SILC Is INT-RUP Secure*

Tetsu Iwata†, Kazuhiko Minematsu, Jian Guo,
Sumio Morioka, and Eita Kobayashi

Early Symmetric Crypto (ESC) 2017
January 16–20, 2017, Canach, Luxembourg

*Supported by JSPS KAKENHI, Grant-in-Aid for Scientific Research (B), Grant Number 26280045
†Currently visiting Nanyang Technological University, Singapore

Overview

- We show that SILC is provably INT-RUP secure against nonce-reusing adversaries up to the birthday bound
- This talk will present technical details of the security proof

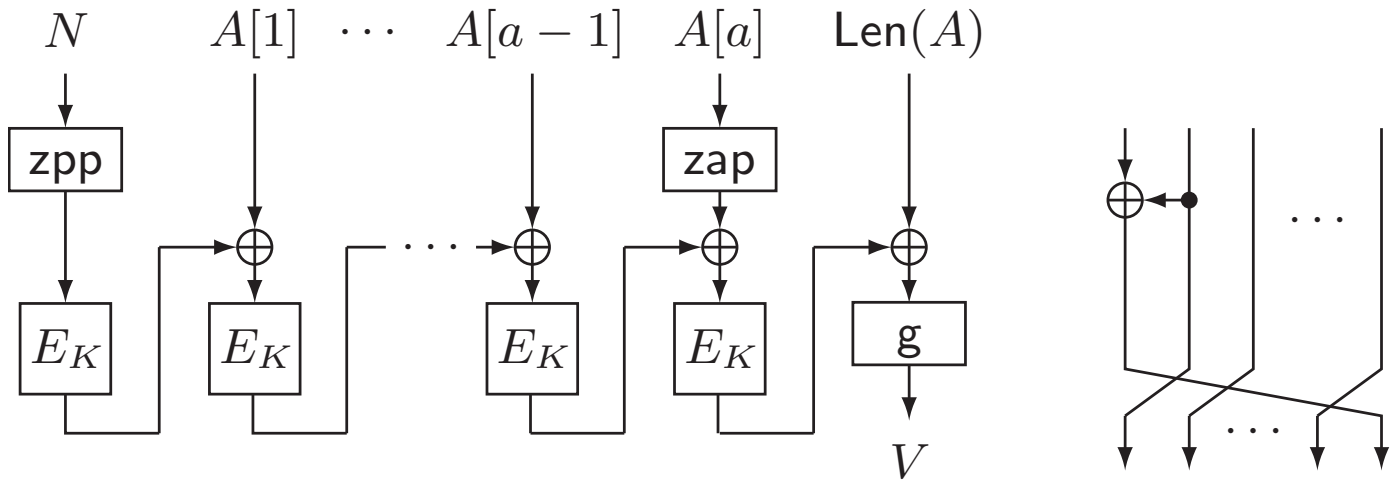
SILC

- Authenticated Encryption with Associated Data (AEAD)
- SImple Lightweight CFB, pronounced as “silk”
- designed by Iwata, Minematsu, Guo, Morioka, and Kobayashi, first presented at DIAC 2014
- CAESAR 3rd round candidate
  - designed for lightweight applications, resource constrained hardware environments
  - small implementation overhead beyond the blockcipher
  - improves CCM (NIST), EAX (ISO/IEC), and EAX-prime (ANSI)

SILC

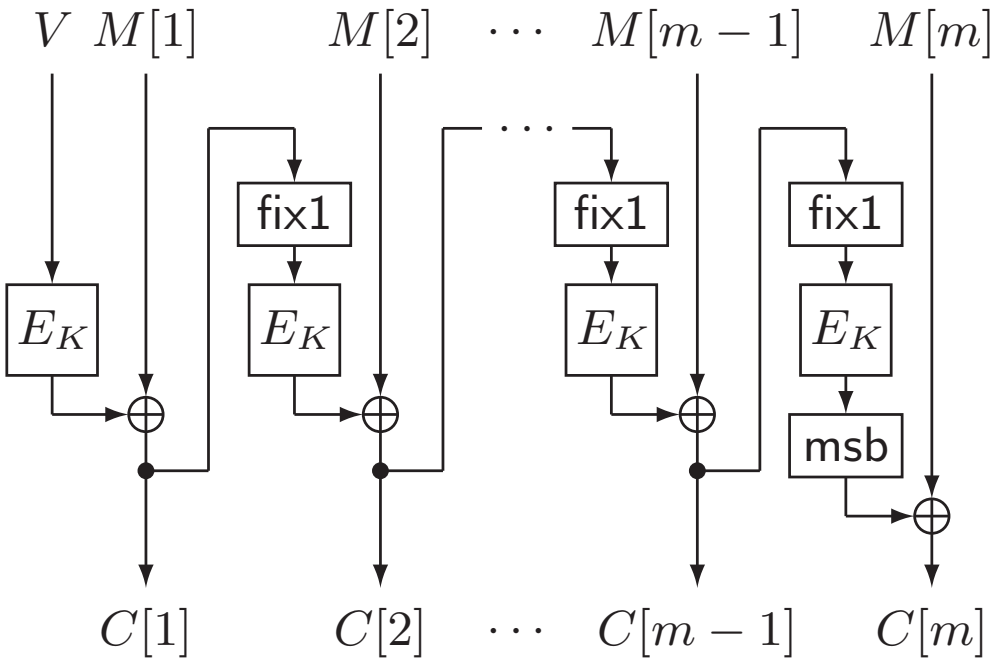
- Parameters of SILC
  - E_K: a blockcipher with an n-bit block
  - ℓ_N: a nonce length in bits, $1 \leq \ell_N \leq n - 1$ (fixed)
  - τ: a tag length in bits, $1 \leq \tau \leq n$ (fixed)
- written as SILC$[E, \ell_N, \tau]$ or simply SILC$[E]$
- Input/Output
  - a blockcipher key K
  - a nonce N
  - associated data A
  - a plaintext M
  - a ciphertext C
  - a tag T
- SILC$[E] =$ (SILC-$\mathcal{E}_K$, SILC-$\mathcal{D}_K$, SILC-$\mathcal{V}_K$)
  - $(N, A, M) \rightarrow$ SILC-$\mathcal{E}_K \rightarrow (C, T)$
  - $(N, A, C, T) \rightarrow$ SILC-$\mathcal{D}_K \rightarrow M$
  - $(N, A, C, T) \rightarrow$ SILC-$\mathcal{V}_K \rightarrow \top/\bot$

Computing V from N and A



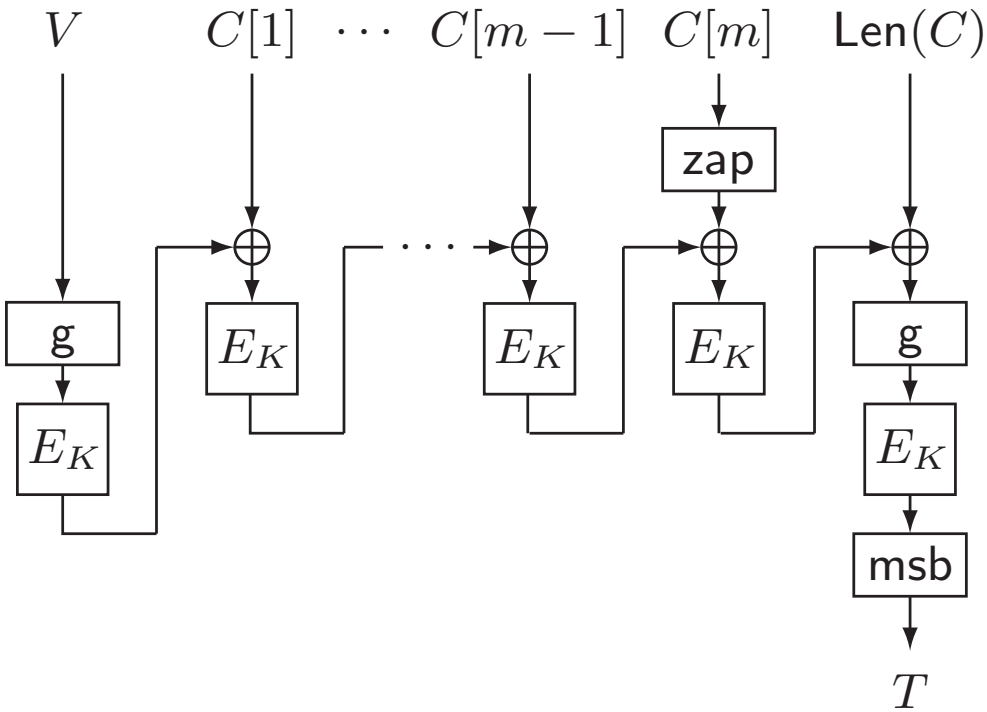
- zpp: zero prepending function, $\mathsf{zpp}(X) = 0 \cdots 0 \,\|\, X$
- zap: zero appending function (possibly none), $\mathsf{zap}(X) = X \,\|\, 0 \cdots 0$
- Len: length encoding function, $\mathsf{Len}(X)$ is the n-bit encoding of the byte length of X
- g: tweak function, the n-bit input is parsed into bytes

Computing C from V and M

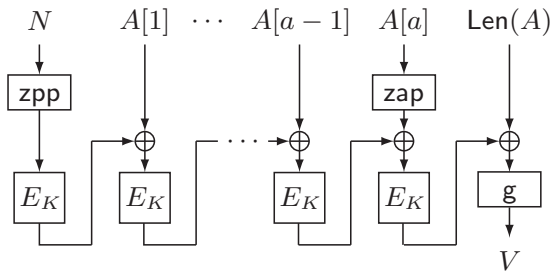


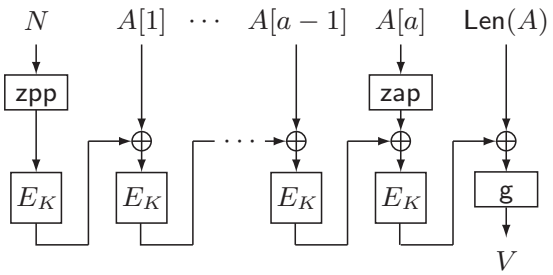
- fix1: bit-fixing function, $\mathsf{fix1}(X) = X \vee 10 \cdots 0$

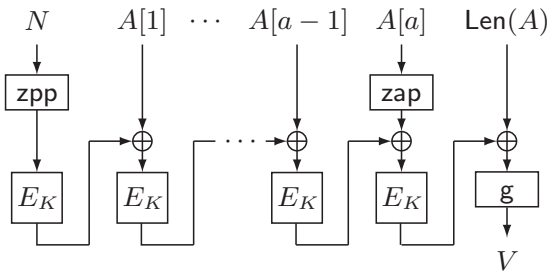
Computing T from V and C

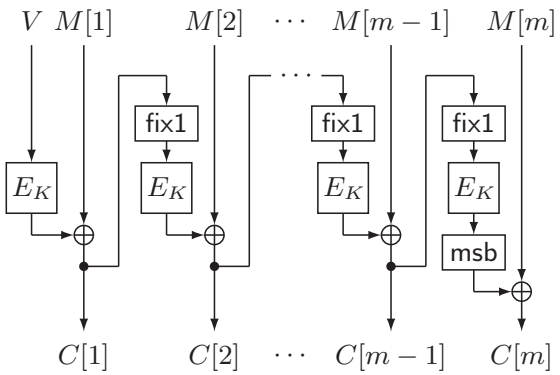


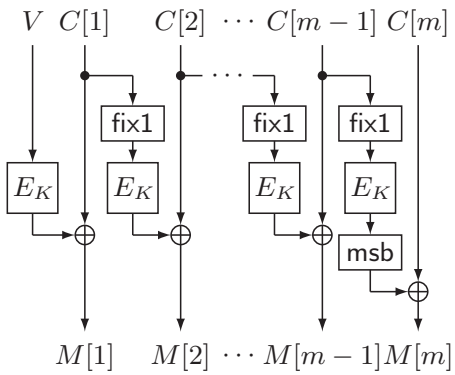
$\mathrm{SILC}[E] = (\mathrm{SILC}\text{-}\mathcal{E}_K, \mathrm{SILC}\text{-}\mathcal{D}_K, \mathrm{SILC}\text{-}\mathcal{V}_K)$

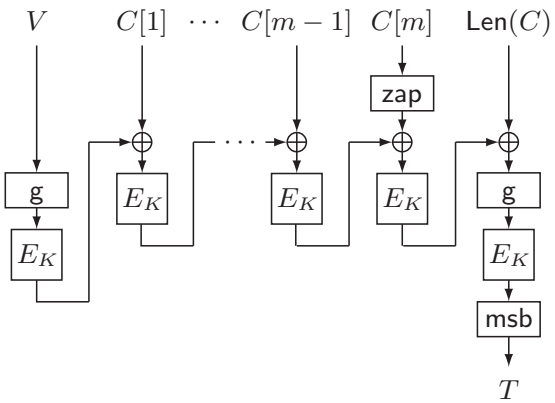


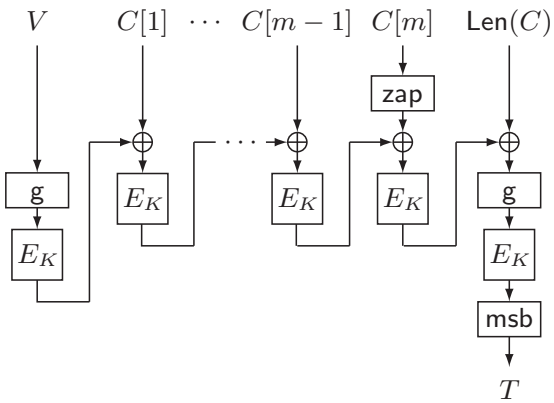












Security of SILC [IMG+14]

- Privacy: Indistinguishability of ciphertexts from random bits against nonce-respecting adversaries in a chosen plaintext attack setting
  - $\mathbf{Adv}^{\mathrm{priv}}_{\mathrm{SILC}[E]}(\mathcal{A}) \stackrel{\mathrm{def}}{=} \Pr\left[\mathcal{A}^{\text{SILC-}\mathcal{E}_K} \Rightarrow 1\right] - \Pr\left[\mathcal{A}^{\$} \Rightarrow 1\right]$
  - $\mathbf{Adv}^{\mathrm{priv}}_{\mathrm{SILC}[\mathrm{Perm}(n)]}(\mathcal{A}) \leq \dfrac{\sigma^2_{\mathrm{priv}}}{2^n}$, where $\sigma_{\mathrm{priv}} = 3q + \sigma_A + 2\sigma_M$
- Authenticity: Unforgeability against nonce-reusing adversaries in a chosen ciphertext attack setting
  - INT-CTXT: integrity of ciphertext
  - $\mathbf{Adv}^{\mathrm{auth}}_{\mathrm{SILC}[E]}(\mathcal{A}) \stackrel{\mathrm{def}}{=} \Pr\left[\mathcal{A}^{\text{SILC-}\mathcal{E}_K,\text{SILC-}\mathcal{V}_K} \text{ forges}\right]$
  - $\mathbf{Adv}^{\mathrm{auth}}_{\mathrm{SILC}[\mathrm{Perm}(n)]}(\mathcal{A}) \leq \dfrac{\sigma^2_{\mathrm{auth}}}{2^n} + \dfrac{q''}{2^\tau}$, where $\sigma_{\mathrm{auth}} = (3q + \sigma_A + 2\sigma_M) + (3q'' + \sigma_{A''} + \sigma_{C''})$

