# Forgery Attacks on FlexAE and FlexAEAD

**Maria Eichlseder** Daniel Kales Markus Schofnegger

Cryptography and Coding – IMACC 2019

# Outline

## Motivation

- The NIST LWC Competition

## Background

- `FlexAEAD`
- Differential Cryptanalysis

## Differential Cryptanalysis of `FlexAEAD`

- Designers' Security Arguments
- Differential Cryptanalysis of the Block Cipher
- Application to the Mode

## Discussion and Conclusion

- Status of `FlexAEAD`
- Conclusion

# Motivation

Lightweight Cryptography

# Lightweight (Symmetric) Cryptography

- Secure **constrained devices**:
  low **energy**, low **area**, low **latency**, …
- Symmetric crypto like `AES` is
  **already quite lightweight**
  - Simplicity
  - Side-channel/fault protection
  - Robustness
  - Lightweight hashing
  - …

# Lightweight (Symmetric) Cryptography

- Secure **constrained devices**:
  low **energy**, low **area**, low **latency**, …
- Symmetric crypto like `AES` is
  **already quite lightweight , but…**
  - Simplicity
  - Side-channel/fault protection
  - Robustness
  - Lightweight hashing
  - …

# Competitions for Lightweight Cryptography

**CAESAR** Competition for Authenticated Encryption: Security, Applicability, Robustness

- Use-case 1: Lightweight cryptography
- Use-case 2: High SW performance
- Use-case 3: Robustness

| 2013 | 2014 | 2015 | 2016 | 2018 | 2019 |
|---|---|---|---|---|---|
| Call | Round 1 | Round 2 | Round 3 | Finalists | Portfolio |

**NIST LWC** LightWeight Cryptography Standardization Process

- Authenticated Encryption (AEAD)
- Hashing (optional)

| 2018 | 2019 | 2019 | . . . |
|---|---|---|---|
| Call | Round 1 | Round 2 | . . . |
| | 56 candidates | 32 candidates | |

National Institute of Standards and Technology
U.S. Department of Commerce

# FlexAEAD

- is an **AEAD design** by Marsola do Nascimento and Moreira Xexéo
- was a **Round-1 candidate** in the NIST LWC competition [NX19a]
- evolved from the previously published design FlexAE [NX17]

- uses a **non-ideal** (distinguishable) internal block cipher $\mathtt{PF}_K$ as its **primitive**
- is still claimed to be secure since data traverses **multiple block cipher calls**

## Main Results

We show that the designers' claim is incorrect and derive **attacks**:

- We introduce differences not **only via the data**, but via the **mode's control flow**.
- We exploit a strong differential **clustering** effect in the block cipher.
- We propose **forgery attacks** on all `FlexAEAD` variants and `FlexAE`:

| | Key size | Tag size | $-\log_2$(Success probability) |
|---|---|---|---|
| `FlexAEAD-64` | 128 bits | 64 bits | 46 (with 1 short CP query) |
| `FlexAEAD-128` | 128 bits | 128 bits | 54 (with 1 short CP query) |
| `FlexAEAD-256` | 256 bits | 256 bits | 70 (with 1 short CP query) |
| `FlexAE-64-128` | 128 bits | 64 bits | 54 (with 0 queries!) |
| ... | | | ... |

- We discuss some additional problems of the mode (easier to fix).

# Background

Design & Cryptanalysis

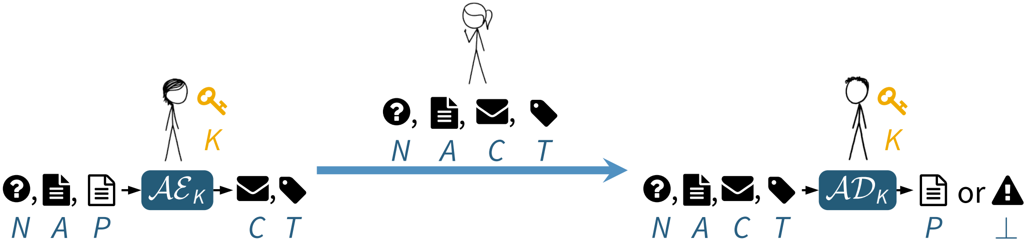
# Authenticated Encryption with Associated Data (AEAD)


An AEAD scheme defines an authenticated encryption function $\mathcal{AE}_K$ that maps a key $K$, nonce $N$, associated data $A$, and message $P$ to a ciphertext $C$ and tag $T$. Its verified decryption function $\mathcal{AD}_K$ returns either the message $P$ or an error $\perp$.

