Cryptanalysis of NORX v2.0

Colin Chaigneau[1] **Thomas Fuhr**[2] Henri Gilbert[2]

Jérémy Jean[2] Jean-René Reinhard[2]

[1]Université de Versailles, France

[2]ANSSI, France

FSE 2017 - March 7, 2017

A CAESAR Candidate

- **CAESAR competition**: Authenticated Encryption with Associated Data (AEAD)
- **Timeline**
  - March 2014: 56 initial submissions
  - July 2015: 28 candidates selected for 2nd round
  - August 2016: 15 candidates selected for 3rd round
- **The NORX authenticated encryption scheme** (Aumasson, Jovanovic, Neves)
  - Initial submission: NORX v1 (selected for Round 2)
  - August 2015: NORX v2.0 (selected for Round 3)
  - September 2016: NORX v3.0

Our results

- Ciphertext-only forgery attack on full NORX v2.0
- Trivial known-plaintext key recovery once a forgery is achieved
- CAESAR NORX handles only byte strings

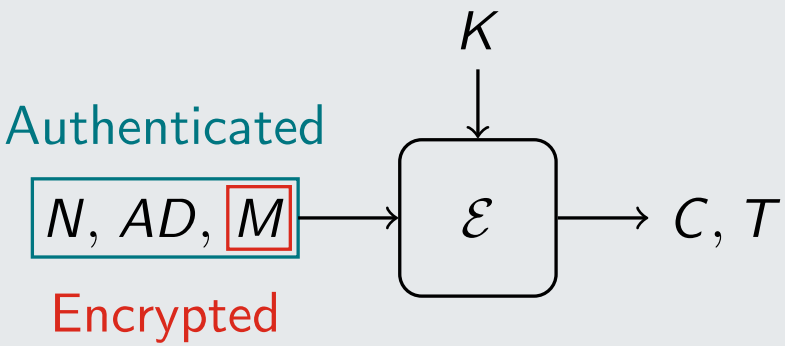
Version	Key size	Tag size	Data	Time
NORX v2.0	128	128	2^{66}	2^{66}
NORX v2.0 CAESAR	128	128	2^{72}	2^{72}
NORX v2.0	256	256	2^{130}	2^{130}
NORX v2.0 CAESAR	256	256	2^{136}	2^{136}

- Related work
  - Privacy and integrity proofs of the mode [JLM14]
  - Analyses of the permutation [AJN14], [AJN15], [DMM15], [BUV17]
  - Attacks on reduced versions [BHJMS16]

