overline{y_{i+3}}\right) &= 0. && (5)
\end{aligned}
$$

Note that Eq. (2) has already been widely used in the preimage attack on Keccak. However, it is interpreted in a different way in that context, i.e. its form does not attract too much attention.

Further Optimizing the Linearization Attack on Dasta



Mainly exploit

$$y_i \oplus x_i \oplus (y_{i+1} \oplus 1)x_{i+2} = 0.$$

Then, attacking r-round Dasta is equivalent to solving a system of nonlinear equations of degree 2^{r-1} rather than $2^{r-1}+1$ in terms of n variables, i.e. Dasta is weaker than Rasta.

Summary of the Results

- Break the 2 out of 3 instances of Agrasta.
- The generic linearization attacks on Rasta and Dasta are all improved by 1 round for most instances.
- Dasta is weaker than Rasta, thus violating the designers' claim.

Conclusion

- New insights into the large-scale χ operation.
- New insights into how to analyze the Rasta-like primitives.
- Significantly improved linearization attacks on Rasta and Dasta.

Question

Can we further construct nonlinear equations of lower degree?

Thank you