$$\mathcal{AE}_K : \mathbb{F}_2^k \times \mathbb{F}_2^n \times \mathbb{F}_2^* \times \mathbb{F}_2^* \to \mathbb{F}_2^* \times \mathbb{F}_2^t, \qquad \mathcal{AE}_K(N, A, P) = C, T$$

$$\mathcal{AD}_K : \mathbb{F}_2^k \times \mathbb{F}_2^n \times \mathbb{F}_2^* \times \mathbb{F}_2^* \times \mathbb{F}_2^t \to \mathbb{F}_2^*, \qquad \mathcal{AD}_K(N, A, C, T) = P$$

# Authenticated Encryption with Associated Data (AEAD)



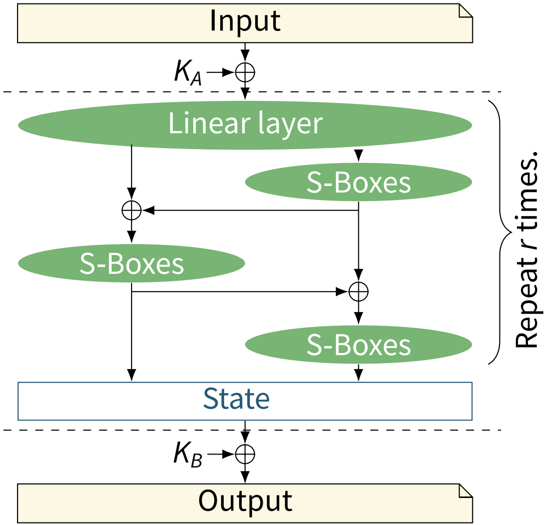

An AEAD scheme defines an authenticated encryption function $\mathcal{AE}_K$ that maps a key $K$, nonce $N$, associated data $A$, and message $P$ to a ciphertext $C$ and tag $T$. Its verified decryption function $\mathcal{AD}_K$ returns either the message $P$ or an error $\perp$.

$$\mathcal{AE}_K : \mathbb{F}_2^k \times \mathbb{F}_2^n \times \mathbb{F}_2^* \times \mathbb{F}_2^* \to \mathbb{F}_2^* \times \mathbb{F}_2^t, \qquad \mathcal{AE}_K(N, A, P) = C, T$$

$$\mathcal{AD}_K : \mathbb{F}_2^k \times \mathbb{F}_2^n \times \mathbb{F}_2^* \times \mathbb{F}_2^* \times \mathbb{F}_2^t \to \mathbb{F}_2^*, \qquad \mathcal{AD}_K(N, A, C, T) = P$$

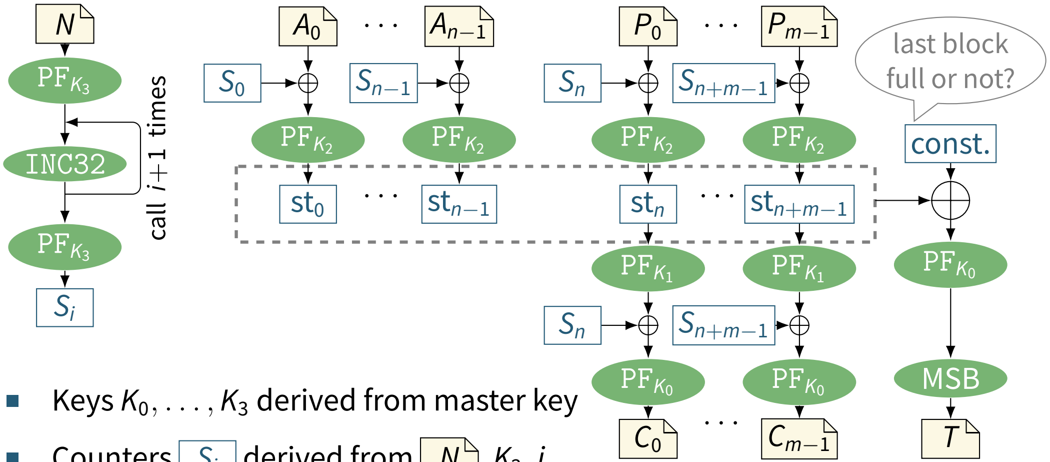
Goal: protect the confidentiality of $P$ and the authenticity of $P$ and $A$.