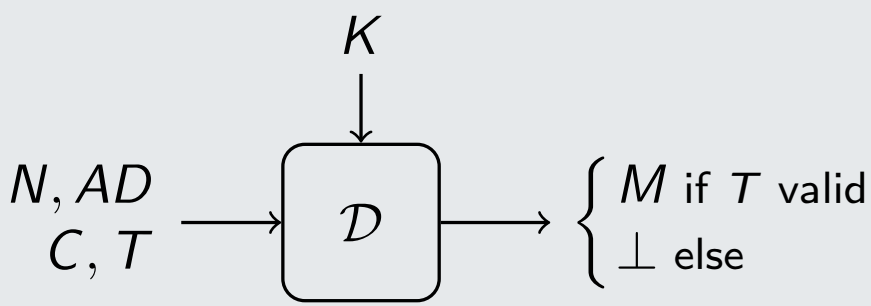
1. Description of NORX v2.0

AEAD framework

Encryption



Decryption



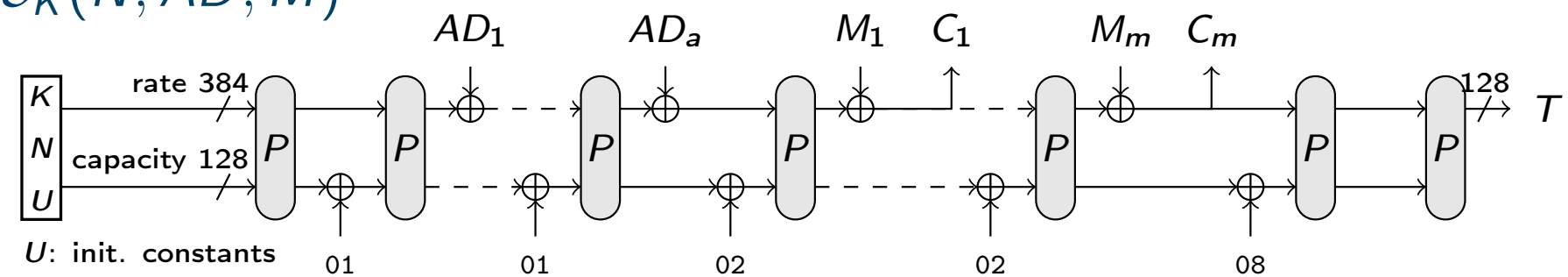
Notations

- M: Plaintext
- AD: Associated data
- N: Nonce
- K: AEAD Key
- C: Ciphertext
- T: Authentication Tag

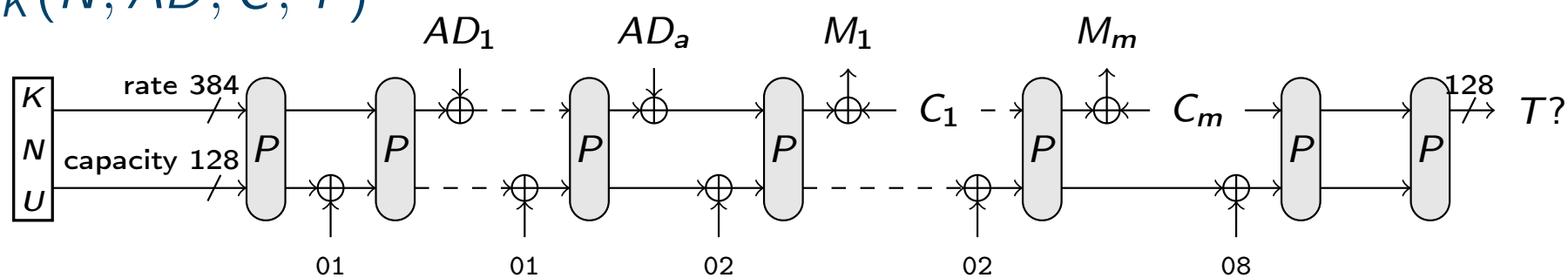
NORX mode of operation

- MonkeyDuplex mode **[BDPV12]**
- This talk: focus on the 128-bit key and 128-bit tag version
- Out of scope: parallel mode, authenticated trailer, 256-bit keys

$\mathcal{E}_K(N, AD, M)$



$\mathcal{D}_K(N, AD, C, T)$



The permutation P

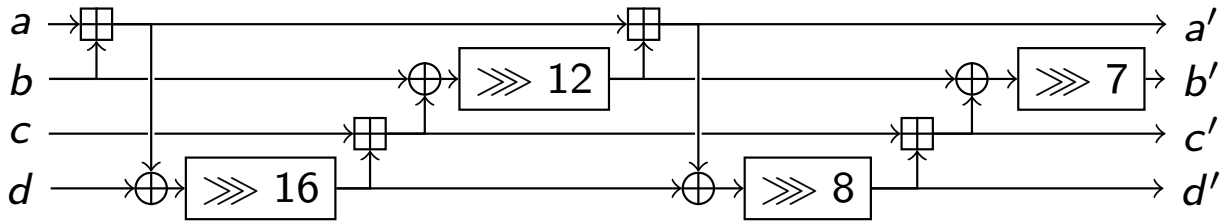
- Inspired by stream cipher ChaCha [B08]
- Operates on a 512-bit state S
- State represented as a 4×4 matrix of 32-bit words

$$S = \begin{pmatrix} s_0 & s_1 & s_2 & s_3 \\ s_4 & s_5 & s_6 & s_7 \\ s_8 & s_9 & s_{10} & s_{11} \\ s_{12} & s_{13} & s_{14} & s_{15} \end{pmatrix} \begin{matrix} \} \\ \} \end{matrix} \begin{matrix} \text{Outer part (rate)} \\ \text{Inner part (capacity)} \end{matrix}$$