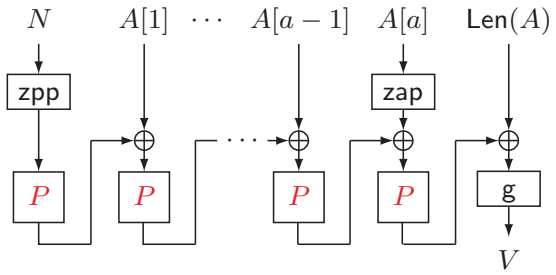
[IMG+14] Iwata, Minematsu, Guo, Morioka, and Kobayashi: SILC: SImple Lightweight CFB. DIAC 2014

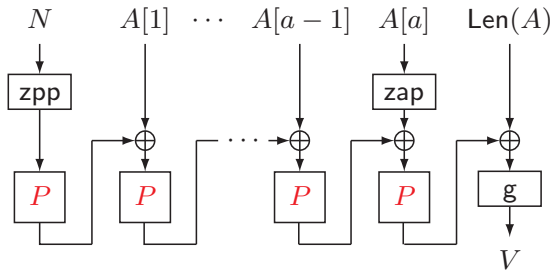
INT-RUP [ABL+14]

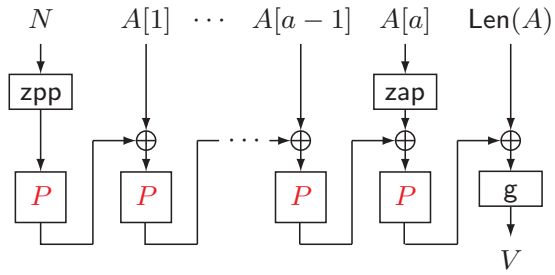
- Authenticity under releasing of unverified plaintext setting
  - INT-RUP
  - there is not enough memory to store the entire plaintext
  - the plaintext is immediately needed for real-time requirements
- $\mathbf{Adv}^{\text{int-rup}}_{\text{SILC}[E]}(\mathcal{A}) \stackrel{\text{def}}{=} \Pr\left[\mathcal{A}^{\text{SILC-}\mathcal{E}_K,\text{SILC-}\mathcal{D}_K,\text{SILC-}\mathcal{V}_K} \text{ forges}\right]$
- We prove that $\mathbf{Adv}^{\text{int-rup}}_{\text{SILC}[\text{Perm}(n)]}(\mathcal{A})$ is small (the standard birthday bound)

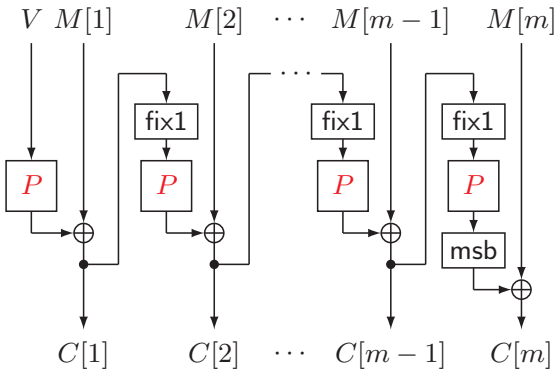
[ABL+14] Andreeva, Bogdanov, Luykx, Mennink, Mouha, and Yasuda: How to Securely Release Unverified Plaintext in Authenticated Encryption. ASIACRYPT 2014, Part I

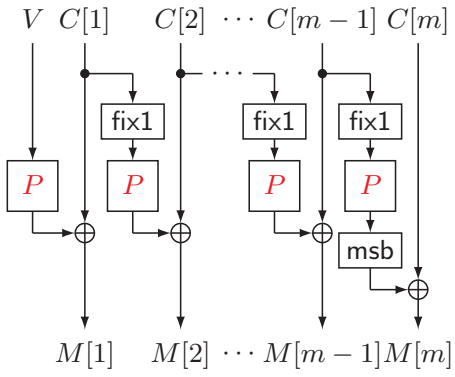
SILC[Perm(n)] with $P \xleftarrow{\$} \mathrm{Perm}(n)$

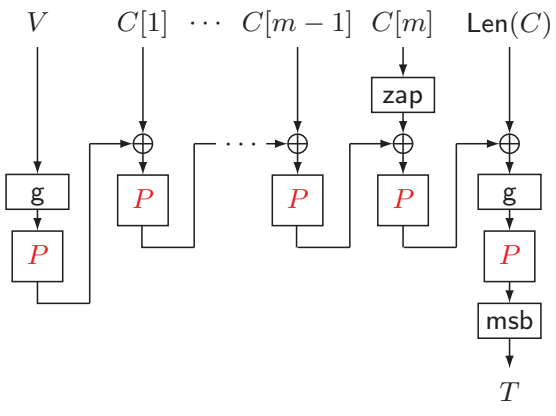


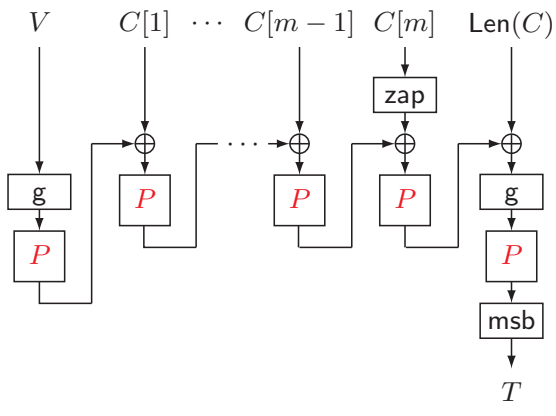




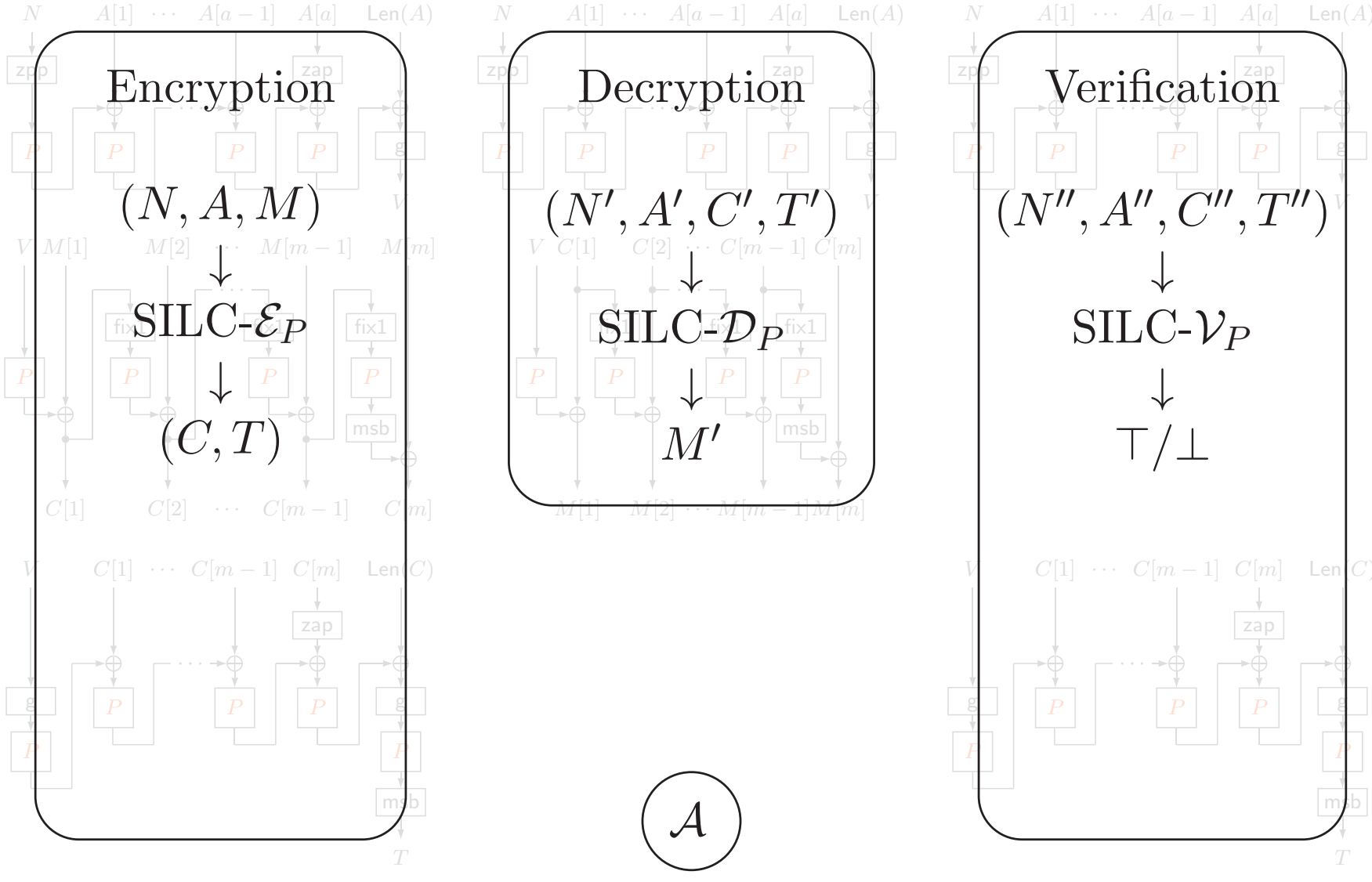




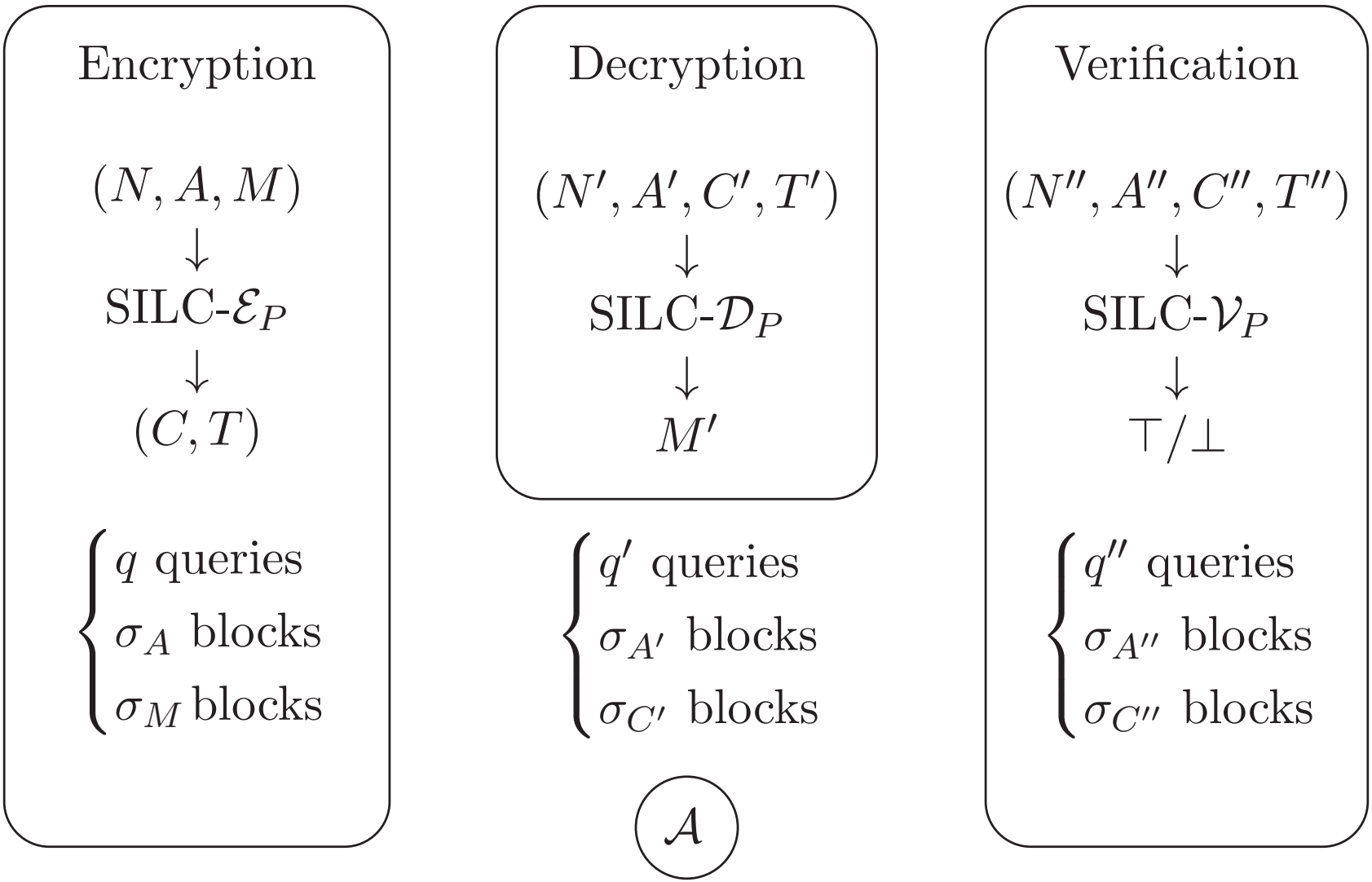




INT-RUP Adversary



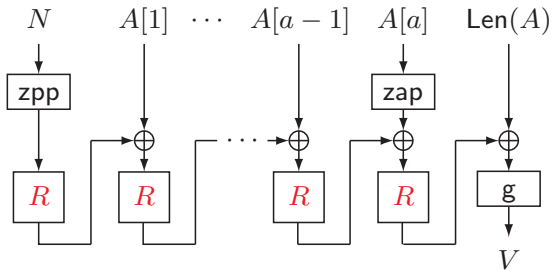
INT-RUP Adversary

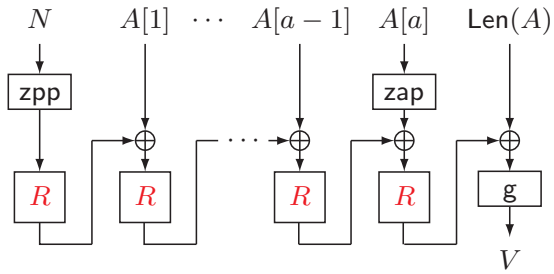


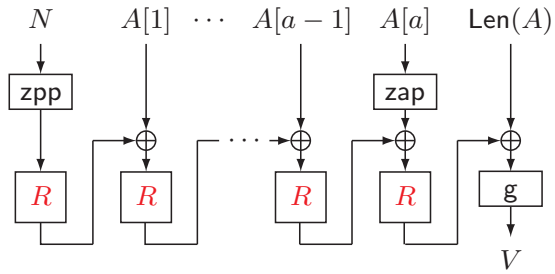
Road Map of the Proof

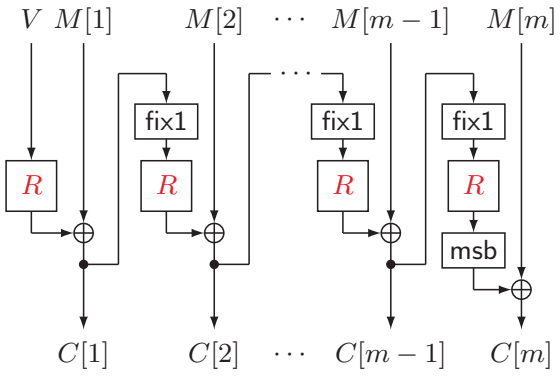
- SILC[Perm(n)]
- SILC[Rand(n)]
- SILC2
- SILC3
- SILC4
- SILC5

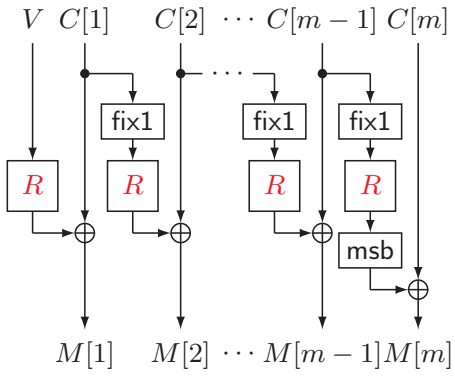
SILC[Rand(n)] with $R \xleftarrow{\$} \mathrm{Rand}(n)$

