Practical Attacks on Full-round FRIET

Senpeng Wang, Dengguo Feng, Bin Hu, Jie Guan, Tairong Shi

State Key Laboratory of Cryptology, Beijing, China

Talked by **Senpeng Wang**

Outline

1. Description of FRIET

2. A Differential Distinguisher for Full-round FRIET-PC

3. A Linear Distinguisher for Full-round FRIET-PC

4. Practical Attacks on Full-round FRIET-AE

5. Conclusions and Future Work

Outline

1. Description of FRIET

2. A Differential Distinguisher for Full-round FRIET-PC

3. A Linear Distinguisher for Full-round FRIET-PC

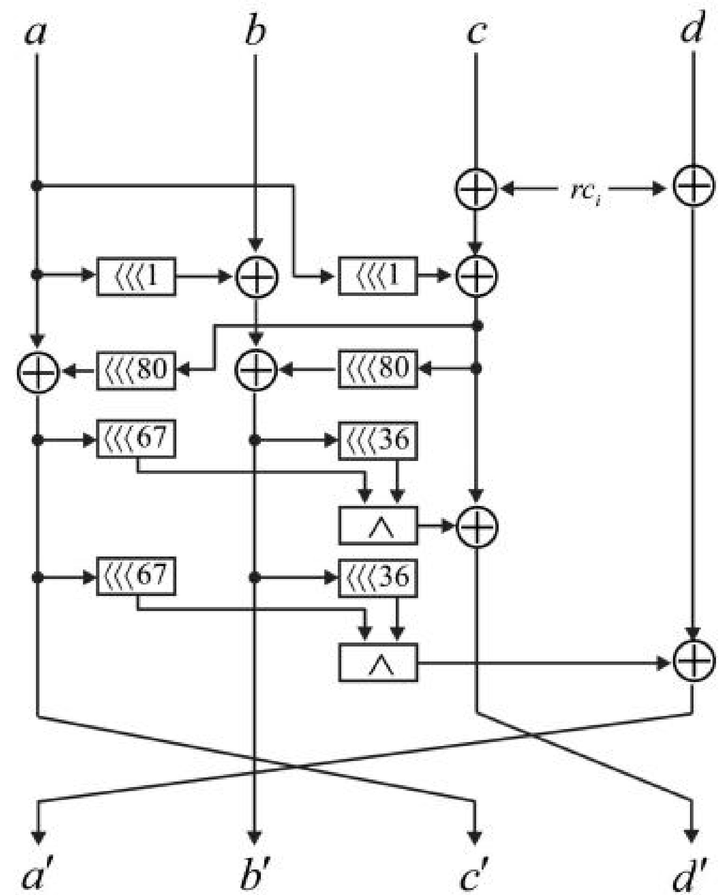
4. Practical Attacks on Full-round FRIET-AE

5. Conclusions and Future Work

1. Description of FRIET

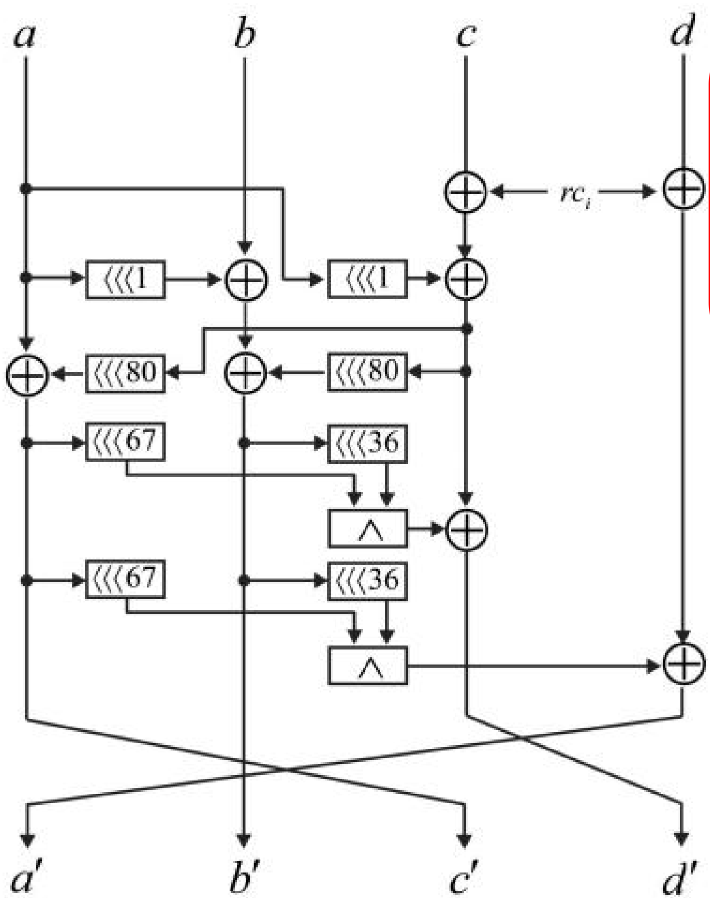
FRIET is an authenticated encryption scheme with built-in fault detection mechanisms proposed at EUROCRYPT 2020.