- P relies on a 128-bit permutation G

The permutation P

- G: 4-branch generalised Feistel



$$a', b', c', d' = G(a, b, c, d)$$
$$x \boxplus y = (x \oplus y) \oplus (x \wedge y) \ll 1$$

$$G_{\text{col}} = \begin{cases} G(s_0, s_4, s_8, s_{12}) \\ G(s_1, s_5, s_9, s_{13}) \\ G(s_2, s_6, s_{10}, s_{14}) \\ G(s_3, s_7, s_{11}, s_{15}) \end{cases}$$

$$G_{\text{diag}} = \begin{cases} G(s_0, s_5, s_{10}, s_{15}) \\ G(s_1, s_6, s_{11}, s_{12}) \\ G(s_2, s_7, s_8, s_{13}) \\ G(s_3, s_4, s_9, s_{14}) \end{cases}$$

- P: 4 rounds of G_{col} then G_{diag}
- Words of row i = i-th input of G

2. Analysis of P

Properties of P

- Preservation of symmetries **[AJN15]**

$$\begin{pmatrix} a & a & a & a \\ b & b & b & b \\ c & c & c & c \\ d & d & d & d \end{pmatrix} \xrightarrow{P} \begin{pmatrix} a' & a' & a' & a' \\ b' & b' & b' & b' \\ c' & c' & c' & c' \\ d' & d' & d' & d' \end{pmatrix}$$

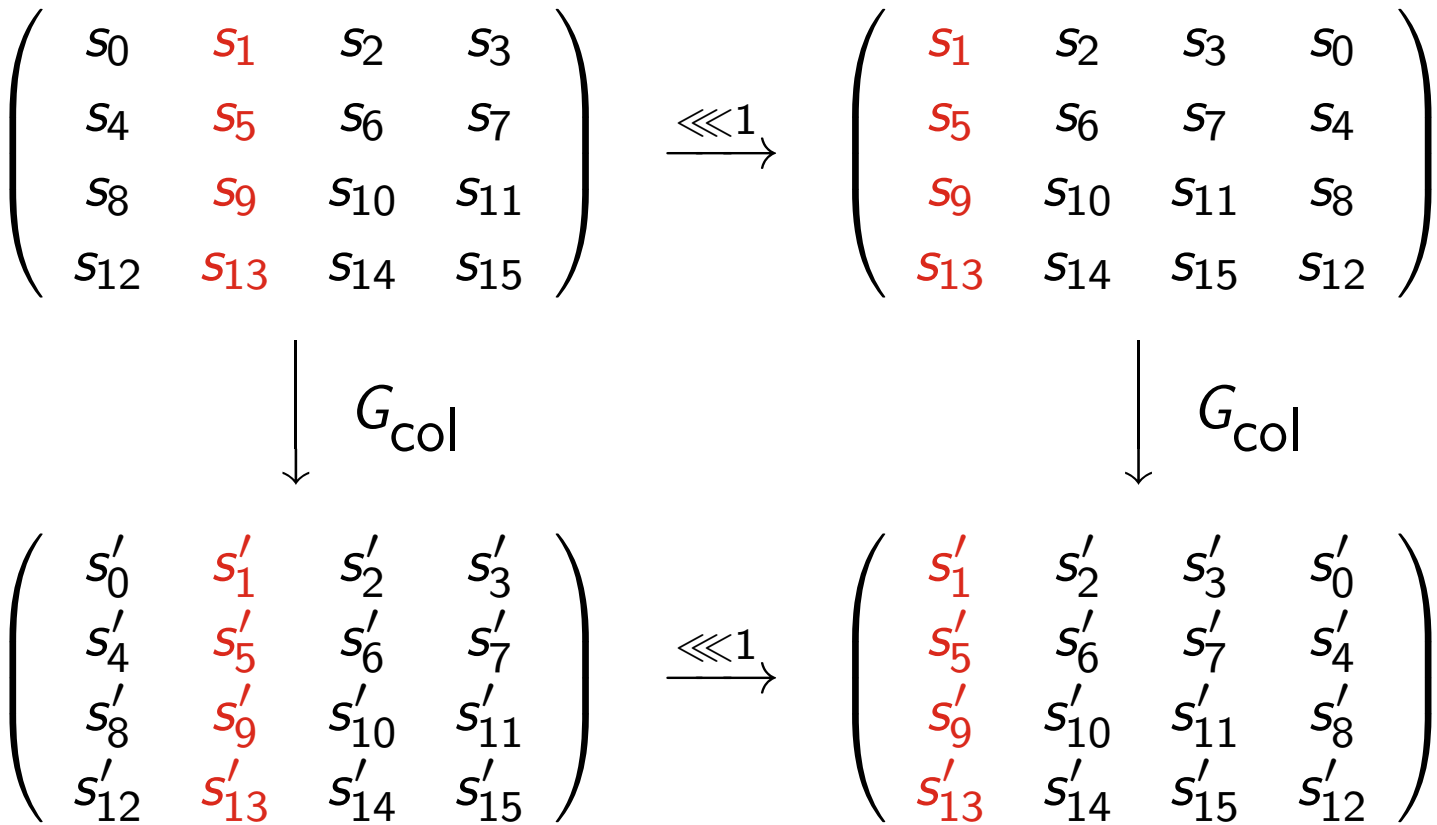
- More generally, P commutes with rotations on columns