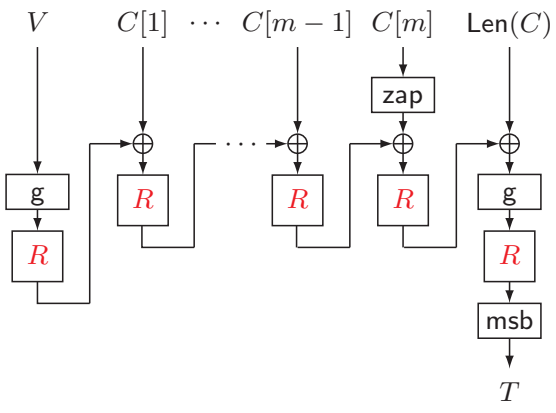


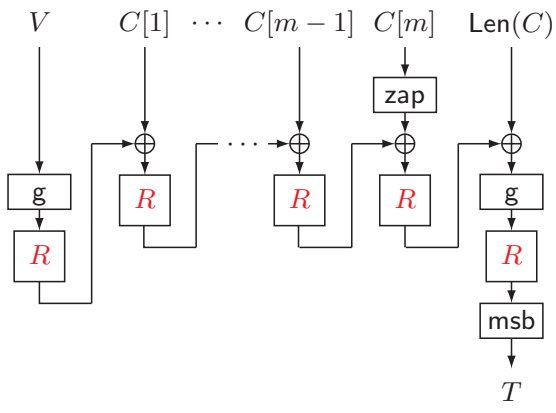










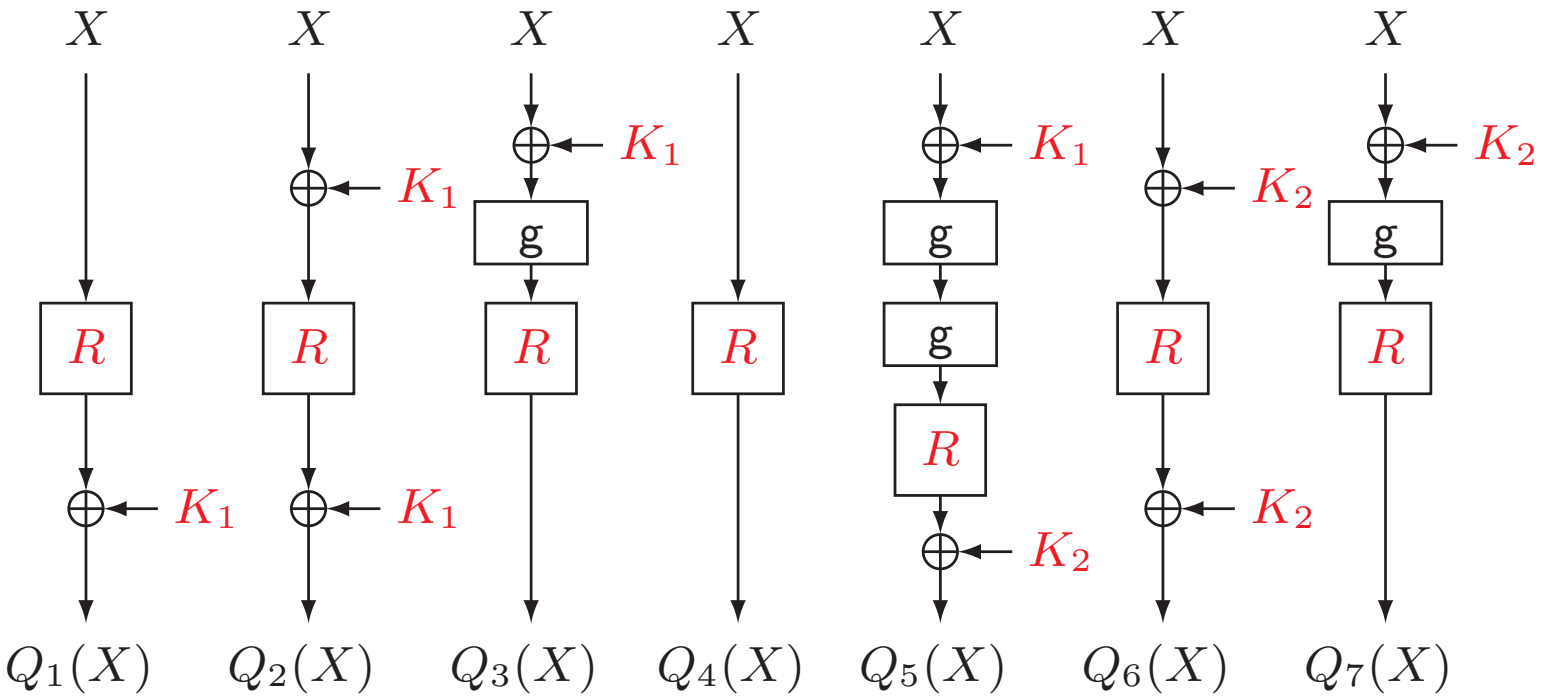


SILC[Perm(n)] **to** SILC[Rand(n)]

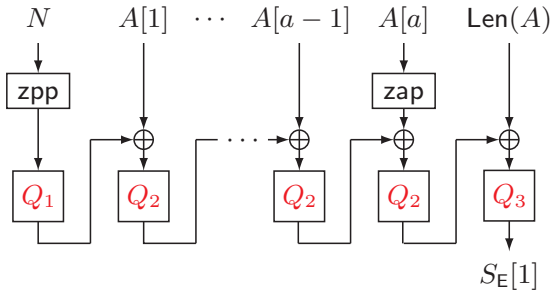
- PRP/PRF switching lemma
- $\mathbf{Adv}^{\text{int-rup}}_{\text{SILC[Perm}(n)]}(\mathcal{A}) \leq \mathbf{Adv}^{\text{int-rup}}_{\text{SILC[Rand}(n)]}(\mathcal{A}) + \dfrac{0.5\sigma^2}{2^n}$
- $\sigma = (3q + \sigma_A + 2\sigma_M) + (q' + \sigma_{A'} + \sigma_{C'}) + (3q'' + \sigma_{A''} + \sigma_{C''})$

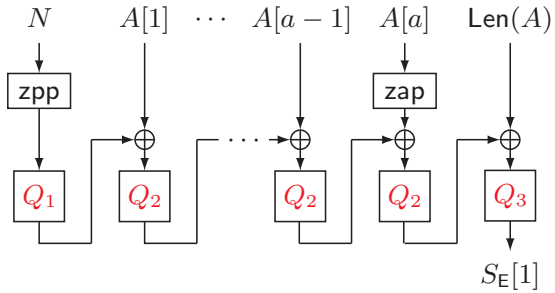
$Q = (Q_1, \ldots, Q_7)$ and SILC2

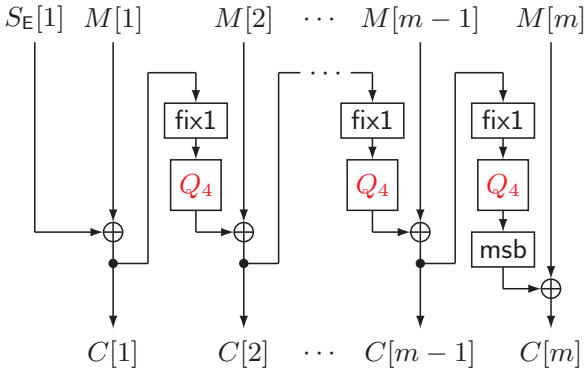
- (R, K_1, K_2), $R \xleftarrow{\$} \mathrm{Rand}(n)$, $K_1 \xleftarrow{\$} \{0,1\}^n$, $K_2 \xleftarrow{\$} \{0,1\}^n$

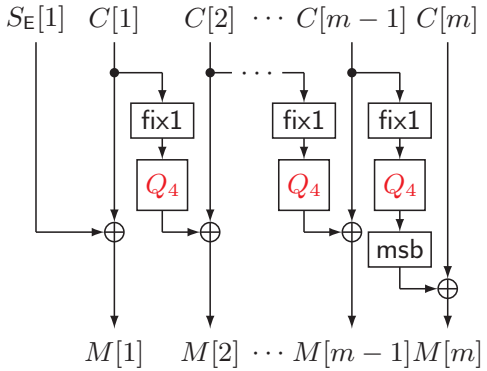


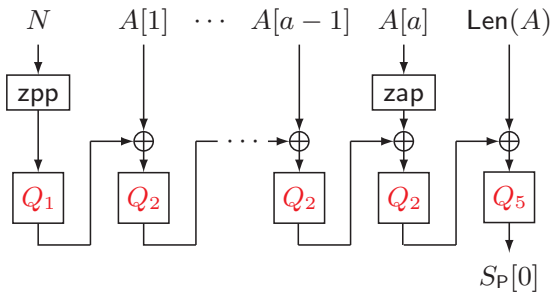
SILC2

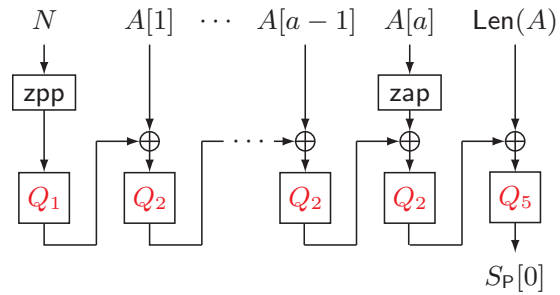

N $A[1]$ $\cdots$ $A[a-1]$ $A[a]$ $\mathsf{Len}(A)$
zpp
Q_1 Q_2 Q_2 Q_2 Q_3
zap
$S_{\mathsf{E}}[1]$

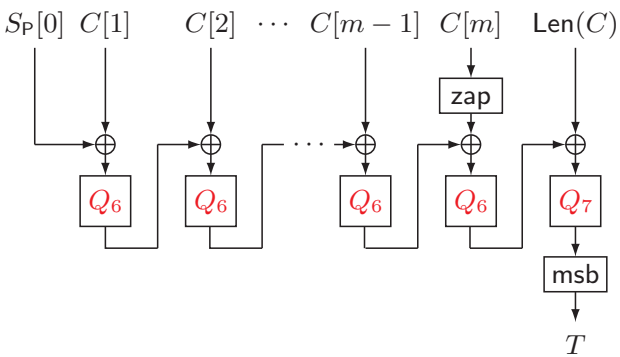

N $A[1]$ $\cdots$ $A[a-1]$ $A[a]$ $\mathsf{Len}(A)$
zpp
Q_1 Q_2 Q_2 Q_2 Q_3
zap
$S_{\mathsf{E}}[1]$

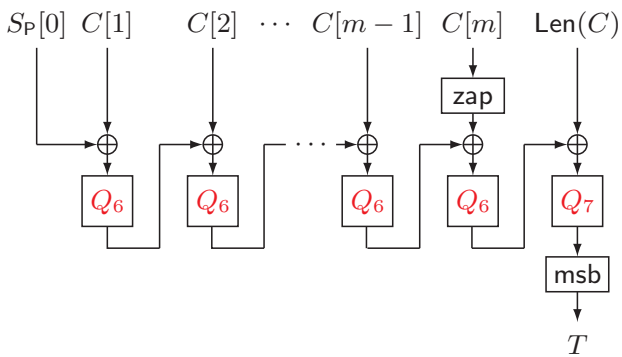

$S_{\mathsf{E}}[1]$ $M[1]$ $M[2]$ $\cdots$ $M[m-1]$ $M[m]$
fix1
Q_4
msb
$C[1]$ $C[2]$ $\cdots$ $C[m-1]$ $C[m]$

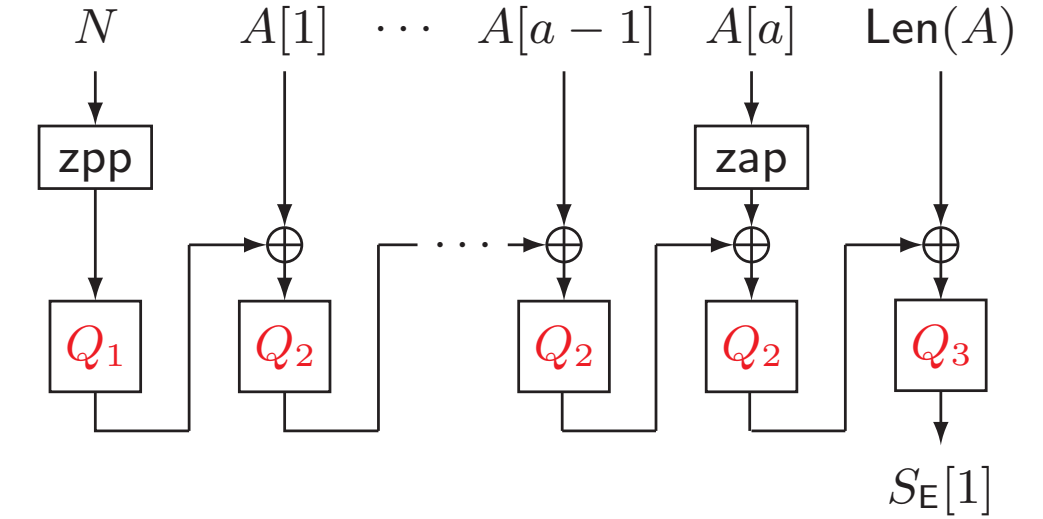

$S_{\mathsf{E}}[1]$ $C[1]$ $C[2]$ $\cdots$ $C[m-1]$ $C[m]$
fix1
Q_4
msb
$M[1]$ $M[2]$ $\cdots$ $M[m-1]$ $M[m]$

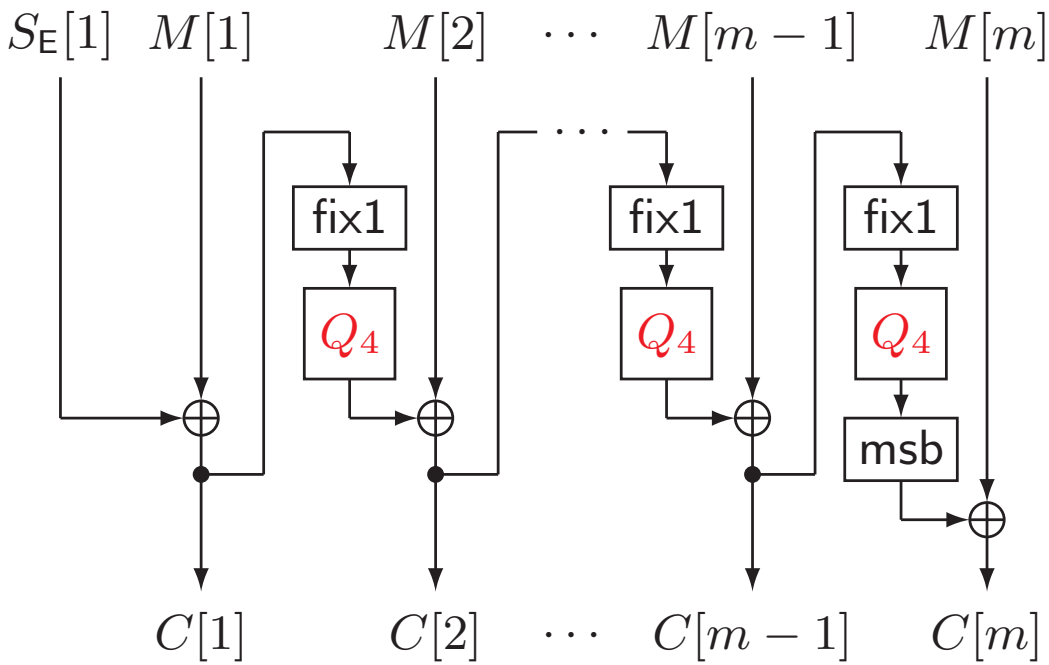

N $A[1]$ $\cdots$ $A[a-1]$ $A[a]$ $\mathsf{Len}(A)$
zpp
Q_1 Q_2 Q_2 Q_2 Q_5
zap
$S_{\mathsf{P}}[0]$