- State size: 4 limbs = 4× 128bits
- Round number: 24



(a) Round function of FRIET-P

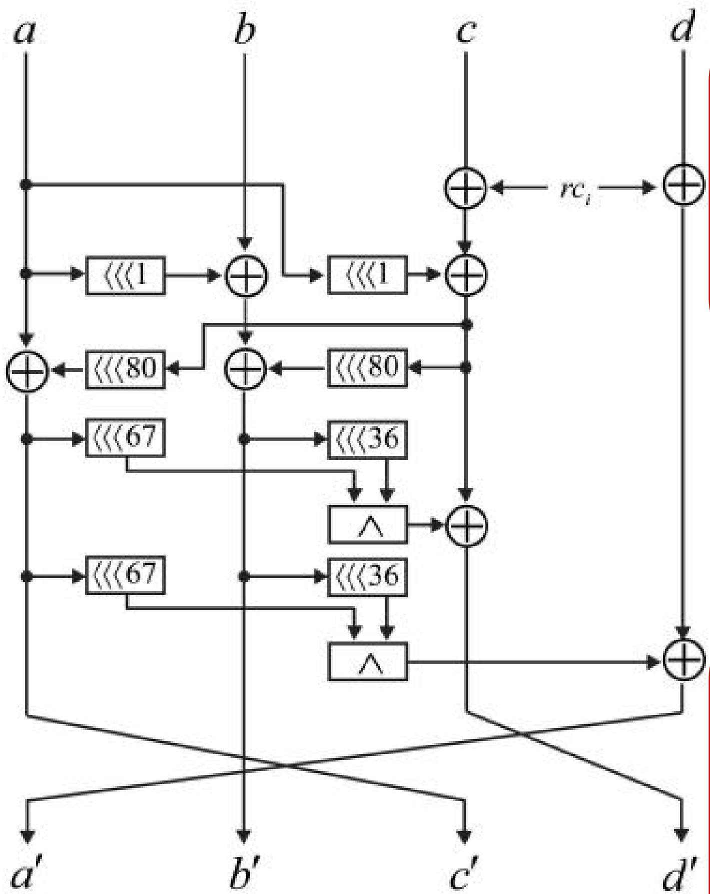
1. Description of FRIET



(a) Round function of FRIET-P

The round function of FRIET-P has slice-wise code-abiding property which means that $a \oplus b \oplus c = d$ implies $a' \oplus b' \oplus c' = d'$。

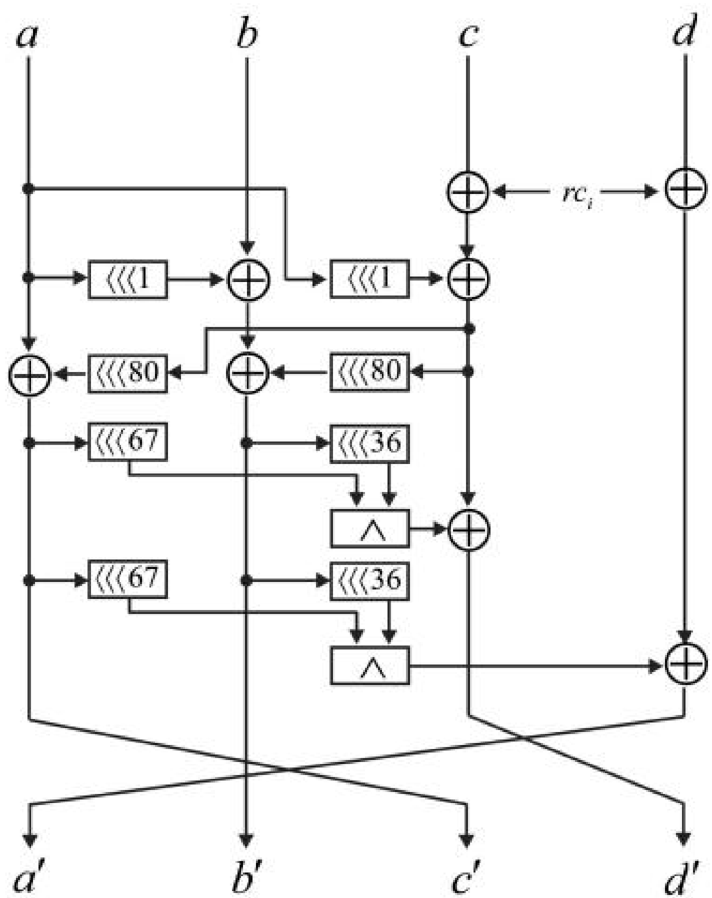
1. Description of FRIET



(a) Round function of FRIET-P

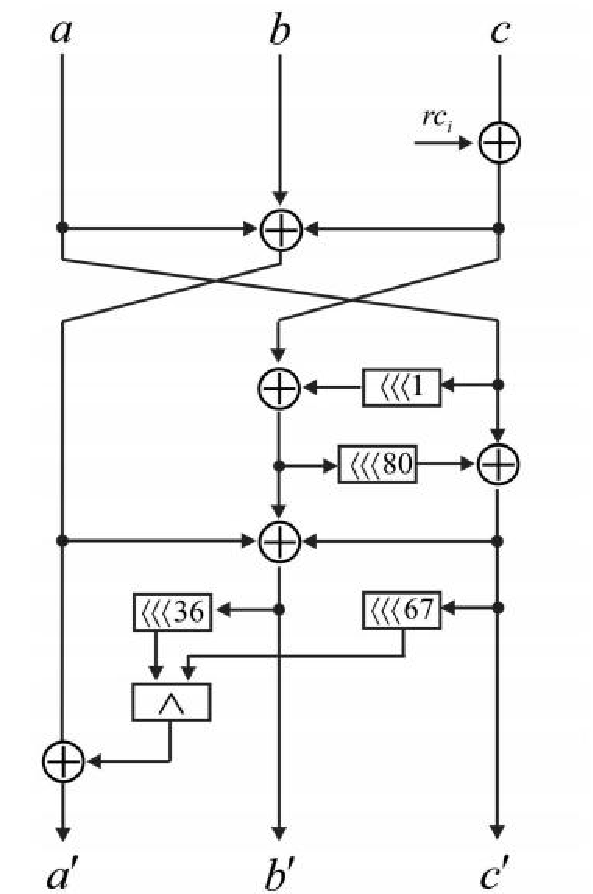
The round function of FRIET-P has slice-wise code-abiding property which means that $a \oplus b \oplus c = d$ implies $a' \oplus b' \oplus c' = d'$。

Faults will be detected if output does not have code–abiding property when the input state has code–abiding property.