$$\begin{pmatrix} s_0 & s_1 & s_2 & s_3 \\ s_4 & s_5 & s_6 & s_7 \\ s_8 & s_9 & s_{10} & s_{11} \\ s_{12} & s_{13} & s_{14} & s_{15} \end{pmatrix} \xrightarrow{\lll 1} \begin{pmatrix} s_1 & s_2 & s_3 & s_0 \\ s_5 & s_6 & s_7 & s_4 \\ s_9 & s_{10} & s_{11} & s_8 \\ s_{13} & s_{14} & s_{15} & s_{12} \end{pmatrix}$$

State S | State $S \lll 1$

$$\forall i \in \{1, 2, 3\}, P(S \lll i) = P(S) \lll i$$

Sketch of proof



Rotation commutes with G_{col} layers...

Sketch of proof

$$\begin{pmatrix} s_0 & s_1 & s_2 & s_3 \\ s_4 & s_5 & s_6 & s_7 \\ s_8 & s_9 & s_{10} & s_{11} \\ s_{12} & s_{13} & s_{14} & s_{15} \end{pmatrix} \xrightarrow{\lll 1} \begin{pmatrix} s_1 & s_2 & s_3 & s_0 \\ s_5 & s_6 & s_7 & s_4 \\ s_9 & s_{10} & s_{11} & s_8 \\ s_{13} & s_{14} & s_{15} & s_{12} \end{pmatrix}$$

$$\downarrow G_{\text{diag}} \qquad\qquad \downarrow G_{\text{diag}}$$

$$\begin{pmatrix} s'_0 & s'_1 & s'_2 & s'_3 \\ s'_4 & s'_5 & s'_6 & s'_7 \\ s'_8 & s'_9 & s'_{10} & s'_{11} \\ s'_{12} & s'_{13} & s'_{14} & s'_{15} \end{pmatrix} \xrightarrow{\lll 1} \begin{pmatrix} s'_1 & s'_2 & s'_3 & s'_0 \\ s'_5 & s'_6 & s'_7 & s'_4 \\ s'_9 & s'_{10} & s'_{11} & s'_8 \\ s'_{13} & s'_{14} & s'_{15} & s'_{12} \end{pmatrix}$$