# FlexAEAD's Internal Block Cipher $\mathtt{PF}_K$




- Block size $\in \{64, 128, 256\}$ bits
  Key size $\in \{128, 256, 512\}$ bits
- Even-Mansour construction with whitening keys $K_A \parallel K_B = K$
- $r \in \{5, 6, 7\}$ rounds for $\mathtt{FlexAEAD}$-$\{64, 128, 256\}$
  - Linear layer: Shuffling of 4-bit nibbles
  - S-box layer: 8-bit AES S-box

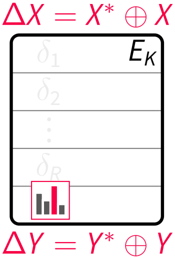
# `FlexAEAD`'s Mode of Operation [NX19a] (slightly simplified)




- Keys $K_0, \ldots, K_3$ derived from master key
- Counters $S_i$ derived from $N$, $K_3$, $i$
- Block cipher $\mathrm{PF}_K$, increment $\mathrm{INC32}$

# Differential Cryptanalysis [BS90]

## Differential




Derivative for $\Delta X = \alpha$:

$$\Delta_\alpha E(X) := E(X \oplus \alpha) \oplus E(X)$$

## Attack Goals



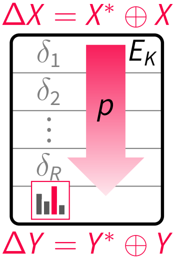

Key recovery




Collision / Forgery

# Differential Cryptanalysis [BS90]

## Diff. Characteristic




Derivative for $\Delta X = \alpha$:

$$\Delta_\alpha E(X) := E(X \oplus \alpha) \oplus E(X)$$

## Attack Goals



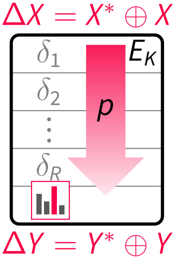

Key recovery




Collision / Forgery

# Differential Cryptanalysis [BS90]

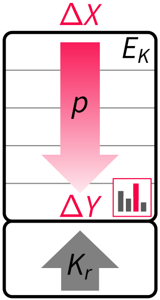
## Diff. Characteristic



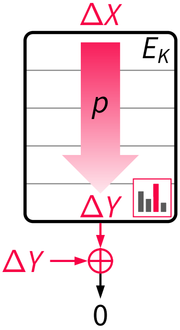

Derivative for $\Delta X = \alpha$:

$$\Delta_\alpha E(X) := E(X \oplus \alpha) \oplus E(X)$$

## Attack Goals




Key recovery



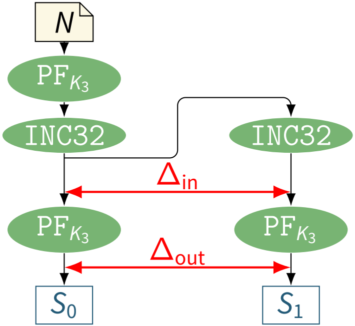

Collision / Forgery

# Differential Cryptanalysis of `FlexAEAD`

# Designers' Security Arguments

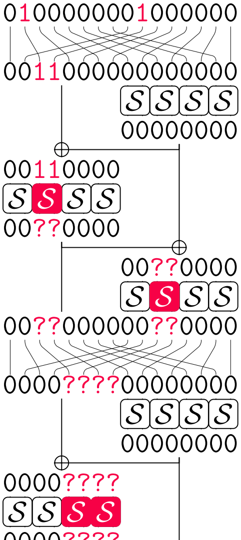
- At least **2 active S-boxes per round** in any characteristic
- **Maximum differential probability** of the `AES` S-box is $2^{-6}$
- Differences in $P_i$ pass through **3 $r$ rounds** ($\mathtt{PF}^3$) before attacker gets $C_i$
- $3\,r \cdot 2 \cdot (-6)$ is much smaller than the blocksize in each variant,
  so differential cryptanalysis gives no advantage over generic attacks

# Differences in the Counter Sequence




- Consider the **difference between two counters**, say, $\boxed{S_0}$ and $\boxed{S_1}$
- INC32 adds $+1$ to every 32-bit subword (little-endian integer)
- Equivalent to $\oplus 1$ with probability $\frac{1}{2}$
  $2^{-2}, 2^{-4}, 2^{-8}$ for `FlexAEAD`-$\{64, 128, 256\}$
- E.g., for $\mathtt{PF}_K$ in `FlexAEAD-64`, consider
  $\Delta_{in} = 01000000\ 01000000 \rightarrow$
  $\Delta_{out} = ???$