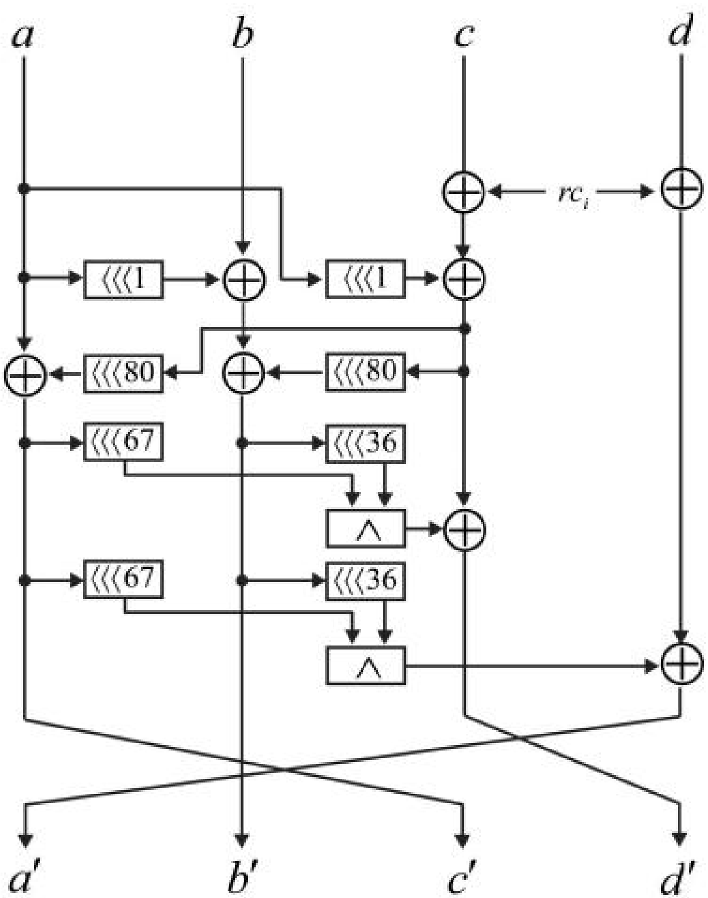
(a) Round function of FRIET-P

ignore *d*



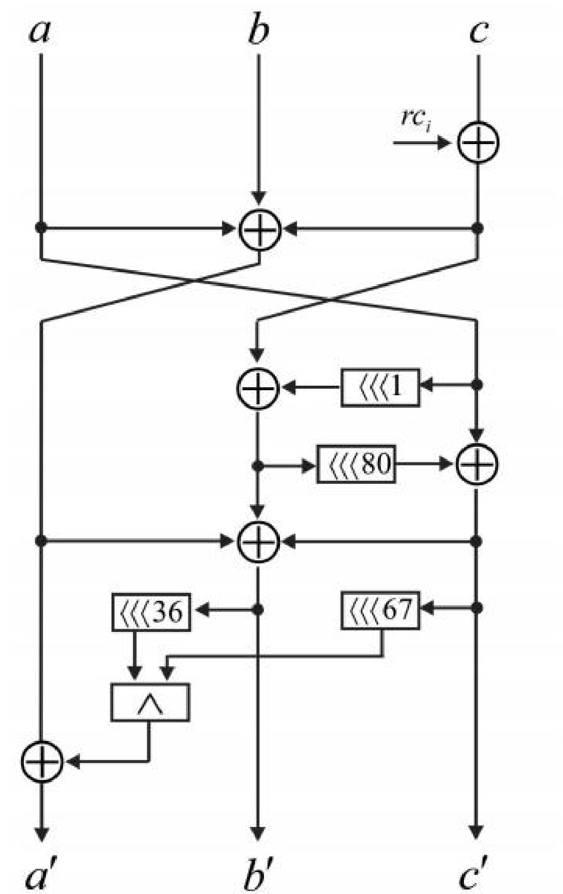
(b) Round function of FRIET-PC

1. Description of FRIET



(a) Round function of FRIET-P

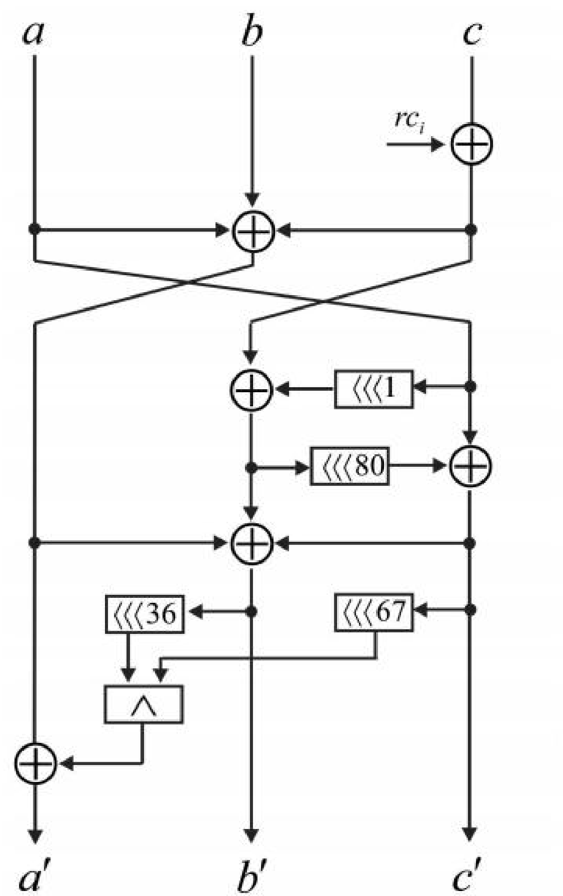
ignore d



(b) Round function of FRIET-PC

Since a distinguisher for FRIET-PC directly translates to a distinguisher for FRIET-P, we focus on FRIET-PC.