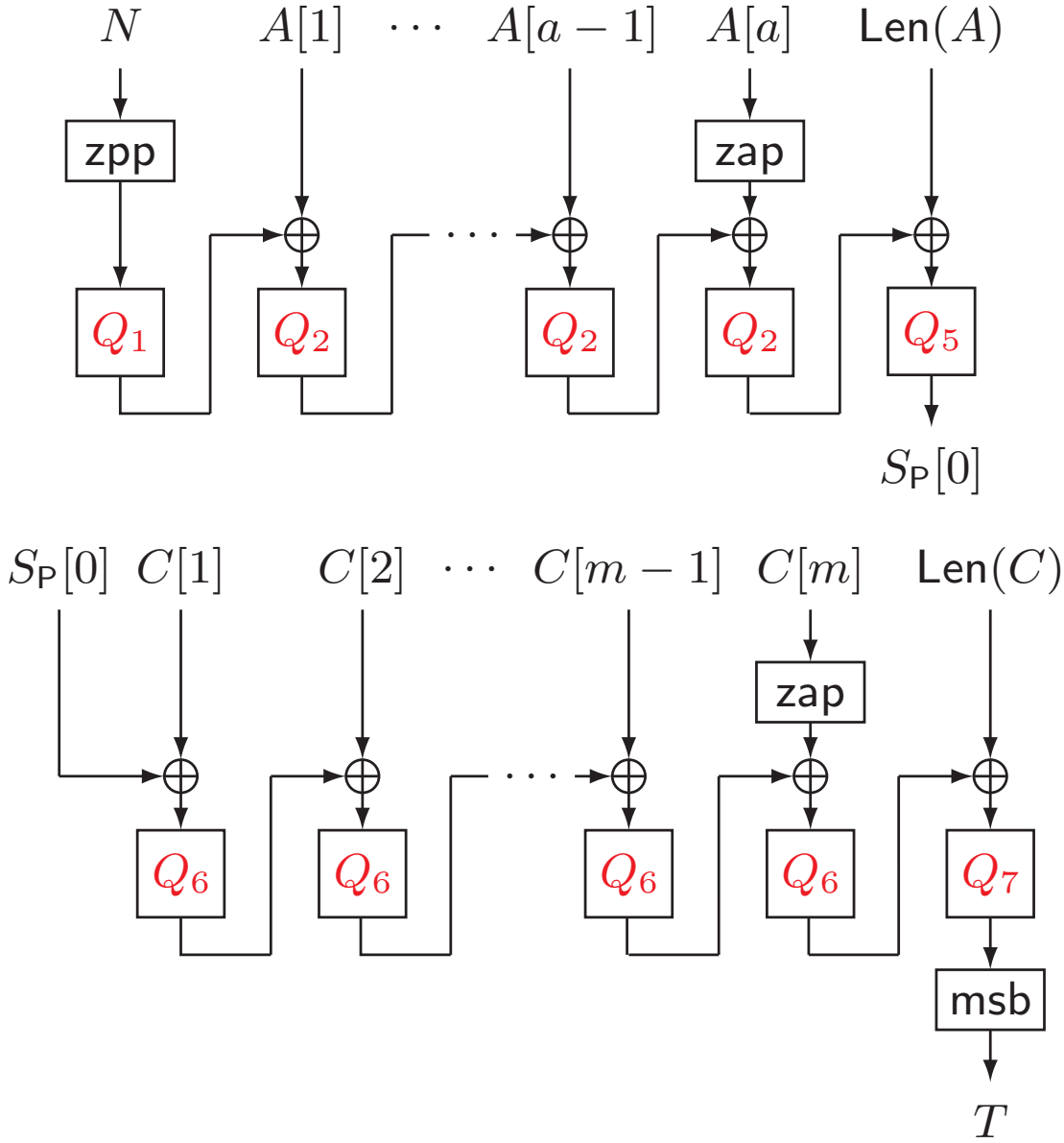

N $A[1]$ $\cdots$ $A[a-1]$ $A[a]$ $\mathsf{Len}(A)$
zpp
Q_1 Q_2 Q_2 Q_2 Q_5
zap
$S_{\mathsf{P}}[0]$


$S_{\mathsf{P}}[0]$ $C[1]$ $C[2]$ $\cdots$ $C[m-1]$ $C[m]$ $\mathsf{Len}(C)$
zap
Q_6 Q_6 Q_6 Q_6 Q_7
msb
T


$S_{\mathsf{P}}[0]$ $C[1]$ $C[2]$ $\cdots$ $C[m-1]$ $C[m]$ $\mathsf{Len}(C)$
zap
Q_6 Q_6 Q_6 Q_6 Q_7
msb
T

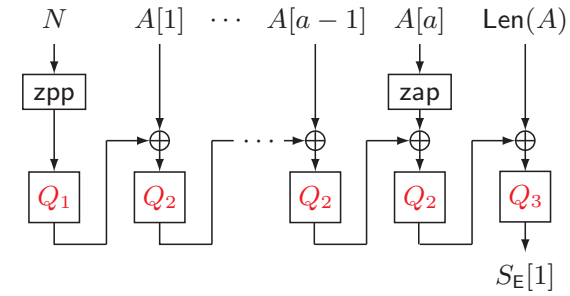

N
$A[1]$
$\cdots$
$A[a-1]$
$A[a]$
$\mathsf{Len}(A)$
zpp
zap
Q_1
Q_2
Q_2
Q_2
Q_3
$S_{\mathsf{E}}[1]$

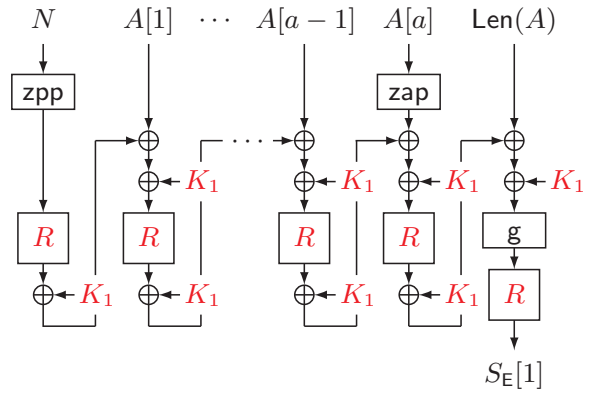

$S_{\mathsf{E}}[1]$
$M[1]$
$M[2]$
$\cdots$
$M[m-1]$
$M[m]$
fix1
fix1
fix1
Q_4
Q_4
Q_4
msb
$C[1]$
$C[2]$
$\cdots$
$C[m-1]$
$C[m]$

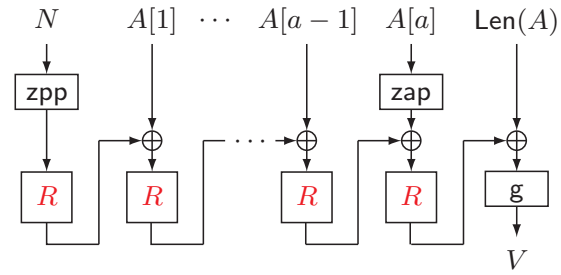

N
$A[1]$
$\cdots$
$A[a-1]$
$A[a]$
$\mathsf{Len}(A)$
zpp
zap
Q_1
Q_2
Q_2
Q_2
Q_5
$S_{\mathsf{P}}[0]$
$S_{\mathsf{P}}[0]$
$C[1]$
$C[2]$
$\cdots$
$C[m-1]$
$C[m]$
$\mathsf{Len}(C)$
zap
Q_6
Q_6
Q_6
Q_6
Q_7
msb
T

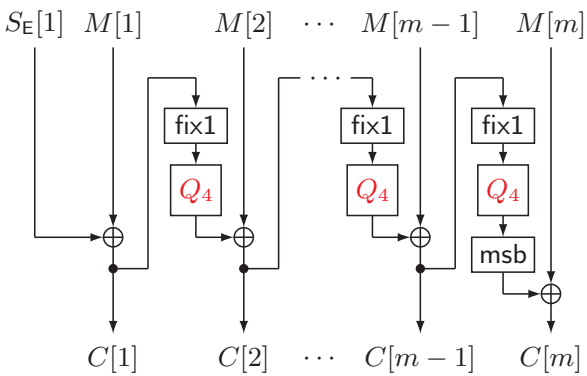
Two Properties of $Q = (Q_1, \ldots, Q_7)$ and SILC2

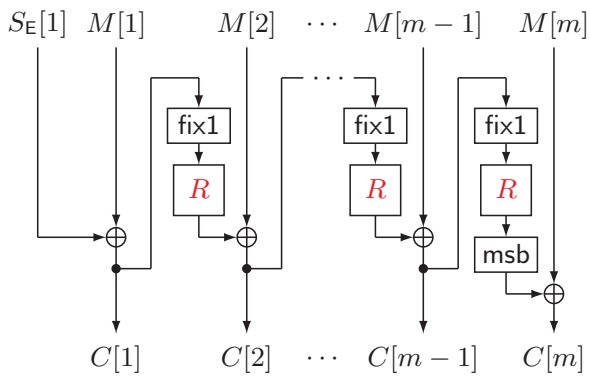
1. $(Q_1, \ldots, Q_7) \approx (F_1, \ldots, F_7)$ against input-respecting adversaries
   - $F_1, \ldots, F_7 \xleftarrow{\$} \mathrm{Rand}(n)$
   - $\mathcal{B}$ is input-respecting if a query X for Q_1/F_1 satisfies $\mathsf{msb}_1(X) = 0$ and a query X for Q_4/F_4 satisfies $\mathsf{msb}_1(X) = 1$
   - For an input-respecting adversary $\mathcal{B}$ that makes q queries,
     $$\Pr\left[\mathcal{B}^{Q_1,\ldots,Q_7} \Rightarrow 1\right] - \Pr\left[\mathcal{B}^{F_1,\ldots,F_7} \Rightarrow 1\right] \leq \frac{0.5q^2}{2^n}$$
2. $\mathrm{SILC2} = \mathrm{SILC}[\mathrm{Rand}(n)]$

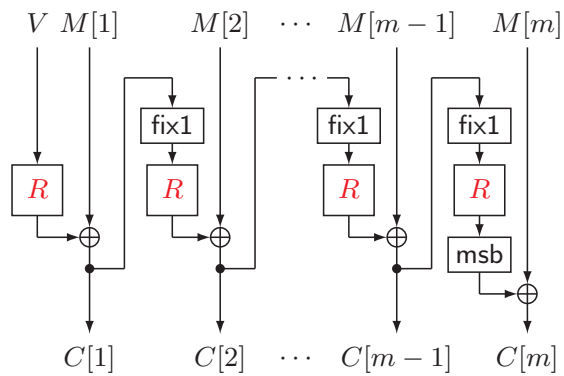

N $A[1]$ $\cdots$ $A[a-1]$ $A[a]$ $\mathsf{Len}(A)$
zpp
zap
Q_1 Q_2 Q_2 Q_2 Q_3
$S_{\mathsf{E}}[1]$

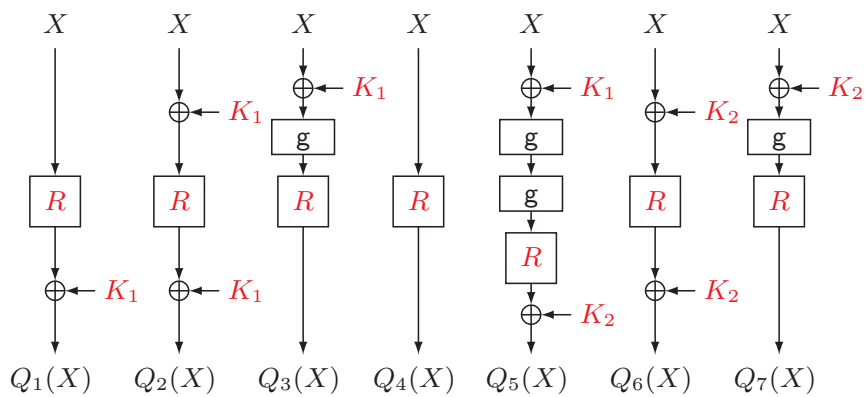

N $A[1]$ $\cdots$ $A[a-1]$ $A[a]$ $\mathsf{Len}(A)$
zpp
zap
K_1
R
g
$S_{\mathsf{E}}[1]$

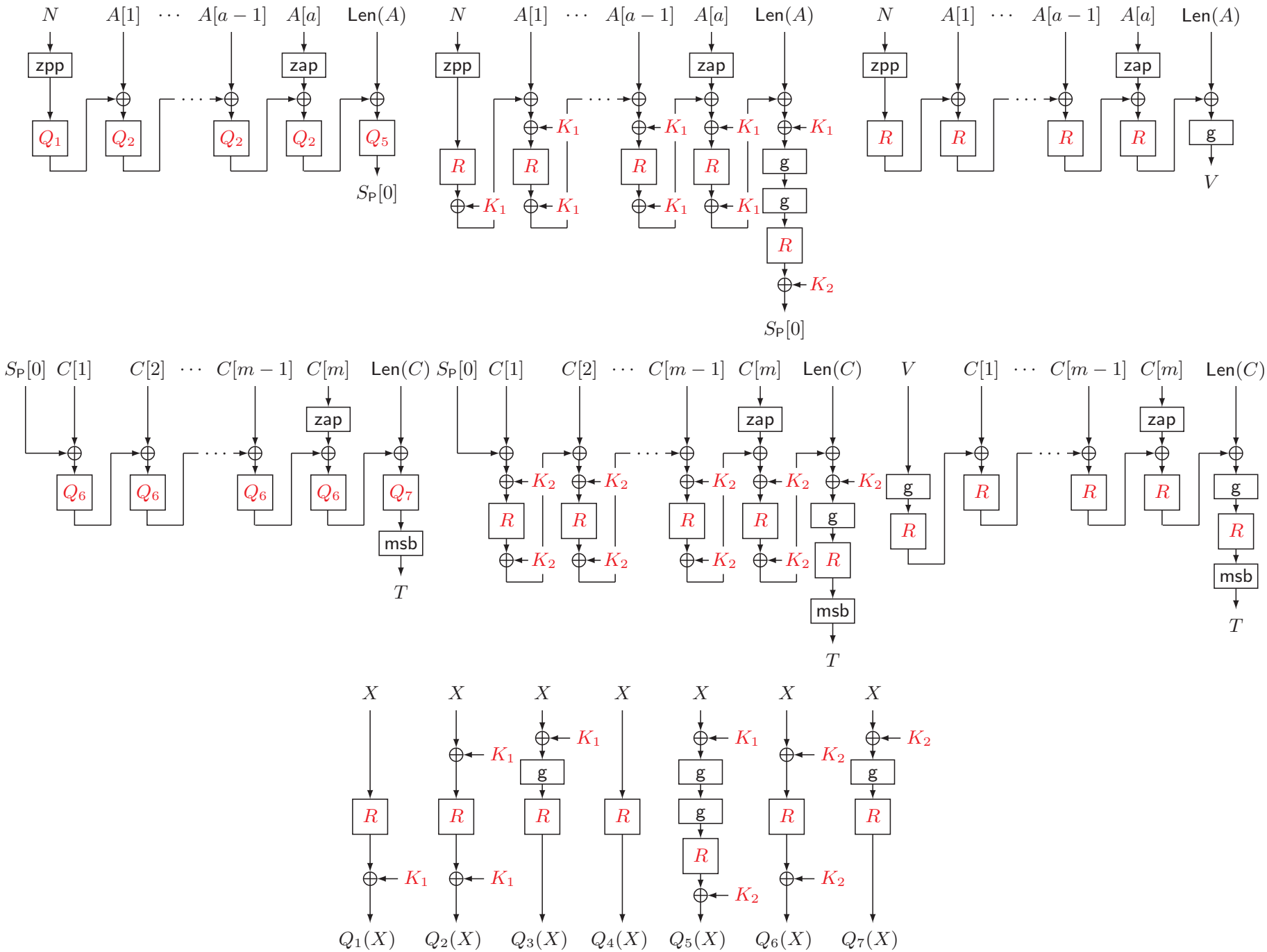

N $A[1]$ $\cdots$ $A[a-1]$ $A[a]$ $\mathsf{Len}(A)$
zpp
zap
R
g
V


$S_{\mathsf{E}}[1]$ $M[1]$ $M[2]$ $\cdots$ $M[m-1]$ $M[m]$
fix1
Q_4
msb
$C[1]$ $C[2]$ $\cdots$ $C[m-1]$ $C[m]$