# Finding Differential Characteristics for $\mathtt{PF}_K$

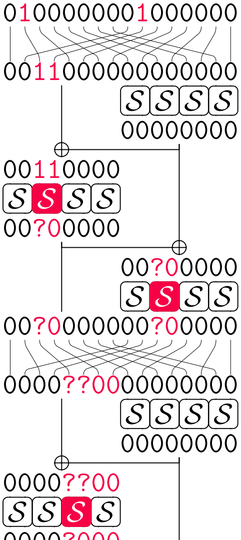



1. Find a “nibble-truncated” characteristic with **Mixed-Integer Linear Programming (MILP)**

   - 2 binary variables $(b_L, b_R)$ per byte $b$
   - 1 binary variable $s$ per S-box, 1 $x$ per nibble XOR
   - $c_* = a_* \oplus b_*$: $\quad 2 \cdot x \leq a_* + b_* + c_* \leq 3 \cdot x$
   - $b = \mathcal{S}(a)$: $\quad a_L + a_R + b_L + b_R \leq 4 \cdot s,$
     $2 \cdot s \leq a_L + a_R, \quad 2 \cdot s \leq b_L + b_R$
   - Minimize sum of $7 \cdot s$ for all S-boxes (bound)

2. Find a bitwise characteristic with **SAT solver**

# Finding Differential Characteristics for $\mathtt{PF}_K$

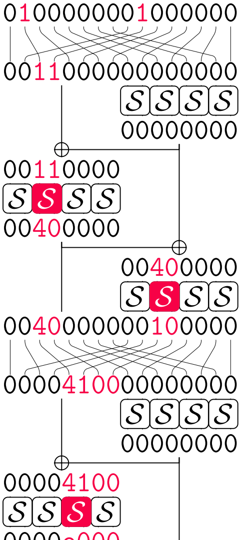



**1** Find a “nibble-truncated” characteristic with **Mixed-Integer Linear Programming (MILP)**

- 2 binary variables $(b_{\mathsf{L}}, b_{\mathsf{R}})$ per byte $b$
- 1 binary variable $s$ per S-box, 1 $x$ per nibble XOR
- $c_* = a_* \oplus b_*$: $\quad 2 \cdot x \leq a_* + b_* + c_* \leq 3 \cdot x$
- $b = \mathcal{S}(a)$: $\quad a_{\mathsf{L}} + a_{\mathsf{R}} + b_{\mathsf{L}} + b_{\mathsf{R}} \leq 4 \cdot s,$
  $2 \cdot s \leq a_{\mathsf{L}} + a_{\mathsf{R}}, \quad 2 \cdot s \leq b_{\mathsf{L}} + b_{\mathsf{R}}$
- Minimize sum of $7 \cdot s$ for all S-boxes (bound)

**2** Find a bitwise characteristic with **SAT solver**

# Finding Differential Characteristics for $\mathtt{PF}_K$

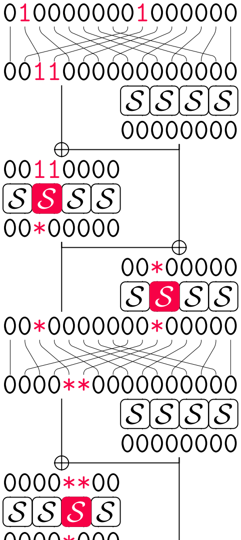



**1** Find a “nibble-truncated” characteristic with **Mixed-Integer Linear Programming (MILP)**

- 2 binary variables $(b_L, b_R)$ per byte $b$
- 1 binary variable $s$ per S-box, 1 $x$ per nibble XOR
- $c_* = a_* \oplus b_*$: $\quad 2 \cdot x \le a_* + b_* + c_* \le 3 \cdot x$
- $b = \mathcal{S}(a)$: $\quad a_L + a_R + b_L + b_R \le 4 \cdot s,$
  $2 \cdot s \le a_L + a_R, \quad 2 \cdot s \le b_L + b_R$
- Minimize sum of $7 \cdot s$ for all S-boxes (bound)