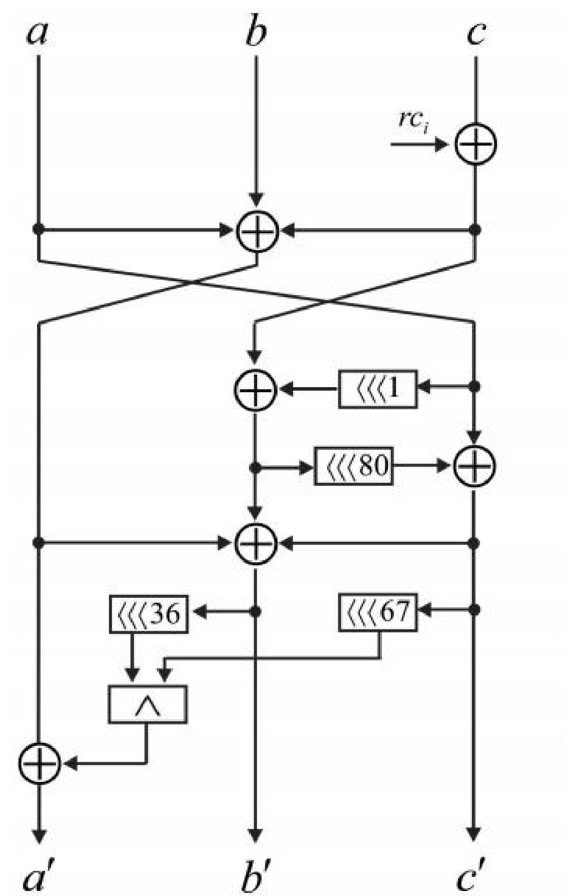
1. Description of FRIET



(b) Round function of FRIET-PC

- FRIET-PC only has four operations: Rotation, XOR, XOR-constant and AND. Bitwise AND is the only nonlinear operation.

1. Description of FRIET



(b) Round function of FRIET-PC

- FRIET-PC only has four operations: Rotation, XOR, XOR-constant and AND. Bitwise AND is the only nonlinear operation.

- If we can effectively control the propagations of differences and linear masks through bitwise AND operation, we can obtain pair of differences with high probabilities and linear masks with high correlations.

Outline

1. Description of FRIET

2. A Differential Distinguisher for Full-round FRIET-PC

3. A Linear Distinguisher for Full-round FRIET-PC

4. Practical Attacks on Full-round FRIET-AE

5. Conclusions and Future Works

2. A Differential Distinguisher for Full-round FRIET-PC

- **Rotation, XOR, XOR-Constant are linear operations, the differential probability of a valid pair of differences for these operations is 1.**

2. A Differential Distinguisher for Full-round FRIET-PC

- **Rotation, XOR, XOR-Constant are linear operations, the differential probability of a valid pair of differences for these operations is 1.**

Differential Property 1 (AND) [SBD+20] Let $z = x \wedge y$ be an AND function. For the input difference $\alpha || \beta \in F_2^{2n}$ of $x || y$ and output difference $\gamma \in F_2^n$ of z. Then, the differential probability can be calculated as following.

$$Pr[\alpha || \beta \to \gamma] = \begin{cases} 2^{-wt(\alpha \vee \beta)}, & \text{if } \overline{\alpha} \wedge \overline{\beta} \wedge \gamma = \mathbf{0}_n, \\ 0, & \text{otherwise,} \end{cases}$$

2. A Differential Distinguisher for Full-round FRIET-PC

- **Rotation, XOR, XOR-Constant are linear operations, the differential probability of a valid pair of differences for these operations is 1.**

Differential Property 1 (AND) [SBD+20] Let $z = x \wedge y$ be an AND function. For the input difference $\alpha||\beta \in F_2^{2n}$ of $x||y$ and output difference $\gamma \in F_2^n$ of z. Then, the differential probability can be calculated as following.

$$Pr[\alpha||\beta \to \gamma] = \begin{cases} 2^{-wt(\alpha \vee \beta)}, & \text{if } \overline{\alpha} \wedge \overline{\beta} \wedge \gamma = \mathbf{0}_n, \\ 0, & \text{otherwise,} \end{cases}$$

Thus, the differential probability of a valid pair of differences for bitwise AND operation is determined by $\boldsymbol{wt(\alpha \vee \beta)}$.

2. A Differential Distinguisher for Full-round FRIET-PC

- **By fixing the input difference of AND operation to 0, we have the following lemma.**

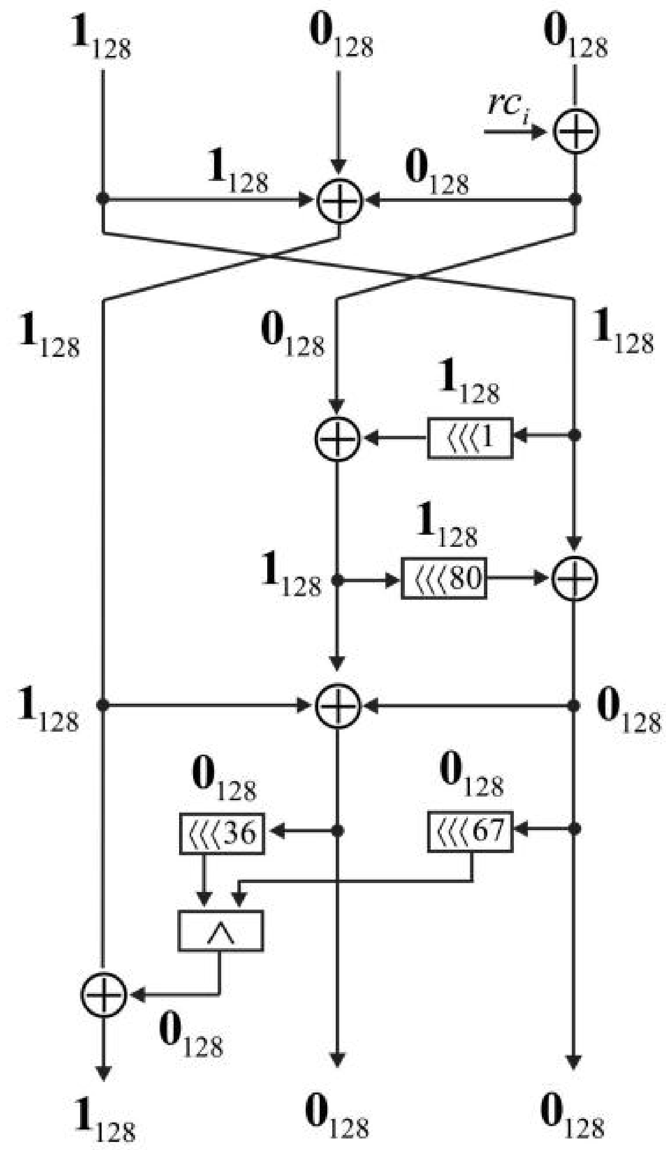
- **By fixing the input difference of AND operation to 0, we have the following lemma.**