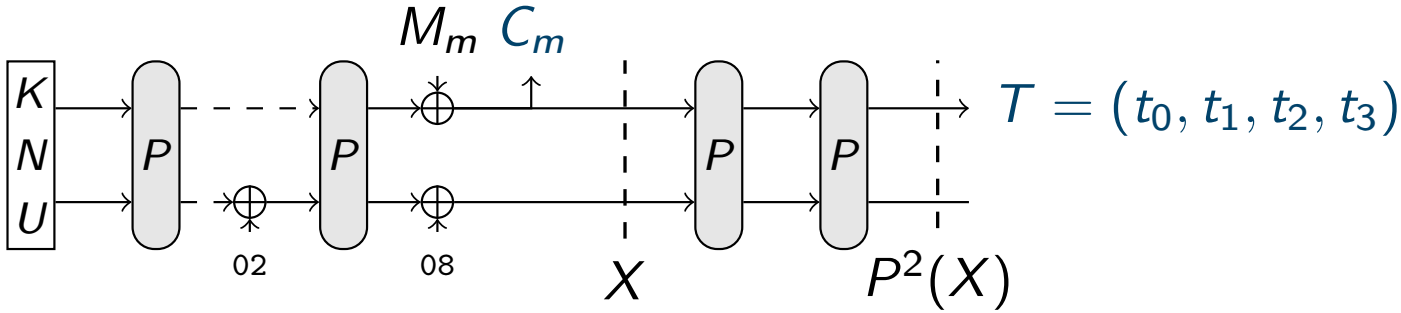
... and with G_{diag} layers (and therefore with P)

3. Forgery attack on NORX v2.0

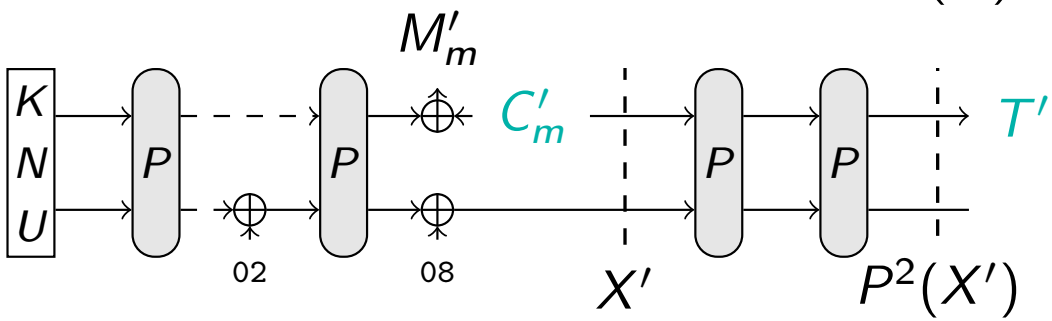
Forgeries on NORX without padding (1/2)

- Idea: modify the last block of a known ciphertext
- $(N, AD, C_1, \ldots, C_m) \rightarrow (N, AD, C_1, \ldots, C'_m)$

(N, AD, C, T):
Known Ciphertext



(N, AD, C', T'):
Forgery Attempt



If $X' = X \lll 2$ then $\begin{cases} P^2(X') = P^2(X \lll 2) \\ \qquad\quad = P^2(X) \lll 2 \end{cases}$ thus $T' = T \lll 2$

Forgeries on NORX without padding (2/2)

- Set $T' = T \lll 2$, choice of C' ?

State X during encryption

$$\begin{pmatrix} c_0 & c_1 & c_2 & c_3 \\ c_4 & c_5 & c_6 & c_7 \\ c_8 & c_9 & c_{10} & c_{11} \\ s_{12} & s_{13} & s_{14} & s_{15} \end{pmatrix} \xrightarrow{\lll 2} \begin{pmatrix} & & & \\ & & & \\ & & & \\ s_{12} & s_{13} & s_{14} & s_{15} \end{pmatrix}$$

State X' during decryption

Known, Unknown

Chosen, Fixed

- Conditions:

Forgeries on NORX without padding (2/2)

- Set $T' = T \lll 2$, choice of C' ?