**2** Find a bitwise characteristic with **SAT solver**

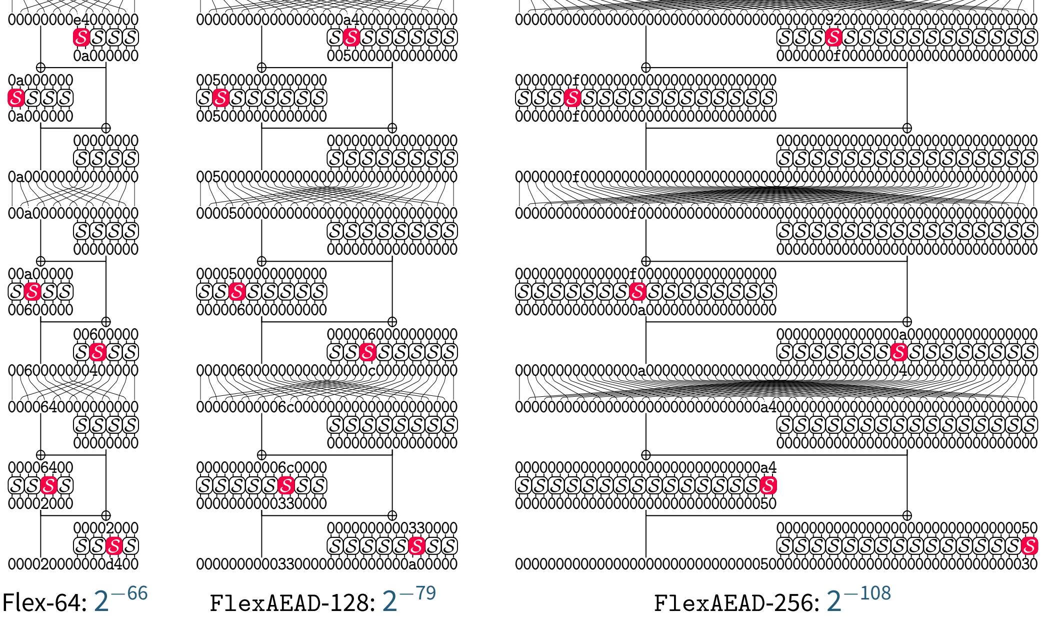
# Clustering Differential Characteristics for $\mathtt{PF}_K$

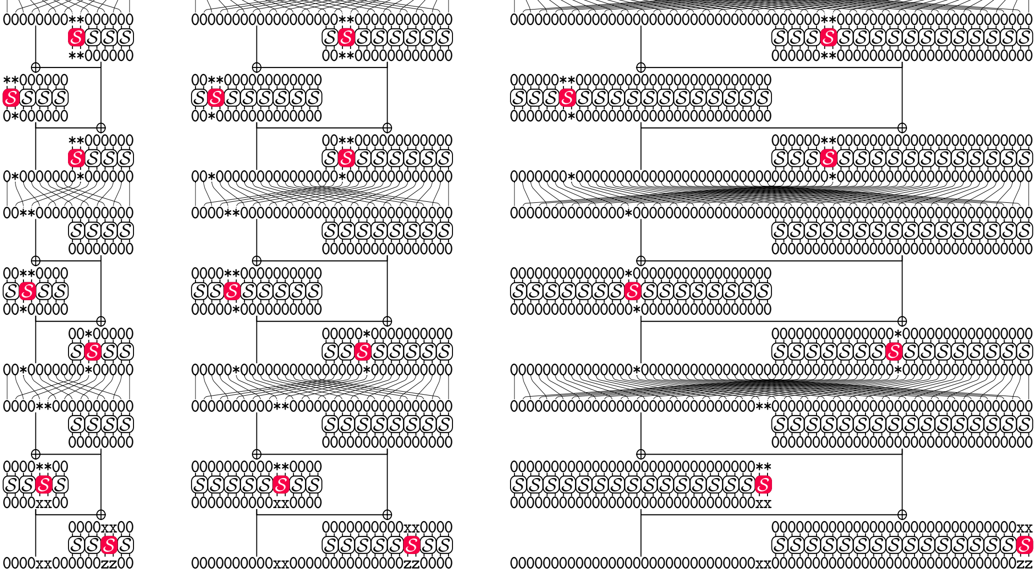



1. Find a "nibble-truncated" characteristic with **Mixed-Integer Linear Programming (MILP)**

   - 2 binary variables $(b_{\mathsf{L}}, b_{\mathsf{R}})$ per byte $b$
   - 1 binary variable $s$ per S-box, 1 $x$ per nibble XOR
   - $c_* = a_* \oplus b_*$: $\quad 2 \cdot x \leq a_* + b_* + c_* \leq 3 \cdot x$
   - $b = \mathcal{S}(a)$: $\quad a_{\mathsf{L}} + a_{\mathsf{R}} + b_{\mathsf{L}} + b_{\mathsf{R}} \leq 4 \cdot s,$
     $2 \cdot s \leq a_{\mathsf{L}} + a_{\mathsf{R}}, \quad 2 \cdot s \leq b_{\mathsf{L}} + b_{\mathsf{R}}$
   - Minimize sum of $4 \cdot (2\,s - b_{\mathsf{L}} - b_{\mathsf{R}})$ for all S-boxes