Lemma 1 The differential probability of difference $(\alpha, \beta, \gamma) \rightarrow (\alpha', \beta', \gamma')$ for the round function of FRIET-PC is 1 if and only if

$$\begin{cases} \alpha' = \alpha \oplus \beta \oplus \gamma, \\ \alpha \oplus (\alpha \lll 1) \oplus \beta = \mathbf{0}_{128}, \\ \alpha \oplus (\alpha \lll 81) \oplus (\gamma \lll 80) = \mathbf{0}_{128}, \\ \beta' = \mathbf{0}_{128}, \\ \gamma' = \mathbf{0}_{128}. \end{cases}$$

2. A Differential Distinguisher for Full-round FRIET-PC

Based on Lemma 1, for full-round FRIET-PC, we obtain a differential distinguisher with probability 1. In order to help readers understand the differential distinguisher better, we show the propagation of it through 1-round FRIET-PC in the right part.



(a) Differential distinguisher

Outline

1. Description of FRIET

2. A Differential Distinguisher for Full-round FRIET-PC

3. A Linear Distinguisher for Full-round FRIET-PC

4. Practical Attacks on Full-round FRIET-AE

5. Conclusions and Future Works

3. A Linear Distinguisher for Full-round FRIET-PC

Because Rotation, XOR, XOR-Constant are all linear operations, the linear correlation of a valid pair of linear masks for these operations is 1 or -1.

3. A Linear Distinguisher for Full-round FRIET-PC

Because Rotation, XOR, XOR-Constant are all linear operations, the linear correlation of a valid pair of linear masks for these operations is 1 or -1.

Linear Property 1 (AND) [SBD+20]. *Let $z = f(x, y)$ be an AND function, where $x \in \mathbb{F}_2^n$ and $y \in \mathbb{F}_2^n$ are the input variables, and the output variable z is calculated as $z = x \wedge y$. Then,*

$$Cor(\alpha||\beta, \gamma) = \begin{cases} 2^{-wt(\gamma)}, & \text{if } \gamma \vee (\overline{\alpha} \wedge \overline{\beta}) = \mathbf{1}_n, \\ 0, & \text{otherwise,} \end{cases}$$

where $\alpha||\beta \in \mathbb{F}_2^{2n}$ and $\gamma \in \mathbb{F}_2^n$ are the linear masks of $x||y$ and z, respectively.

3. A Linear Distinguisher for Full-round FRIET-PC

Because Rotation, XOR, XOR-Constant are all linear operations, the linear correlation of a valid pair of linear masks for these operations is 1 or -1.

Linear Property 1 (AND) [SBD+20]. *Let $z = f(x, y)$ be an AND function, where $x \in \mathbb{F}_2^n$ and $y \in \mathbb{F}_2^n$ are the input variables, and the output variable z is calculated as $z = x \wedge y$. Then,*

$$Cor(\alpha||\beta, \gamma) = \begin{cases} 2^{-wt(\gamma)}, & \text{if } \gamma \vee (\overline{\alpha} \wedge \overline{\beta}) = \mathbf{1}_n, \\ 0, & \text{otherwise}, \end{cases}$$

where $\alpha||\beta \in \mathbb{F}_2^{2n}$ and $\gamma \in \mathbb{F}_2^n$ are the linear masks of $x||y$ and z, respectively.

Thus, the linear correlation of a valid pair of linear masks for bitwise AND operations is determined by $wt(\gamma)$.

3. A Linear Distinguisher for Full-round FRIET-PC

- **By fixing the output linear masks of AND operation to 0, we have the following lemma.**