State X during encryption

$$\begin{pmatrix} \boxed{c_0} & c_1 & c_2 & c_3 \\ \boxed{c_4} & c_5 & c_6 & c_7 \\ \boxed{c_8} & c_9 & c_{10} & c_{11} \\ \boxed{s_{12}} & s_{13} & s_{14} & s_{15} \end{pmatrix} \xrightarrow{\lll 2} \begin{pmatrix} & & \boxed{c_0} & \\ & & \boxed{c_4} & \\ & & \boxed{c_8} & \\ s_{12} & s_{13} & \boxed{s_{14}} & s_{15} \end{pmatrix}$$

State X' during decryption

Known, Unknown

Chosen, Fixed

- Conditions: $s_{12} = s_{14}$

Forgeries on NORX without padding (2/2)

- Set $T' = T \lll 2$, choice of C' ?

State X during encryption

$$\begin{pmatrix} c_0 & \boxed{c_1} & c_2 & c_3 \\ c_4 & c_5 & c_6 & c_7 \\ c_8 & c_9 & c_{10} & c_{11} \\ s_{12} & s_{13} & s_{14} & s_{15} \end{pmatrix} \xrightarrow{\lll 2} \begin{pmatrix} & & c_0 & \boxed{c_1} \\ & & c_4 & c_5 \\ & & c_8 & c_9 \\ s_{12} & s_{13} & s_{14} & s_{15} \end{pmatrix}$$

State X' during decryption

Known, Unknown

Chosen, Fixed

- Conditions: $s_{12} = s_{14}$, $s_{13} = s_{15}$

Forgeries on NORX without padding (2/2)

- Set $T' = T \lll 2$, choice of C' ?

State X during encryption

$$\begin{pmatrix} c_0 & c_1 & \boxed{c_2} & c_3 \\ c_4 & c_5 & c_6 & c_7 \\ c_8 & c_9 & c_{10} & c_{11} \\ s_{12} & s_{13} & s_{14} & s_{15} \end{pmatrix} \xrightarrow{\lll 2} \begin{pmatrix} \boxed{c_2} & & c_0 & c_1 \\ c_6 & & c_4 & c_5 \\ c_{10} & & c_8 & c_9 \\ s_{12} & s_{13} & s_{14} & s_{15} \end{pmatrix}$$

State X' during decryption

Known, Unknown

Chosen, Fixed

- Conditions: $s_{12} = s_{14}$, $s_{13} = s_{15}$

Forgeries on NORX without padding (2/2)

- Set $T' = T \lll 2$, choice of C' ?

State X during encryption

$$\begin{pmatrix} c_0 & c_1 & c_2 & \boxed{c_3} \\ c_4 & c_5 & c_6 & \boxed{c_7} \\ c_8 & c_9 & c_{10} & \boxed{c_{11}} \\ s_{12} & s_{13} & s_{14} & \boxed{s_{15}} \end{pmatrix} \xrightarrow{\lll 2} \begin{pmatrix} c_2 & \boxed{c_3} & c_0 & c_1 \\ c_6 & \boxed{c_7} & c_4 & c_5 \\ c_{10} & \boxed{c_{11}} & c_8 & c_9 \\ s_{12} & \boxed{s_{13}} & s_{14} & s_{15} \end{pmatrix}$$

State X' during decryption

Known, Unknown

Chosen, Fixed

- Conditions: $s_{12} = s_{14}$, $s_{13} = s_{15}$
- Probability 2^{-64} (for each forgery attempt)