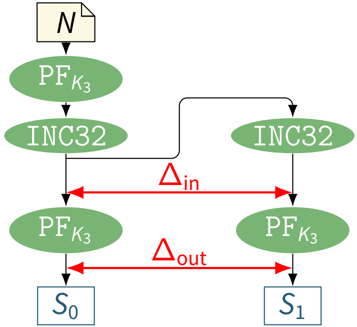
2. Fix suitable bitwise input/output differential (easy)

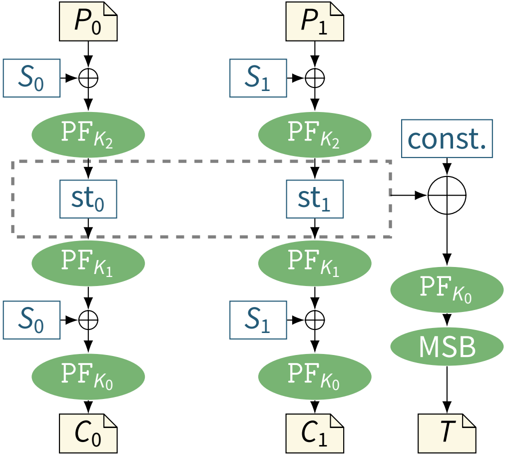

Flex-64: $2^{-66}$
FlexAEAD-128: $2^{-79}$
FlexAEAD-256: $2^{-108}$



Flex-64: $2^{-46}$ FlexAEAD-128: $2^{-54}$ FlexAEAD-256: $2^{-70}$

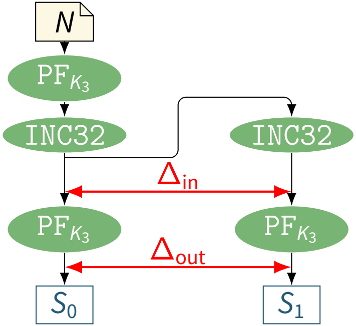
# Forgery Attacks for `FlexAEAD` – Example: Ciphertext Swap

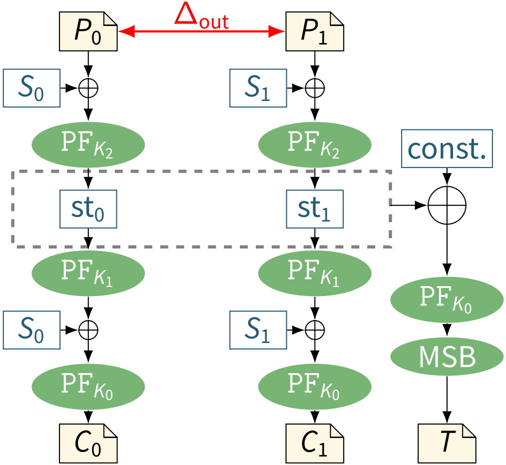



- Query $N$ and $P_0 \oplus P_1 = \Delta_{out}$
- With prob. $p$, $S_0 \oplus S_1 = \Delta_{out}$
- Then ($C_1 \| C_0$, $T$) is a valid ciphertext-tag pair with nonce $N$!

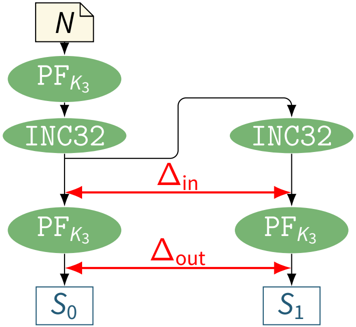
# Forgery Attacks for `FlexAEAD` – Example: Ciphertext Swap

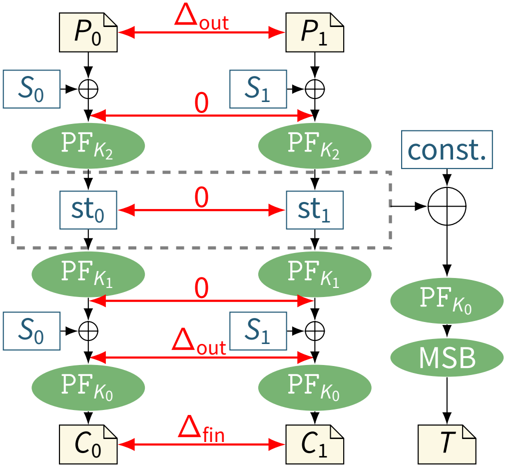



- Query $N$ and $P_0 \oplus P_1 = \Delta_{out}$
- With prob. $p$, $S_0 \oplus S_1 = \Delta_{out}$
- Then ($C_1 \parallel C_0$, $T$) is a valid ciphertext-tag pair with nonce $N$!