3. A Linear Distinguisher for Full-round FRIET-PC

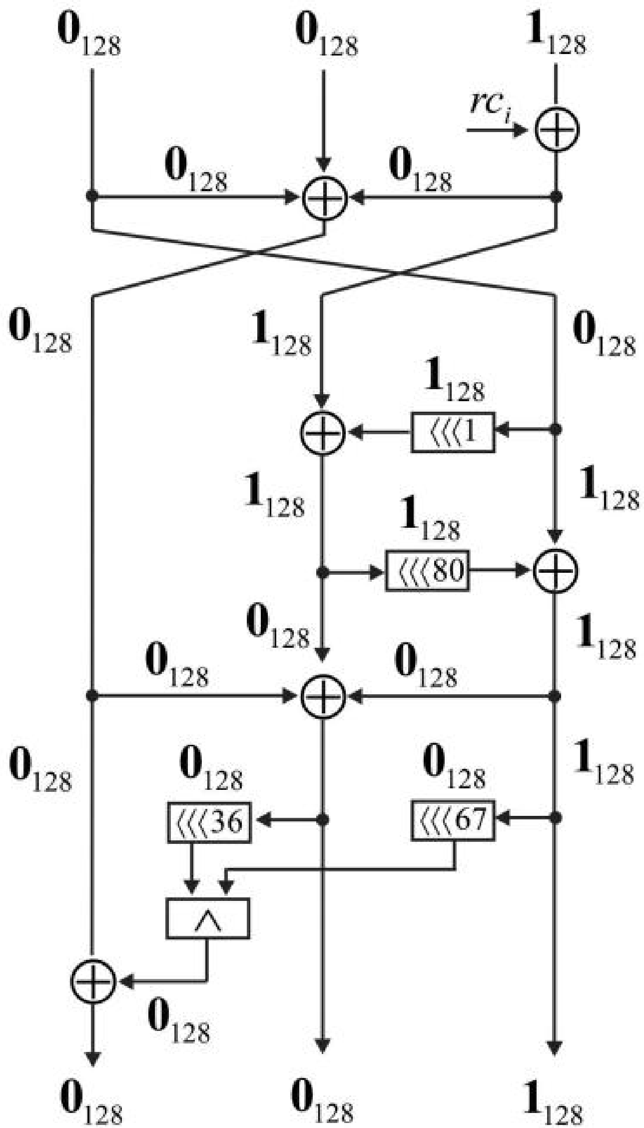
- **By fixing the output linear masks of AND operation to 0, we have the following lemma.**

Lemma 3. *Let* $\Gamma_{in} = (\alpha, \beta, \gamma)$ *and* $\Gamma_{out} = (\alpha', \beta', \gamma')$ *be the input and output linear masks of the i-th round function* $(a', b', c') = FRIET\text{-}PC_i\,(a, b, c)$*. The absolute value of correlation* $Cor\,(\Gamma_{in}, \Gamma_{out})$ *is 1 if and only if*

$$\begin{cases} \alpha' = \mathbf{0}_{128}, \\ \alpha \oplus (\beta' \ggg 1) \oplus \gamma' \oplus ((\beta' \oplus \gamma') \ggg 81) = \mathbf{0}_{128}, \\ \beta \oplus \beta' = \mathbf{0}_{128}, \\ \gamma \oplus ((\beta' \oplus \gamma') \ggg 80) = \mathbf{0}_{128}. \end{cases} \tag{13}$$

3. A Linear Distinguisher for Full-round FRIET-PC

According to Lemma 3, we obtain a linear distinguisher for full-round FRIET-PC whose absolute value of correlation is 1. We show the propagation of it through 1-round FRIET-PC in the right part.



(b) Linear distinguisher

Outline

1. Description of FRIET

2. A Differential Distinguisher for Full-round FRIET-PC

3. A Linear Distinguisher for Full-round FRIET-PC

4. Practical Attacks on Full-round FRIET-AE

5. Conclusions and Future Works

4. Practical Attacks on Full-round FRIET-AE

When FRIET-P is used in authenticated encryption scheme, FRIET-AE is obtained.