$S_{\mathsf{E}}[1]$ $M[1]$ $M[2]$ $\cdots$ $M[m-1]$ $M[m]$
fix1
R
msb
$C[1]$ $C[2]$ $\cdots$ $C[m-1]$ $C[m]$


V $M[1]$ $M[2]$ $\cdots$ $M[m-1]$ $M[m]$
fix1
R
msb
$C[1]$ $C[2]$ $\cdots$ $C[m-1]$ $C[m]$

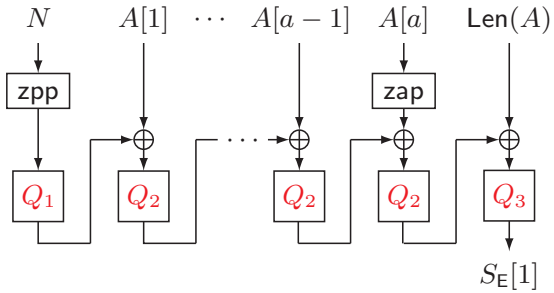

X
K_1 K_2
g
R
$Q_1(X)$ $Q_2(X)$ $Q_3(X)$ $Q_4(X)$ $Q_5(X)$ $Q_6(X)$ $Q_7(X)$

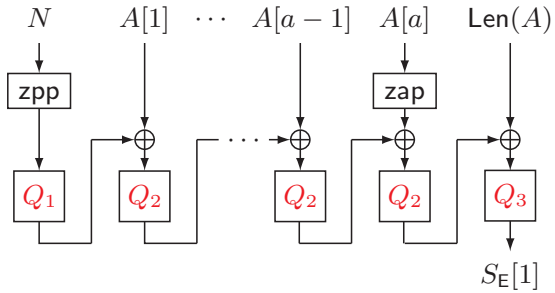

N
A[1]
A[a − 1]
A[a]
Len(A)
zpp
zap
Q1
Q2
Q5
SP[0]
R
K1
K2
g
V
S_P[0]
C[1]
C[2]
C[m − 1]
C[m]
Len(C)
Q6
Q7
msb
T
X
Q1(X)
Q2(X)
Q3(X)
Q4(X)
Q5(X)
Q6(X)
Q7(X)

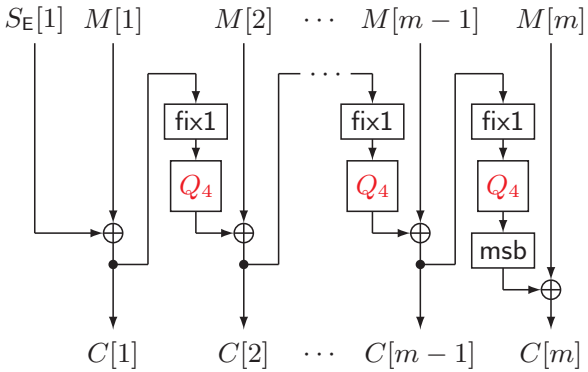
SILC[Rand(n)] to SILC2 to SILC3

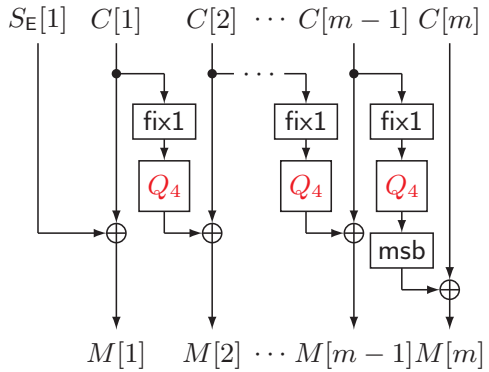
- $\mathbf{Adv}^{\text{int-rup}}_{\text{SILC[Rand}(n)\text{]}}(\mathcal{A}) = \mathbf{Adv}^{\text{int-rup}}_{\text{SILC2}}(\mathcal{A})$
- SILC3 is SILC2 with $F = (F_1, \ldots, F_7)$ instead of $Q = (Q_1, \ldots, Q_7)$
- $\mathbf{Adv}^{\text{int-rup}}_{\text{SILC2}}(\mathcal{A}) \leq \mathbf{Adv}^{\text{int-rup}}_{\text{SILC3}}(\mathcal{A}) + \dfrac{0.5\sigma^2}{2^n}$
- $\sigma = (3q + \sigma_A + 2\sigma_M) + (q' + \sigma_{A'} + \sigma_{C'}) + (3q'' + \sigma_{A''} + \sigma_{C''})$

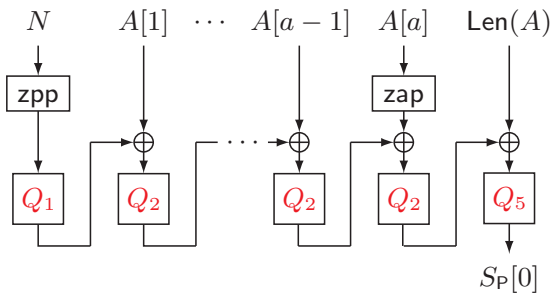
SILC2

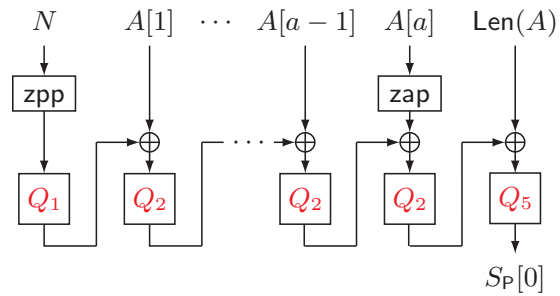

N $A[1]$ $\cdots$ $A[a-1]$ $A[a]$ $\mathsf{Len}(A)$
zpp
zap
Q_1 Q_2 Q_2 Q_2 Q_3
$S_{\mathsf{E}}[1]$

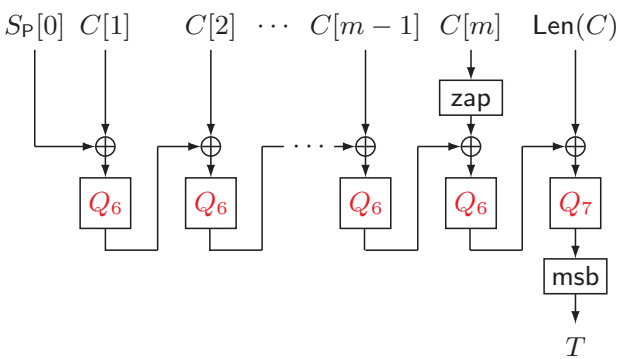

N $A[1]$ $\cdots$ $A[a-1]$ $A[a]$ $\mathsf{Len}(A)$
zpp
zap
Q_1 Q_2 Q_2 Q_2 Q_3
$S_{\mathsf{E}}[1]$

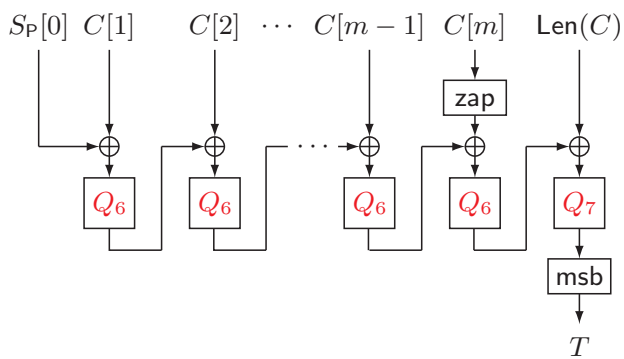

$S_{\mathsf{E}}[1]$ $M[1]$ $M[2]$ $\cdots$ $M[m-1]$ $M[m]$
fix1
Q_4
msb
$C[1]$ $C[2]$ $\cdots$ $C[m-1]$ $C[m]$


$S_{\mathsf{E}}[1]$ $C[1]$ $C[2]$ $\cdots$ $C[m-1]$ $C[m]$
fix1
Q_4
msb
$M[1]$ $M[2]$ $\cdots$ $M[m-1]$ $M[m]$

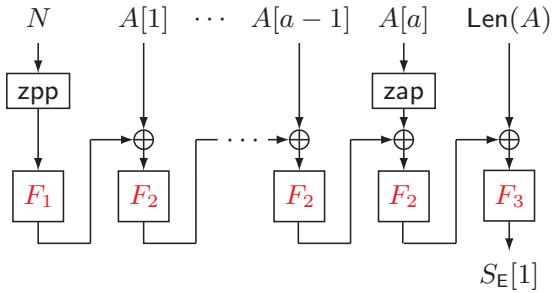

N $A[1]$ $\cdots$ $A[a-1]$ $A[a]$ $\mathsf{Len}(A)$
zpp
zap
Q_1 Q_2 Q_2 Q_2 Q_5
$S_{\mathsf{P}}[0]$

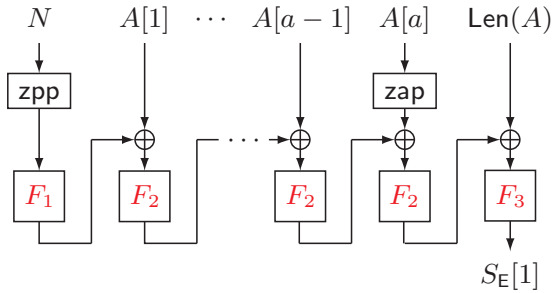

N $A[1]$ $\cdots$ $A[a-1]$ $A[a]$ $\mathsf{Len}(A)$
zpp
zap
Q_1 Q_2 Q_2 Q_2 Q_5
$S_{\mathsf{P}}[0]$

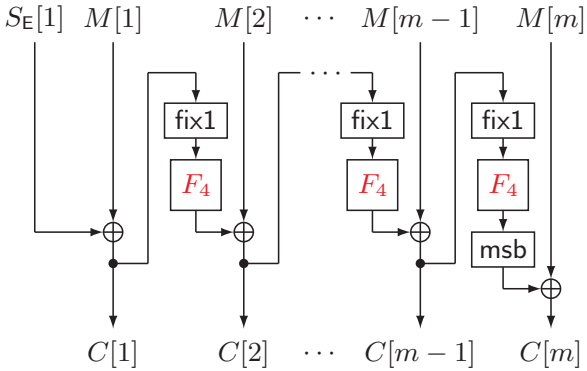

$S_{\mathsf{P}}[0]$ $C[1]$ $C[2]$ $\cdots$ $C[m-1]$ $C[m]$ $\mathsf{Len}(C)$
zap
Q_6 Q_6 Q_6 Q_6 Q_7
msb
T

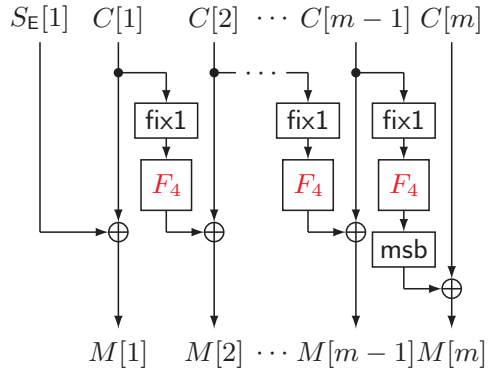

$S_{\mathsf{P}}[0]$ $C[1]$ $C[2]$ $\cdots$ $C[m-1]$ $C[m]$ $\mathsf{Len}(C)$
zap
Q_6 Q_6 Q_6 Q_6 Q_7
msb
T

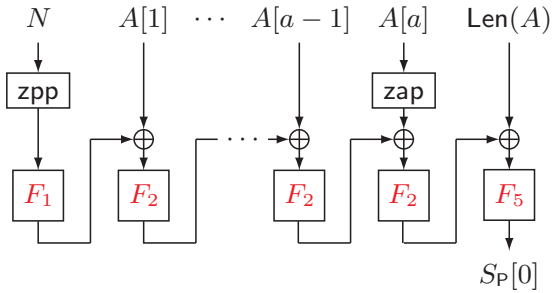
SILC3

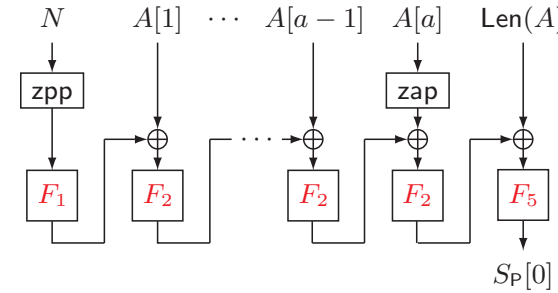

N $A[1]$ $\cdots$ $A[a-1]$ $A[a]$ $\mathsf{Len}(A)$
zpp
zap
F_1 F_2 F_2 F_2 F_3
$S_{\mathsf{E}}[1]$

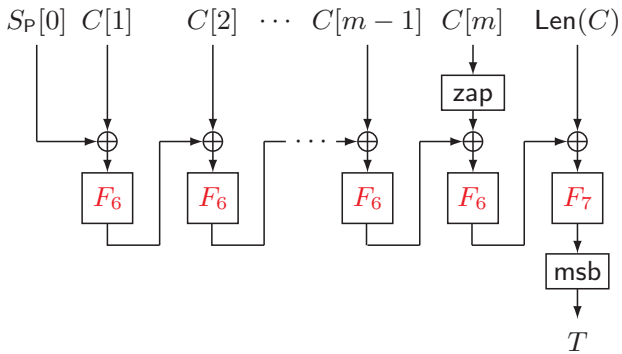

N $A[1]$ $\cdots$ $A[a-1]$ $A[a]$ $\mathsf{Len}(A)$
zpp
zap
F_1 F_2 F_2 F_2 F_3
$S_{\mathsf{E}}[1]$

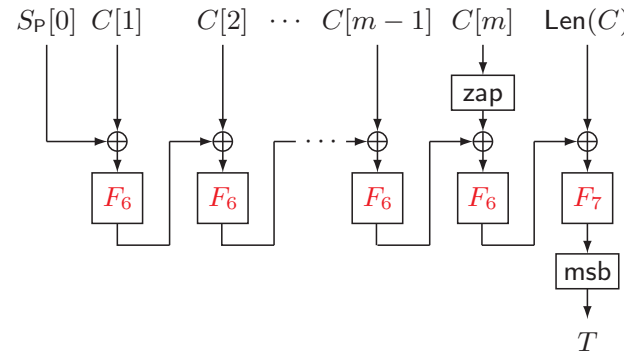

$S_{\mathsf{E}}[1]$ $M[1]$ $M[2]$ $\cdots$ $M[m-1]$ $M[m]$
fix1
F_4
msb
$C[1]$ $C[2]$ $\cdots$ $C[m-1]$ $C[m]$