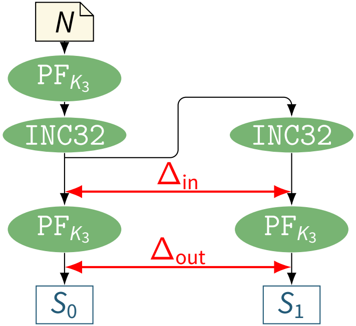
# Forgery Attacks for `FlexAEAD` – Example: Ciphertext Swap

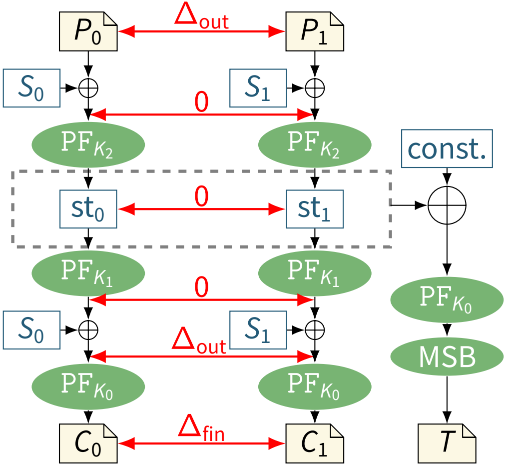



- Query $N$ and $P_0 \oplus P_1 = \Delta_{\mathrm{out}}$
- With prob. $p$, $S_0 \oplus S_1 = \Delta_{\mathrm{out}}$
- Then ($C_1 \,\|\, C_0$, $T$) is a valid ciphertext-tag pair with nonce $N$!

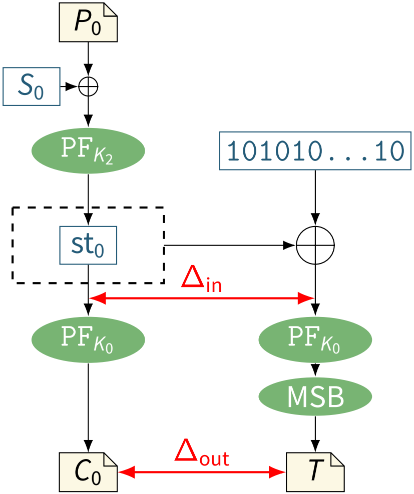
# Forgery Attacks for `FlexAEAD` – Example: Ciphertext Swap




- Query $N$ and $P_0 \oplus P_1 = \Delta_{\text{out}}$
- With prob. $p$, $S_0 \oplus S_1 = \Delta_{\text{out}}$
- Then $(C_1 \| C_0, T)$ is a valid ciphertext-tag pair with nonce $N$!

# Forgery Attacks for `FlexAE` – Example: Zero-Query Forgery




- Original `FlexAE` is simpler ($\mathtt{PF}_K^2$, not $\mathtt{PF}_K^3$)
- Forgeries with 0 encryption queries:
  1. Let $\Delta_{\mathrm{in}} = \mathtt{10101010\,10101010}$
     $\Delta_{\mathrm{out}} = \mathtt{01000000\,1f000000}$
  2. Pick any $N$ and $C_0$
  3. Set $T = C_0 \oplus \Delta_{\mathrm{out}}$
- Success probability $\Delta_{\mathrm{in}} \to \Delta_{\mathrm{out}}$ is $\geq 2^{-54}$ for `FlexAE-64-128`

# Discussion and Conclusion

# Further Comments

- Experimental verification suggests that the success probability is even higher
- The designers were aware of high-probability characteristics for $\mathtt{PF}$, but (incorrectly) argued that only $\mathtt{PF} \circ \mathtt{PF} \circ \mathtt{PF}$ is relevant
- This could be fixed with (much) more rounds for $\mathtt{PF}$ or a better diffusion layer
- The mode has some other bugs that lead to trivial attacks, but are easy to fix (domain separation, zero-length input, padding [Mèg19], long messages, …)

# Further Comments

- Experimental verification suggests that the success probability is even higher
- The designers were aware of high-probability characteristics for $\mathtt{PF}$, but (incorrectly) argued that only $\mathtt{PF} \circ \mathtt{PF} \circ \mathtt{PF}$ is relevant
- This could be fixed with (much) more rounds for $\mathtt{PF}$ or a better diffusion layer
- The mode has some other bugs that lead to trivial attacks, but are easy to fix (domain separation, zero-length input, padding [Mèg19], long messages, …)