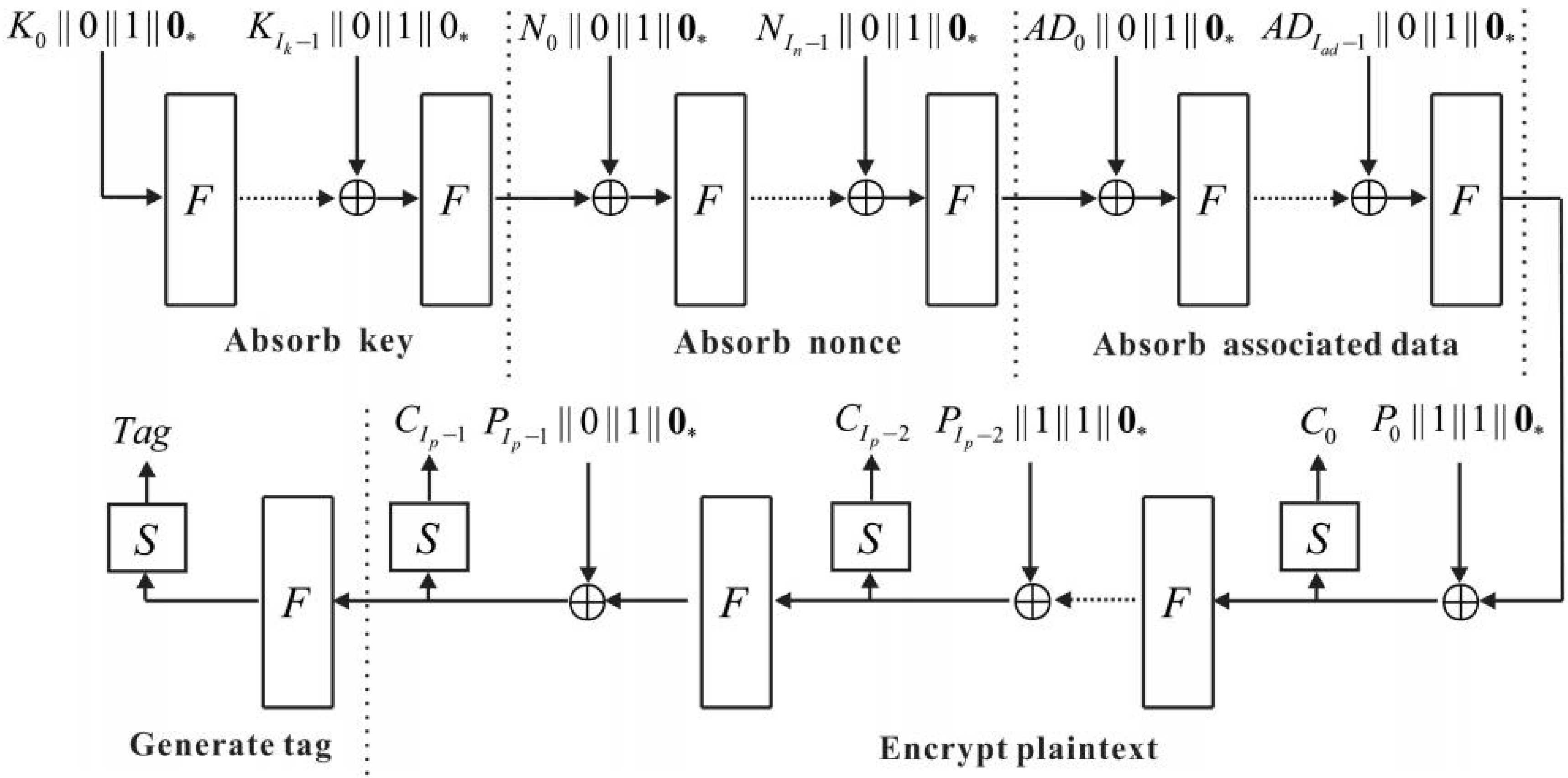


Figure 3: The encryption procedure of FRIET-AE [SBD+20]

4. Practical Attacks on Full-round FRIET-AE

Because the differential probabilities of $(1_{128}, 0_{128}, 0_{128}) \rightarrow (1_{128}, 0_{128}, 0_{128})$ over the full-round FRIET-PC are 1. Thus, we can introduce difference into key, nonce, associate data, and plaintext.

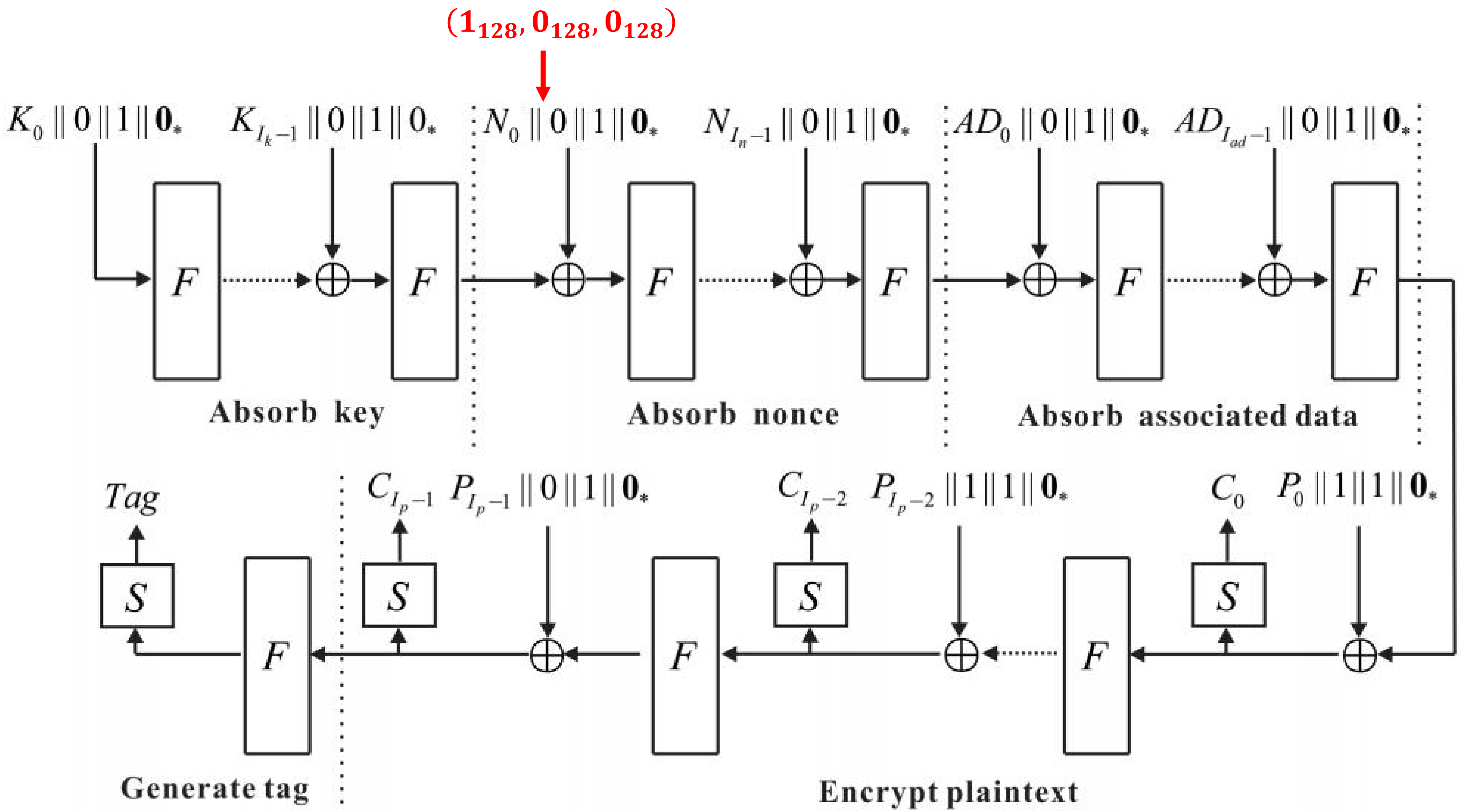


Figure 3: The encryption procedure of FRIET-AE [SBD+20]

4. Practical Attacks on Full-round FRIET-AE

Because the differential probabilities of $(1_{128}, 0_{128}, 0_{128}) \rightarrow (1_{128}, 0_{128}, 0_{128})$ over the full-round FRIET-PC are 1. Thus, we can introduce difference into key, nonce, associate data, and plaintext.