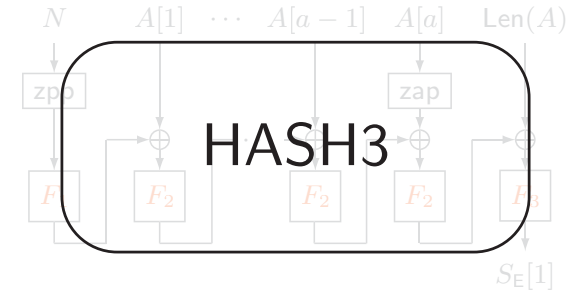

$S_{\mathsf{E}}[1]$ $C[1]$ $C[2]$ $\cdots$ $C[m-1]$ $C[m]$
fix1
F_4
msb
$M[1]$ $M[2]$ $\cdots$ $M[m-1]$ $M[m]$

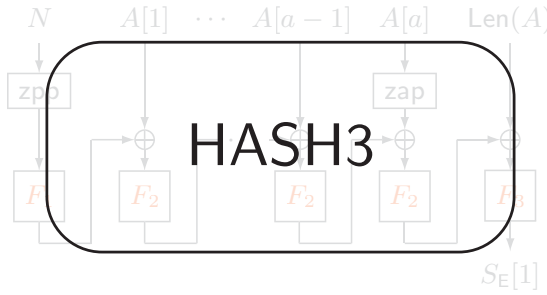

N $A[1]$ $\cdots$ $A[a-1]$ $A[a]$ $\mathsf{Len}(A)$
zpp
zap
F_1 F_2 F_2 F_2 F_5
$S_{\mathsf{P}}[0]$


N $A[1]$ $\cdots$ $A[a-1]$ $A[a]$ $\mathsf{Len}(A)$
zpp
zap
F_1 F_2 F_2 F_2 F_5
$S_{\mathsf{P}}[0]$

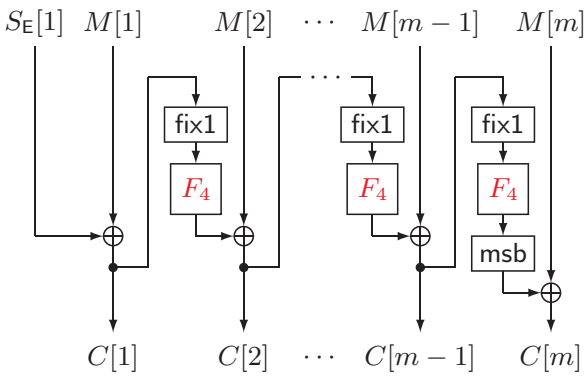

$S_{\mathsf{P}}[0]$ $C[1]$ $C[2]$ $\cdots$ $C[m-1]$ $C[m]$ $\mathsf{Len}(C)$
zap
F_6 F_6 F_6 F_6 F_7
msb
T

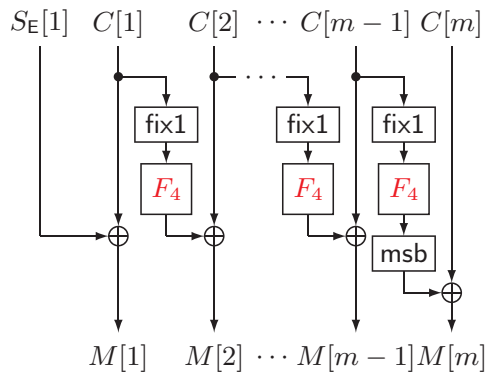

$S_{\mathsf{P}}[0]$ $C[1]$ $C[2]$ $\cdots$ $C[m-1]$ $C[m]$ $\mathsf{Len}(C)$
zap
F_6 F_6 F_6 F_6 F_7
msb
T

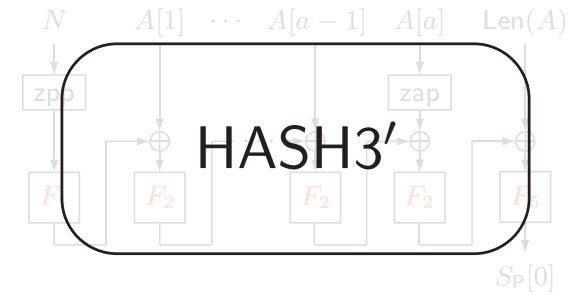

N
A[1]
A[a − 1]
A[a]
Len(A)
zap
HASH3
F
F2
F2
F2
F
S_E[1]

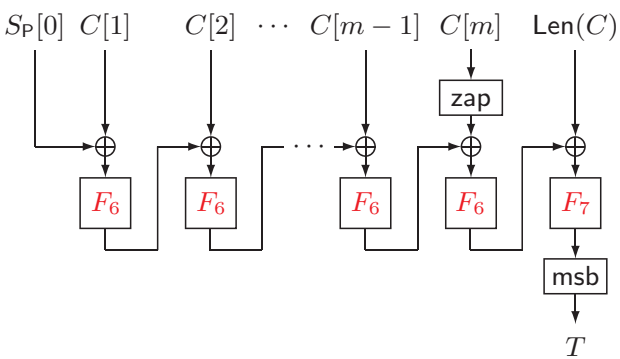

N
A[1]
A[a − 1]
A[a]
Len(A)
zap
HASH3
F
F2
F2
F2
F
S_E[1]

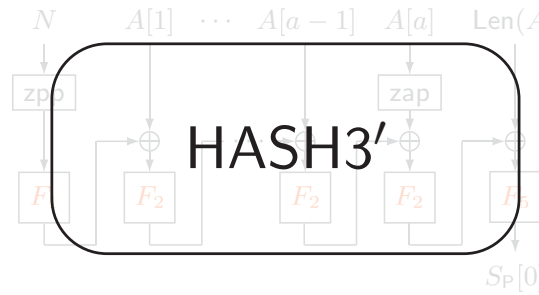
SILC3

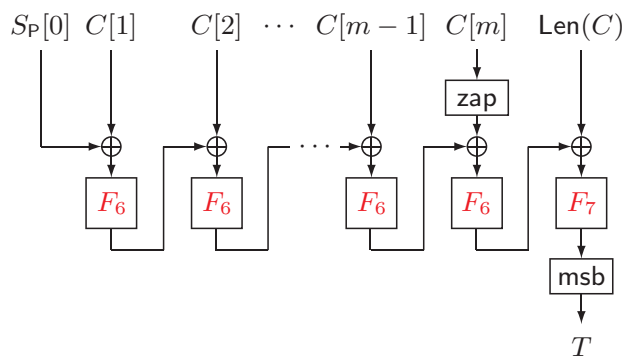

S_E[1]
M[1]
M[2]
M[m − 1]
M[m]
fix1
F4
msb
C[1]
C[2]
C[m − 1]
C[m]


S_E[1]
C[1]
C[2]
C[m − 1]
C[m]
fix1
F4
msb
M[1]
M[2]
M[m − 1]
M[m]


N
A[1]
A[a − 1]
A[a]
Len(A)
zap
HASH3′
F
F2
F2
F2
F
S_P[0]


S_P[0]
C[1]
C[2]
C[m − 1]
C[m]
Len(C)
zap
F6
F7
msb
T


N
A[1]
A[a − 1]
A[a]
Len(A)
zap
HASH3′
F
F2
F2
F2
F
S_P[0]


S_P[0]
C[1]
C[2]
C[m − 1]
C[m]
Len(C)
zap
F6
F7
msb
T

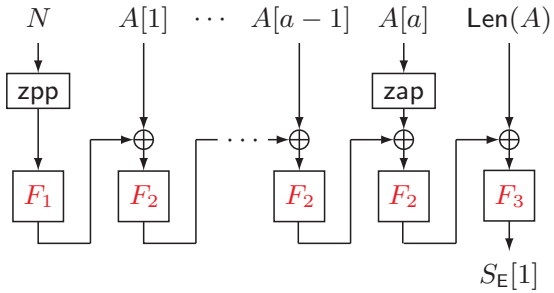
SILC3 to SILC4

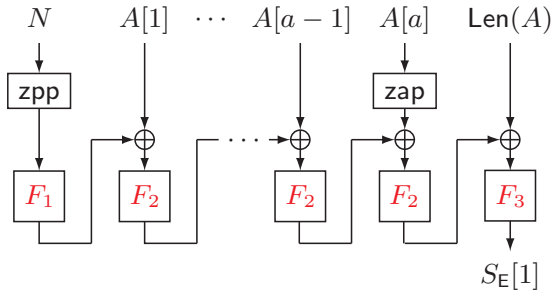
- $\mathsf{HASH4}, \mathsf{HASH4}' \xleftarrow{\$} \mathrm{Rand}(\mathcal{N}_{\mathrm{SILC}} \times \mathcal{A}_{\mathrm{SILC}}, n)$
- $(\mathsf{HASH3}, \mathsf{HASH3}') \approx (\mathsf{HASH4}, \mathsf{HASH4}')$
- For an adversary $\mathcal{B}$ that makes q queries with a total of σ_A blocks,

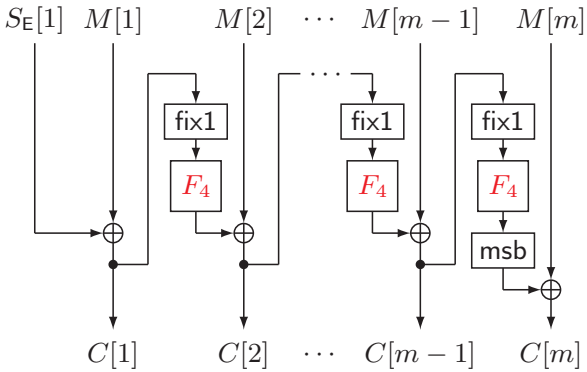
$$\Pr\left[\mathcal{B}^{\mathsf{HASH3},\mathsf{HASH3}'} \Rightarrow 1\right] - \Pr\left[\mathcal{B}^{\mathsf{HASH4},\mathsf{HASH4}'} \Rightarrow 1\right] \leq \frac{0.5q^2}{2^n} + \frac{(q+\sigma_A)^2}{2^n}$$

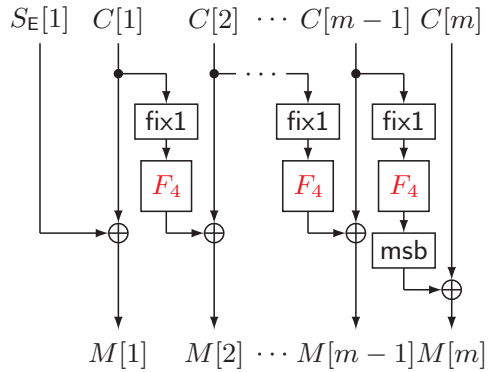
- SILC4 is SILC3 with $(\mathsf{HASH4}, \mathsf{HASH4}')$ instead of $(\mathsf{HASH3}, \mathsf{HASH3}')$
- $\mathbf{Adv}^{\text{int-rup}}_{\text{SILC3}}(\mathcal{A}) \leq \mathbf{Adv}^{\text{int-rup}}_{\text{SILC4}}(\mathcal{A}) + \frac{0.5(2q+q'+q'')^2}{2^n} + \frac{\left((2q+q'+q'')+(2\sigma_A+\sigma_{A'}+\sigma_{A''})\right)^2}{2^n}$

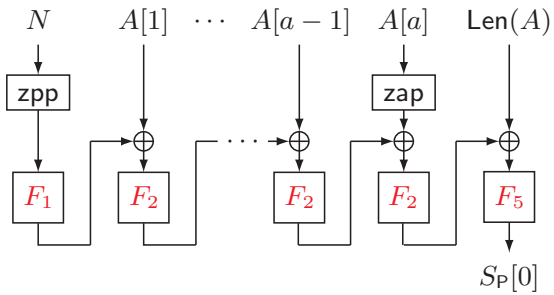
SILC3

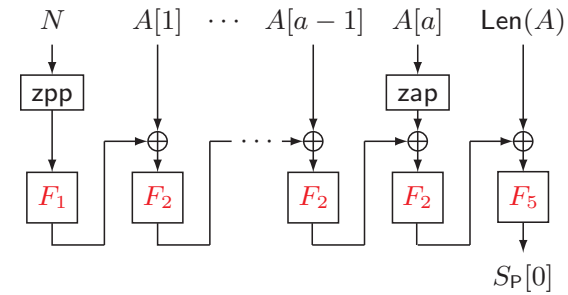

N $A[1]$ $\cdots$ $A[a-1]$ $A[a]$ $\mathsf{Len}(A)$
zpp
zap
F_1 F_2 F_2 F_2 F_3
$S_{\mathsf{E}}[1]$

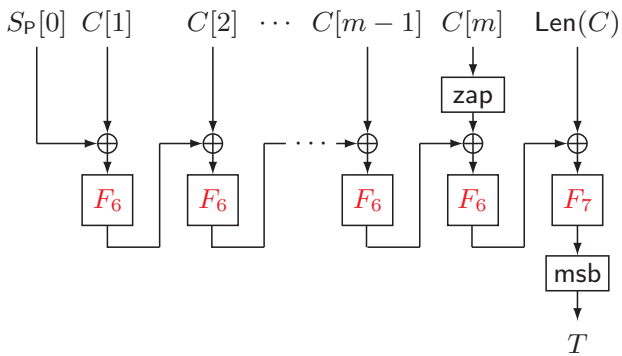

N $A[1]$ $\cdots$ $A[a-1]$ $A[a]$ $\mathsf{Len}(A)$
zpp
zap
F_1 F_2 F_2 F_2 F_3
$S_{\mathsf{E}}[1]$

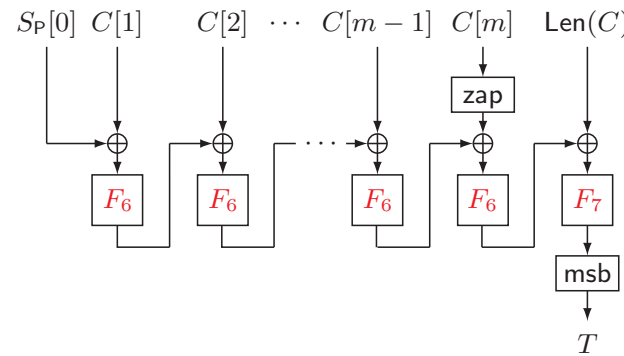

$S_{\mathsf{E}}[1]$ $M[1]$ $M[2]$ $\cdots$ $M[m-1]$ $M[m]$
fix1
F_4
msb
$C[1]$ $C[2]$ $\cdots$ $C[m-1]$ $C[m]$

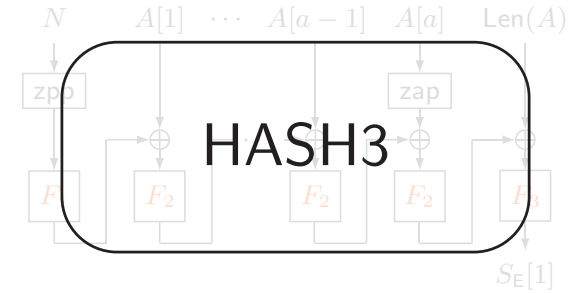

$S_{\mathsf{E}}[1]$ $C[1]$ $C[2]$ $\cdots$ $C[m-1]$ $C[m]$
fix1
F_4
msb
$M[1]$ $M[2]$ $\cdots$ $M[m-1]$ $M[m]$

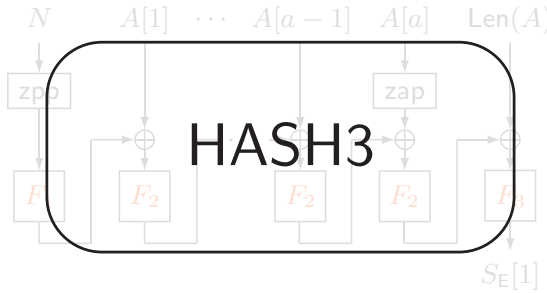

N $A[1]$ $\cdots$ $A[a-1]$ $A[a]$ $\mathsf{Len}(A)$
zpp
zap
F_1 F_2 F_2 F_2 F_5
$S_{\mathsf{P}}[0]$