# Further Comments

- Experimental verification suggests that the success probability is even higher
- The designers were aware of high-probability characteristics for $\texttt{PF}$, but (incorrectly) argued that only $\texttt{PF} \circ \texttt{PF} \circ \texttt{PF}$ is relevant
- This could be fixed with (much) more rounds for $\texttt{PF}$ or a better diffusion layer
- The mode has some other bugs that lead to trivial attacks, but are easy to fix (domain separation, zero-length input, padding [Mèg19], long messages, …)

# Further Comments

- Experimental verification suggests that the success probability is even higher
- The designers were aware of high-probability characteristics for `PF`, but (incorrectly) argued that only $\mathtt{PF} \circ \mathtt{PF} \circ \mathtt{PF}$ is relevant
- This could be fixed with (much) more rounds for `PF` or a better diffusion layer
- The mode has some other bugs that lead to trivial attacks, but are easy to fix (domain separation, zero-length input, padding [Mèg19], long messages, …)

# Related Work

- Other, independent **cryptanalysis**:
  - Truncated differential and Yoyo distinguisher on $\mathtt{PF}_K$ [RSP19a; RSP19b]
  - Simple padding domain separation attack for associated data [Még19]
- **Tweaks** proposed by the designers [NX19c; NX19b]:
  - Changing the increment in `INC32` from `0x00000001` to `0x11111111`
  - Reducing data limits to at most $2^{32}$ blocks per encryption
  - Modifying the associated data padding and domain separation
  - Strengthening the linear layer

# Conclusion

- We show forgery attacks against the NIST LWC Round-1 candidate `FlexAEAD` and its predecessor `FlexAE`
- Some of the attacks have practical complexity (ymmv)
- We exploit high-probability clusters of differential characteristics for $\mathtt{PF}_K$ instead of $\mathtt{PF}_K \circ \mathtt{PF}_K \circ \mathtt{PF}_K$ as analyzed by the designers
- The designers proposed many fixes which may mitigate most attacks
- `FlexAEAD` did not make it to Round 2 of NIST LWC

# Questions

# Bibliography I


[BS90] Eli Biham and Adi Shamir. **Differential Cryptanalysis of DES-like Cryptosystems.** Advances in Cryptology – CRYPTO 1990. Vol. 537. LNCS. Springer, 1990, pp. 2–21. DOI: 10.1007/3-540-38424-3_1.

[Mèg19] Alexandre Mège. **OFFICIAL COMMENT: FlexAEAD.** Posting on the NIST LWC mailing list. June 3, 2019. URL: https://groups.google.com/a/list.nist.gov/d/msg/lwc-forum/DPQVEJ5oBeU/YXW0QjfjBQAJ.

[NX17] Eduardo Marsola do Nascimento and José Antônio Moreira Xexéo. **A flexible authenticated lightweight cipher using Even-Mansour construction.** IEEE International Conference on Communications – ICC 2017. IEEE, 2017, pp. 1–6. URL: https://doi.org/10.1109/ICC.2017.7996734.

# Bibliography II


[NX19a] Eduardo Marsola do Nascimento and José Antônio Moreira Xexéo. **FlexAEAD.** Submission to Round 1 of the NIST Lightweight Cryptography Standardization process. 2019. URL: https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/spec-doc/FlexAEAD-spec.pdf.

[NX19b] Eduardo Marsola do Nascimento and José Antônio Moreira Xexéo. **FlexAEAD v1.1 – A Lightweight AEAD Cipher with Integrated Authentication.** Journal of Information Security and Cryptography (Enigma) 6.1 (2019), pp. 15–24. DOI: 10.17648/jisc.v6i1.74.

[NX19c] Eduardo Marsola do Nascimento and José Antônio Moreira Xexéo. **OFFICIAL COMMENT: FlexAEAD.** Posting on the NIST LWC mailing list. 2019. URL: https://csrc.nist.gov/CSRC/media/Projects/Lightweight-Cryptography/documents/round-1/official-comments/FlexAEAD-official-comment.pdf.

# Bibliography III


[RSP19a] Mostafizar Rahman, Dhiman Saha, and Goutam Paul. **Attacks Against FlexAEAD**. Posting on the NIST LWC mailing list. May 22, 2019. URL: https://groups.google.com/a/list.nist.gov/d/msg/lwc-forum/VLWtGnJStew/X3Fxexg1AQAJ.

[RSP19b] Mostafizar Rahman, Dhiman Saha, and Goutam Paul. **Interated Truncated Differential for Internal Keyed Permutation of FlexAEAD**. IACR Cryptology ePrint Archive, Report 2019/539. 2019. URL: https://eprint.iacr.org/2019/539.