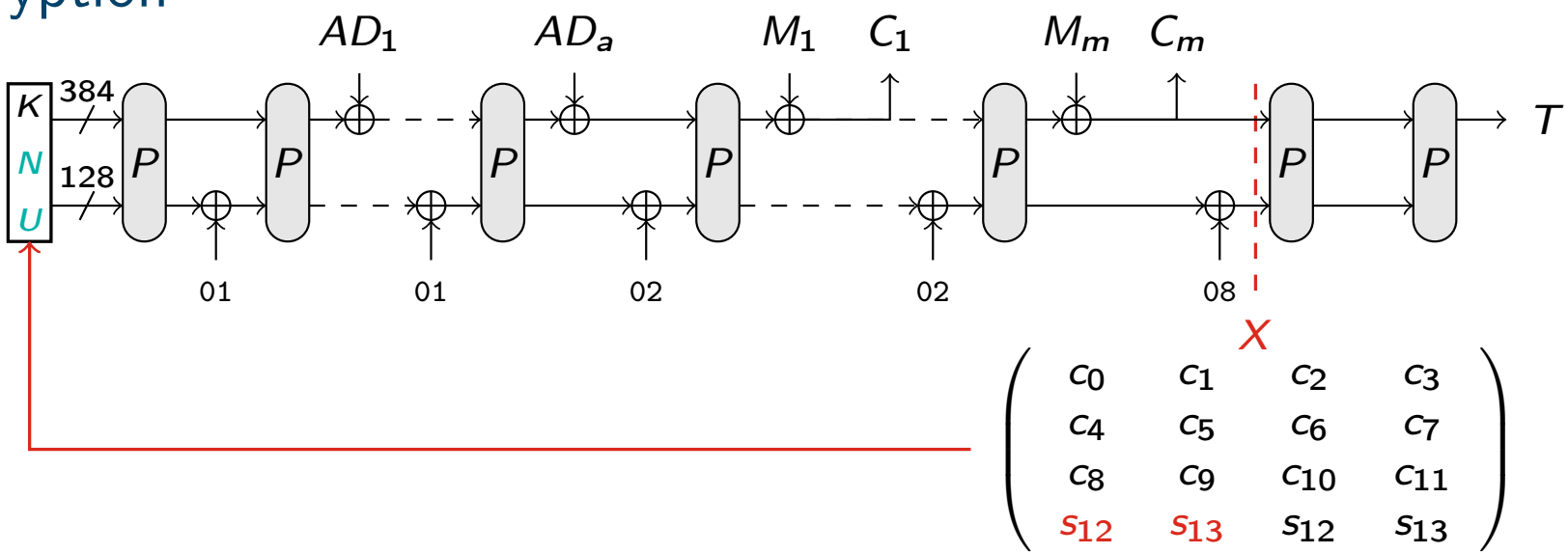
Forgeries on full NORX v2.0 with padding

- Encryption with padding
  - Padding: $M_{\text{pad}} = M||10^*1$
  - Ciphertext: only $|C| = |M|$ bits of the state returned
- Impact on the forgery attack
  - ℓ more conditions for $\ell \leq 64$ padding bits
  - General case: $\Pr[\text{forgery}] = 2^{-64-\ell}$ for ℓ padding bits
  - Best case: 2 padding bits $\Rightarrow \Pr[\text{forgery}] = 2^{-66}$
  - CAESAR version: works on byte level $\Rightarrow \Pr[\text{forgery}] = 2^{-72}$
- $\Pr[\text{forgery}] \geq 1/2$ for 2^{66} or 2^{72} forgery attempts
- General case: attack with any number of blocks of M and AD

Extension to a key-recovery attack

- Key recovery: guess s_{12} and s_{13} and compute backwards
  - Check on the initial value of the state (constants and nonce)
  - Requires the knowledge of the plaintext
  - Complexity: 2^{64} encryptions

Encryption



Other versions

- NORX v2.0, 256-bit keys: attacks work with time and data complexity 2^{130}
- NORX v1: capacity $c = 192$, forgery with probability 2^{-128}
- NORX v3.0: extra key additions thwart the attack

Conclusion

Conclusion

- Constant marginal success probability $\Rightarrow$ Rekeying is useless
- Special property of $P \Rightarrow$ No contradiction with the security proof
- Almost practical forgery and key recovery attack on NORX v2.0
  - Version selected for CAESAR round 3
  - Weakening tweak from NORX v1 to NORX v2.0
  - Too high confidence in the security proof without satisfying its hypothesis
- Tweaks decreasing the security margin should be avoided

Thank you for your attention