N $A[1]$ $\cdots$ $A[a-1]$ $A[a]$ $\mathsf{Len}(A)$
zpp
zap
F_1 F_2 F_2 F_2 F_5
$S_{\mathsf{P}}[0]$

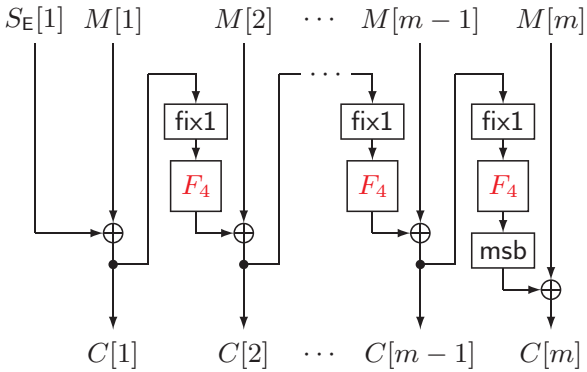

$S_{\mathsf{P}}[0]$ $C[1]$ $C[2]$ $\cdots$ $C[m-1]$ $C[m]$ $\mathsf{Len}(C)$
zap
F_6 F_6 F_6 F_6 F_7
msb
T

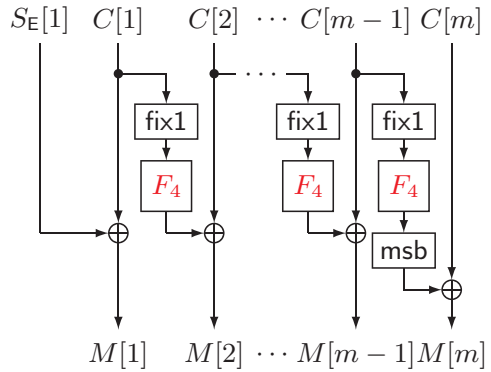

$S_{\mathsf{P}}[0]$ $C[1]$ $C[2]$ $\cdots$ $C[m-1]$ $C[m]$ $\mathsf{Len}(C)$
zap
F_6 F_6 F_6 F_6 F_7
msb
T

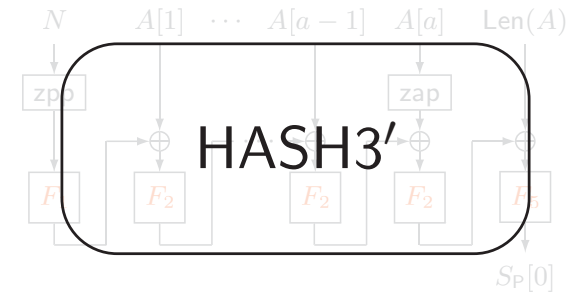

N $A[1]$ $\cdots$ $A[a-1]$ $A[a]$ $\mathsf{Len}(A)$
zap
HASH3
F_2
$S_{\mathsf{E}}[1]$

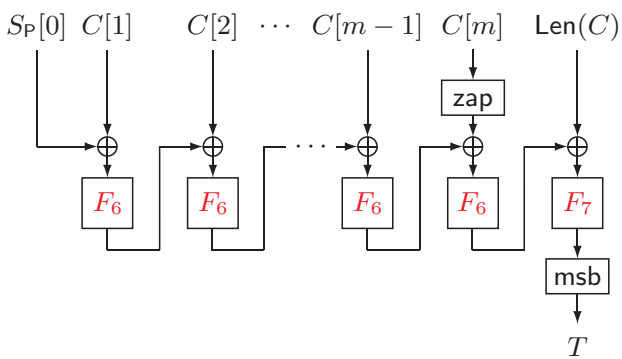

N $A[1]$ $\cdots$ $A[a-1]$ $A[a]$ $\mathsf{Len}(A)$
zap
HASH3
F_2
$S_{\mathsf{E}}[1]$

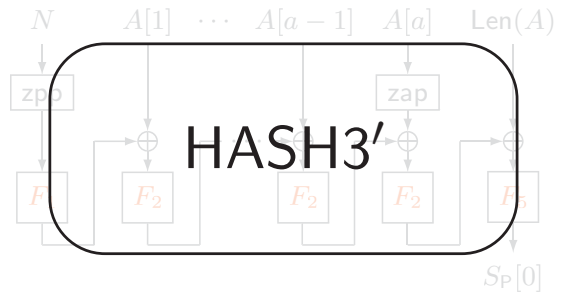
SILC3

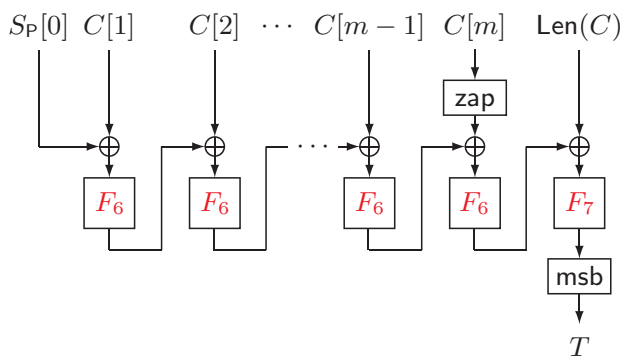

$S_{\mathsf{E}}[1]$ $M[1]$ $M[2]$ $\cdots$ $M[m-1]$ $M[m]$
fix1
F_4
msb
$C[1]$ $C[2]$ $\cdots$ $C[m-1]$ $C[m]$


$S_{\mathsf{E}}[1]$ $C[1]$ $C[2]$ $\cdots$ $C[m-1]$ $C[m]$
fix1
F_4
msb
$M[1]$ $M[2]$ $\cdots$ $M[m-1]$ $M[m]$

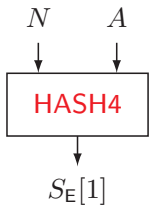

N $A[1]$ $\cdots$ $A[a-1]$ $A[a]$ $\mathsf{Len}(A)$
zap
HASH3′
F_2
$S_{\mathsf{P}}[0]$

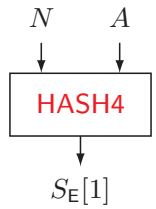

$S_{\mathsf{P}}[0]$ $C[1]$ $C[2]$ $\cdots$ $C[m-1]$ $C[m]$ $\mathsf{Len}(C)$
zap
F_6
F_7
msb
T

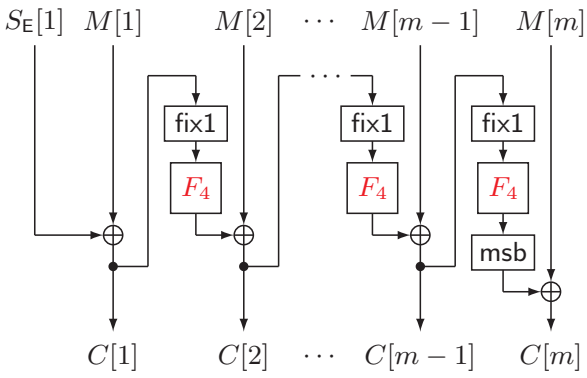

N $A[1]$ $\cdots$ $A[a-1]$ $A[a]$ $\mathsf{Len}(A)$
zap
HASH3′
F_2
$S_{\mathsf{P}}[0]$

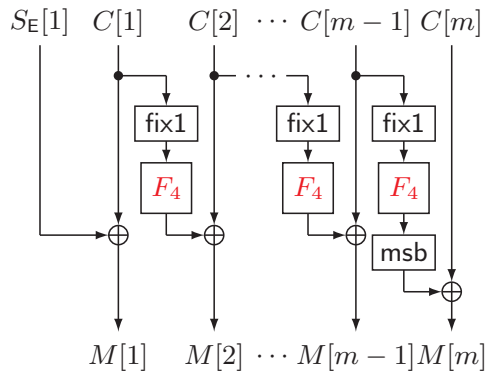

$S_{\mathsf{P}}[0]$ $C[1]$ $C[2]$ $\cdots$ $C[m-1]$ $C[m]$ $\mathsf{Len}(C)$
zap
F_6
F_7
msb
T

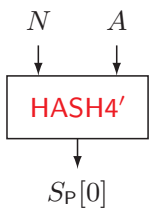
SILC4

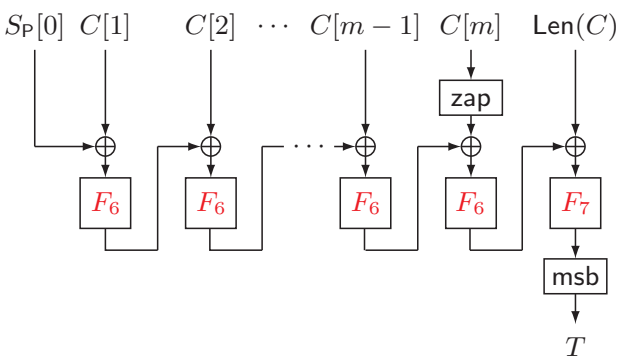

N
A
HASH4
$S_E[1]$

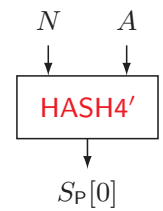

N
A
HASH4
$S_E[1]$

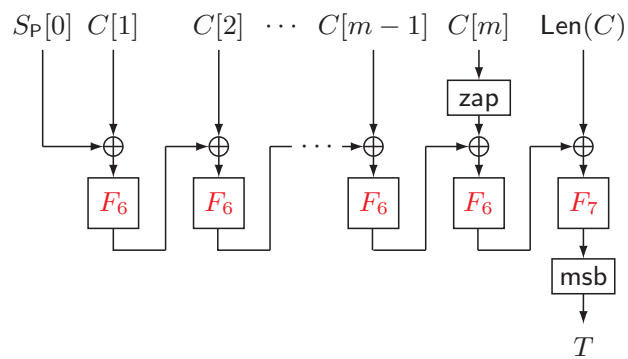

$S_E[1]$ $M[1]$ $M[2]$ $\cdots$ $M[m-1]$ $M[m]$
fix1
F_4
msb
$C[1]$ $C[2]$ $\cdots$ $C[m-1]$ $C[m]$

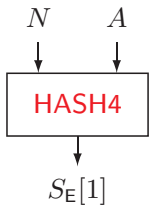

$S_E[1]$ $C[1]$ $C[2]$ $\cdots$ $C[m-1]$ $C[m]$
fix1
F_4
msb
$M[1]$ $M[2]$ $\cdots$ $M[m-1]$ $M[m]$

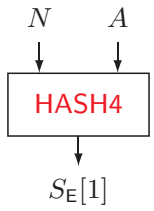

N
A
HASH4′
$S_P[0]$


$S_P[0]$ $C[1]$ $C[2]$ $\cdots$ $C[m-1]$ $C[m]$ Len(C)
zap
F_6
F_7
msb
T

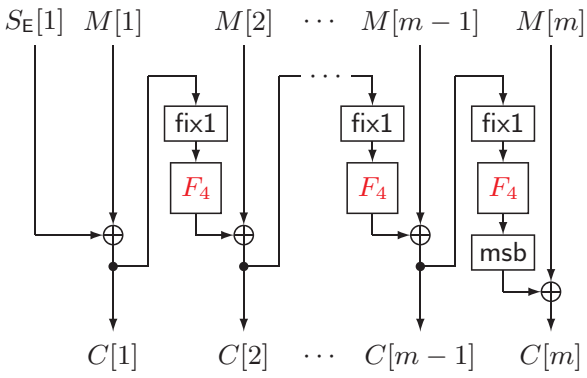

N
A
HASH4′
$S_P[0]$

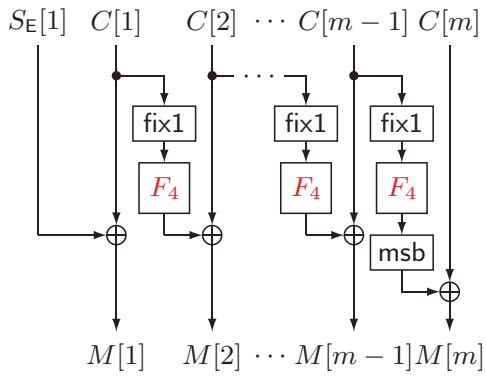

$S_P[0]$ $C[1]$ $C[2]$ $\cdots$ $C[m-1]$ $C[m]$ Len(C)
zap
F_6
F_7
msb
T

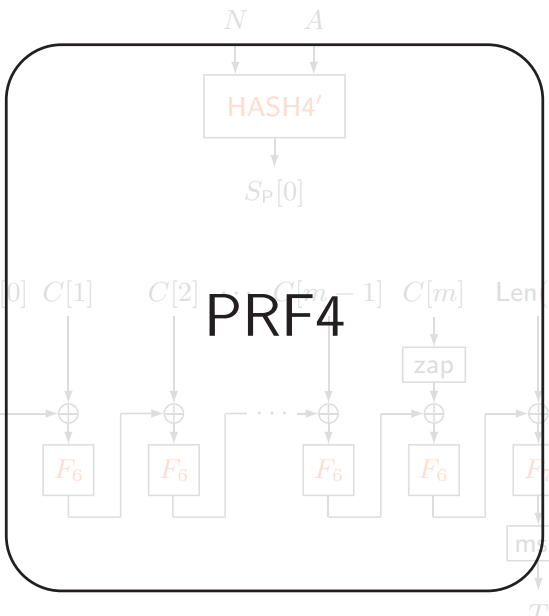

N
A
HASH4
$S_E[1]$

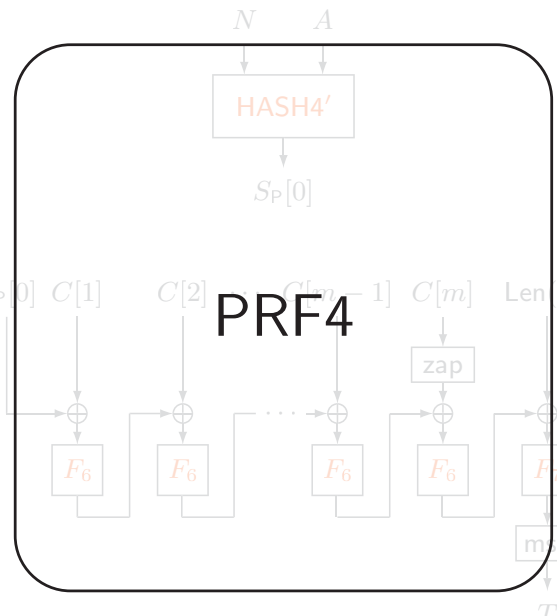

N
A
HASH4
$S_E[1]$

SILC4


$S_E[1]$ $M[1]$ $M[2]$ $\cdots$ $M[m-1]$ $M[m]$
fix1
F_4
msb
$C[1]$ $C[2]$ $\cdots$ $C[m-1]$ $C[m]$


$S_E[1]$ $C[1]$ $C[2]$ $\cdots$ $C[m-1]$ $C[m]$
fix1
F_4
msb
$M[1]$ $M[2]$ $\cdots$ $M[m-1]$ $M[m]$