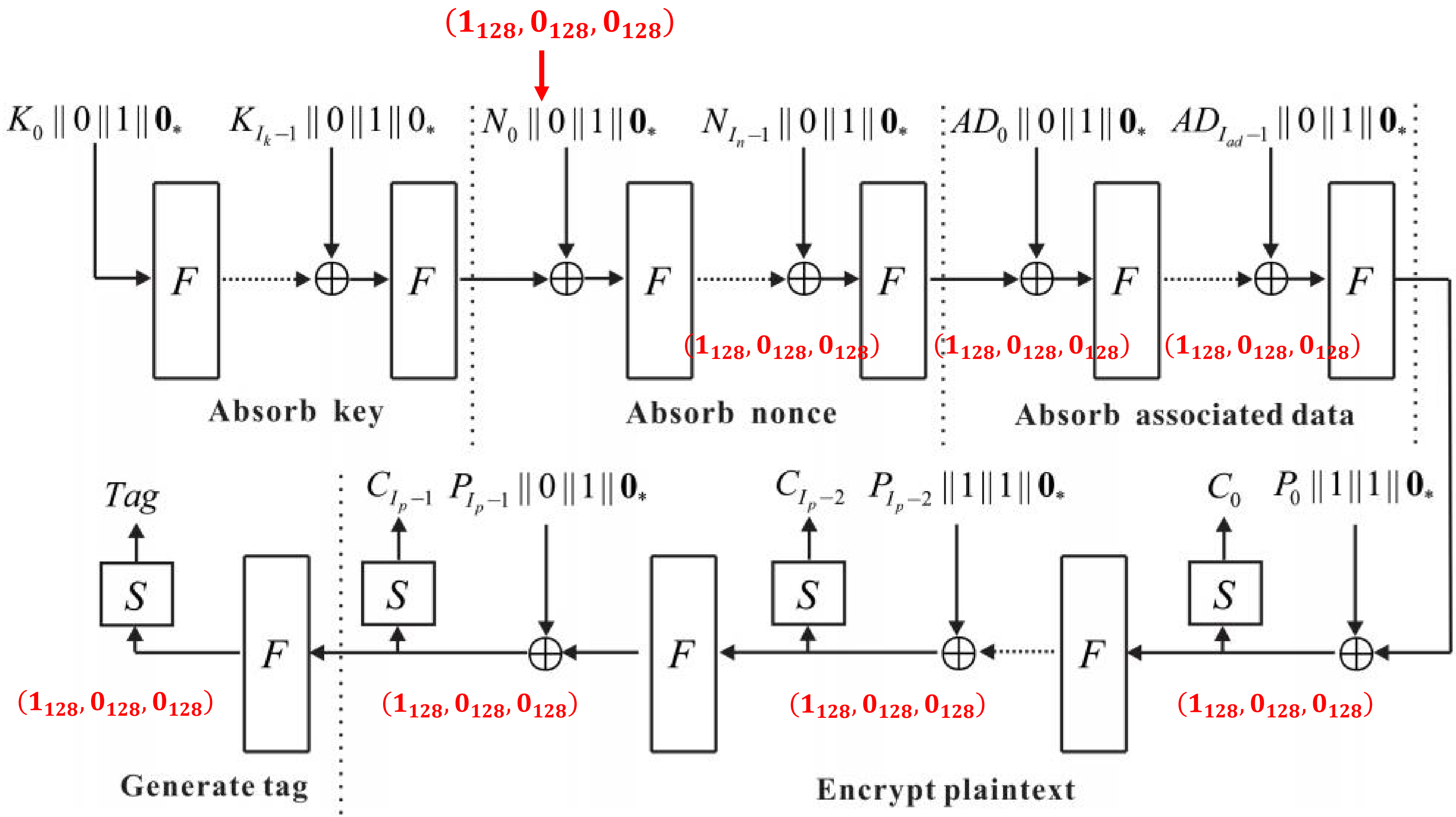


Figure 3: The encryption procedure of FRIET-AE [SBD+20]

Outline

1. Description of FRIET

2. A Differential Distinguisher for Full-round FRIET-PC

3. A Linear Distinguisher for Full-round FRIET-PC

4. Practical Attacks on Full-round FRIET-AE

5. Conclusions and Future Works

Conclusions

- Differential and linear distinguishers for the full-round FRIET-PC are proposed.

Table 1: The comparison of the distinguishers for FRIET-PC

*Type	Round	†Probability/Correlation/Data	Reference
LC	7	2^{-29}	[SBD+20]
	8	2^{-40}	[SBD+20]
	$^*R$	1 or -1	Sect. 3.1
R-DL	8	$2^{-17.81}$	[LSL21]
	9	$2^{-29.81}$	[LSL21]
	13	$2^{-117.81}$	[LSL21]
IC	13	2^{-31}	[ISS+21]
	15	2^{-63}	[ISS+21]
	17	2^{-127}	[ISS+21]
	30	2^{-383}	[ISS+21]
DC	6	2^{-59}	[SBD+20]
	9	$2^{-20.04}$	[ISS+21]
	$^*R$	1	Sect. 3.2

⋆ R-DL denotes rotational differential-linear distinguisher. LC denotes linear distinguisher. DC denotes differential distinguisher. IC denotes integral distinguisher.

† The DC is showed with probability. LC/DL/R-DL are showed with correlation. IC is showed with data.

* R means that the differential or linear distinguisher is valid for any-round FRIET-PC.

Conclusions

- Differential and linear distinguishers for the full-round FRIET-PC are proposed.
- Using the differential distinguisher with probability 1, we propose an algorithm which can generate a set consisting of valid tags and ciphertexts which are not created by legal users. This breaks the integrity and confidentiality security claims of FRIET-AE.

Conclusions

- Differential and linear distinguishers for the full-round FRIET-PC are proposed.
- Using the differential distinguisher with probability 1, we propose an algorithm which can generate a set consisting of valid tags and ciphertexts which are not created by legal users. This breaks the integrity and confidentiality security claims of FRIET-AE.

Future Works

- Our attack in this paper does not recover the secret key of FRIET-AE. How to give a key-recovery attack needs further research

Thanks