N
A
HASH4′
$S_P[0]$
PRF4
zap
F_6
F_7
msb
T


N
A
HASH4′
$S_P[0]$
PRF4
zap
F_6
F_7
msb
T

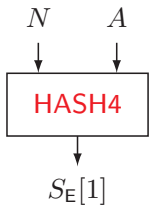
SILC4 to SILC5

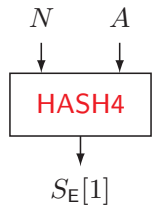
- $\mathsf{PRF5} \xleftarrow{\$} \mathrm{Rand}(\mathcal{N}_{\mathrm{SILC}} \times \mathcal{A}_{\mathrm{SILC}} \times \mathcal{C}_{\mathrm{SILC}}, \tau)$
- $\mathsf{PRF4} \approx \mathsf{PRF5}$
- For an adversary $\mathcal{B}$ that makes q queries with a total of σ_C ciphertext blocks,

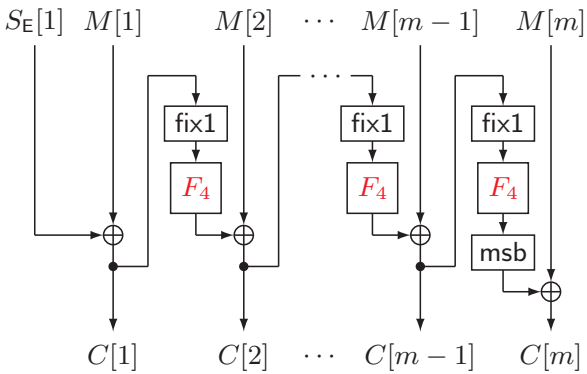
  $$\Pr\left[\mathcal{B}^{\mathsf{PRF4}} \Rightarrow 1\right] - \Pr\left[\mathcal{B}^{\mathsf{PRF5}} \Rightarrow 1\right] \leq \frac{0.5q^2}{2^n} + \frac{(q+\sigma_C)^2}{2^n}$$

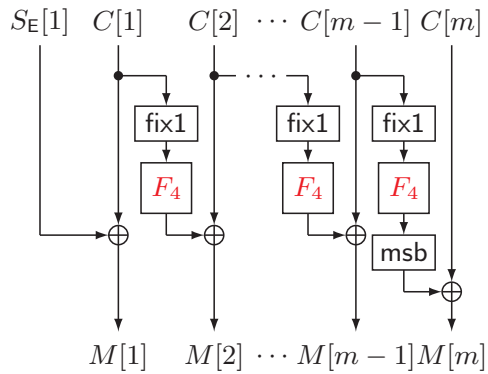
- SILC5 is SILC4 with PRF5 instead of PRF4 (and HASH4 is renamed to HASH5)
- $$\mathbf{Adv}^{\text{int-rup}}_{\mathrm{SILC4}}(\mathcal{A}) \leq \mathbf{Adv}^{\text{int-rup}}_{\mathrm{SILC5}}(\mathcal{A}) + \frac{0.5(q+q'')^2}{2^n} + \frac{\left((q+q'')+(\sigma_M+\sigma_{C''})\right)^2}{2^n}$$
- Transition from SILC[Perm(n)] to SILC5 does not rely on the nonce uniqueness

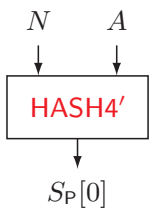
SILC4

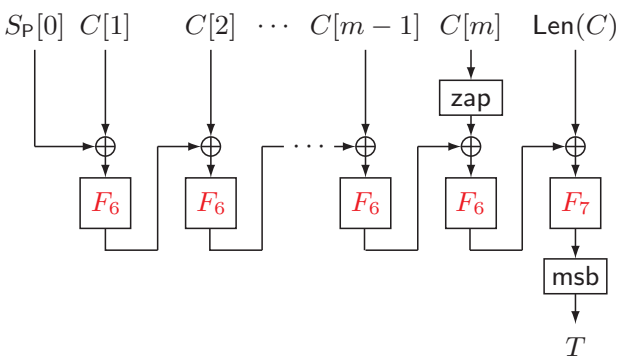

N
A
HASH4
$S_E[1]$

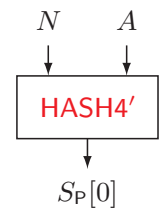

N
A
HASH4
$S_E[1]$

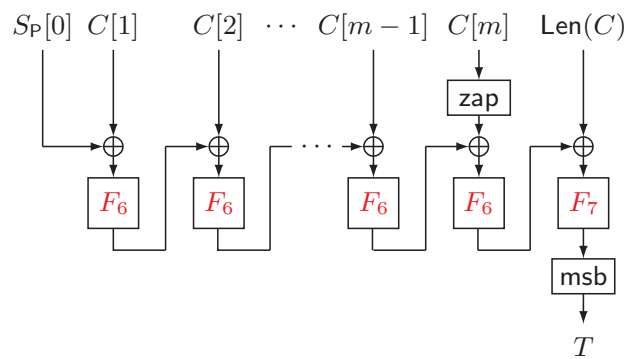

$S_E[1]$ $M[1]$ $M[2]$ $\cdots$ $M[m-1]$ $M[m]$
fix1
F_4
msb
$C[1]$ $C[2]$ $\cdots$ $C[m-1]$ $C[m]$

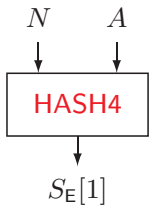

$S_E[1]$ $C[1]$ $C[2]$ $\cdots$ $C[m-1]$ $C[m]$
fix1
F_4
msb
$M[1]$ $M[2]$ $\cdots$ $M[m-1]$ $M[m]$

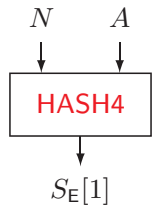

N
A
HASH4′
$S_P[0]$


$S_P[0]$ $C[1]$ $C[2]$ $\cdots$ $C[m-1]$ $C[m]$ Len(C)
zap
F_6
F_7
msb
T

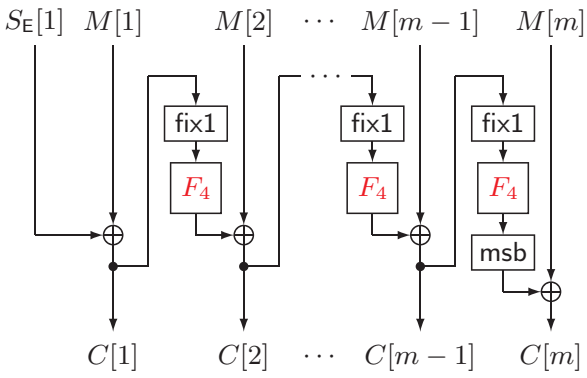

N
A
HASH4′
$S_P[0]$

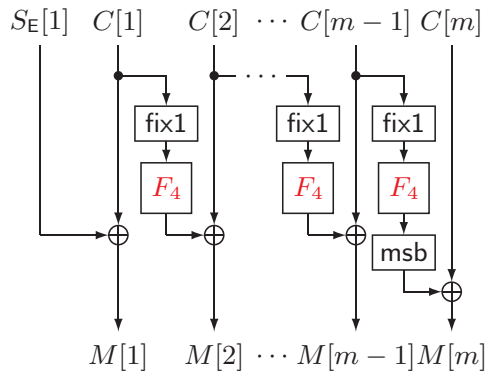

$S_P[0]$ $C[1]$ $C[2]$ $\cdots$ $C[m-1]$ $C[m]$ Len(C)
zap
F_6
F_7
msb
T

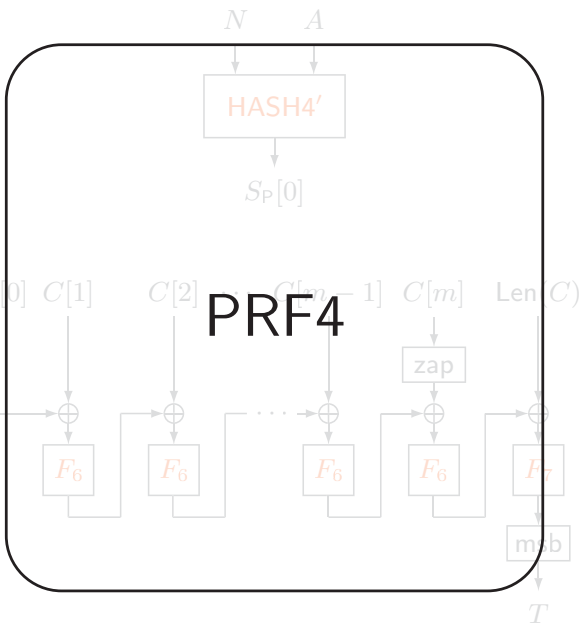

N
A
HASH4
$S_E[1]$

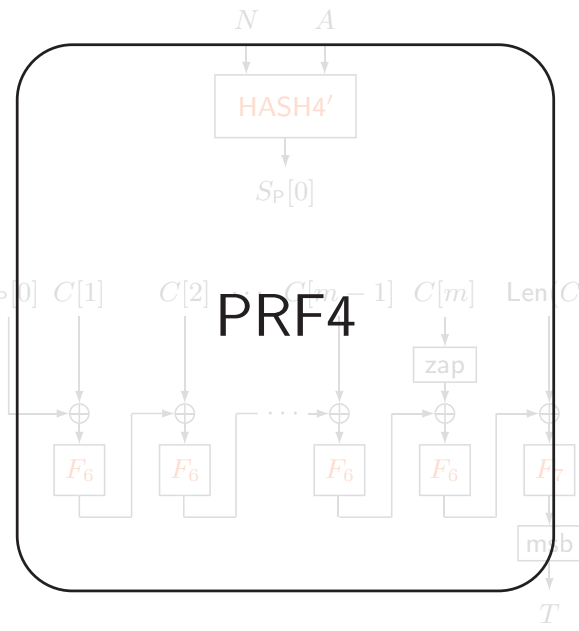

N
A
HASH4
$S_E[1]$

SILC4

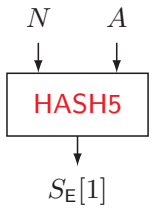

$S_E[1]$ $M[1]$ $M[2]$ $\cdots$ $M[m-1]$ $M[m]$
fix1
F_4
msb
$C[1]$ $C[2]$ $\cdots$ $C[m-1]$ $C[m]$

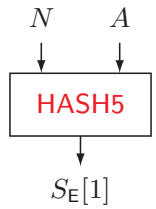

$S_E[1]$ $C[1]$ $C[2]$ $\cdots$ $C[m-1]$ $C[m]$
fix1
F_4
msb
$M[1]$ $M[2]$ $\cdots$ $M[m-1]$ $M[m]$

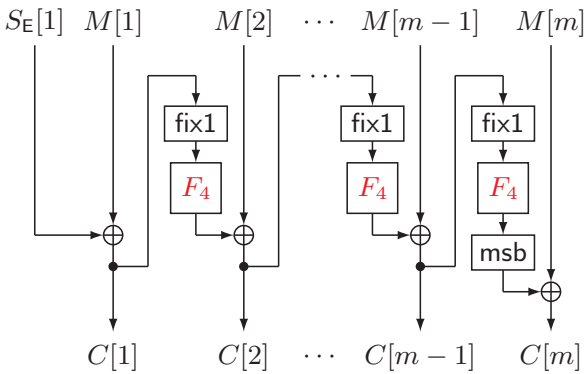

N
A
HASH4′
$S_P[0]$
PRF4
zap
F_6
F_7
msb
T

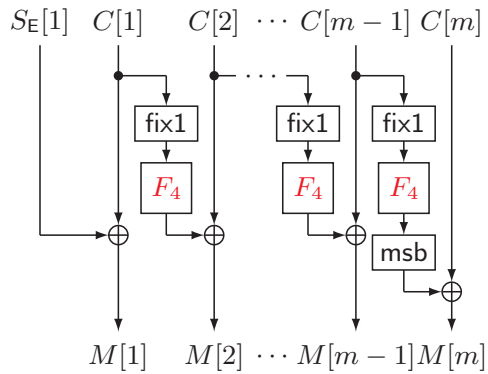

N
A
HASH4′
$S_P[0]$
PRF4
zap
F_6
F_7
msb
T

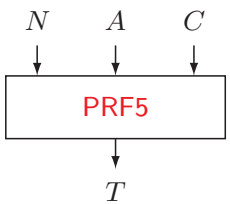
SILC5

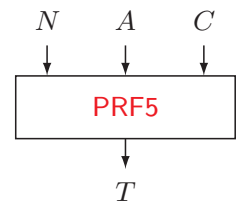

N
A
HASH5
$S_E[1]$


N
A
HASH5
$S_E[1]$

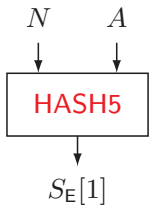

$S_E[1]$
$M[1]$
$M[2]$
$\cdots$
$M[m-1]$
$M[m]$
fix1
F_4
msb
$C[1]$
$C[2]$
$\cdots$
$C[m-1]$
$C[m]$

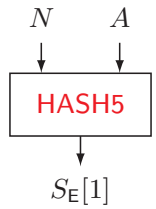

$S_E[1]$
$C[1]$
$C[2]$
$\cdots$
$C[m-1]$
$C[m]$
fix1
F_4
msb
$M[1]$
$M[2]$
$\cdots$
$M[m-1]$
$M[m]$

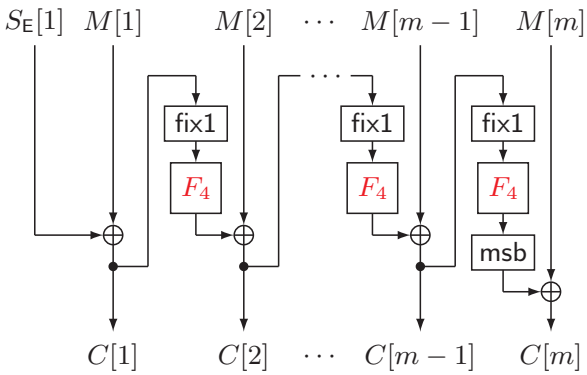

N
A
C
PRF5
T

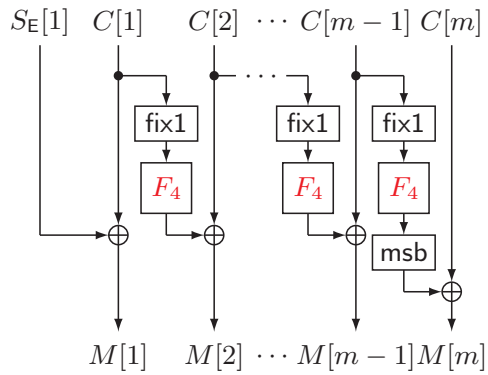

N
A
C
PRF5
T

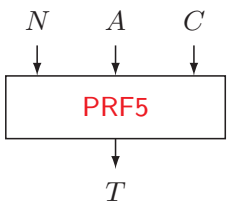
SILC5

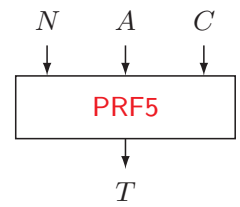

N
A
HASH5
$S_E[1]$


N
A
HASH5
$S_E[1]$


$S_E[1]$ $M[1]$ $M[2]$ $\cdots$ $M[m-1]$ $M[m]$
fix1
F_4
msb
$C[1]$ $C[2]$ $\cdots$ $C[m-1]$ $C[m]$


$S_E[1]$ $C[1]$ $C[2]$ $\cdots$ $C[m-1]$ $C[m]$
fix1
F_4
msb
$M[1]$ $M[2]$ $\cdots$ $M[m-1]$ $M[m]$


N
A
C
PRF5
T


N
A
C
PRF5
T


$\mathcal{A}$

$\mathbf{Adv}^{\text{int-rup}}_{\text{SILC5}}(\mathcal{A})$ and the Summary So Far

- $\mathbf{Adv}^{\text{int-rup}}_{\text{SILC5}}(\mathcal{A}) \leq \dfrac{q''}{2^\tau}$
- $\mathbf{Adv}^{\text{int-rup}}_{\text{SILC}[\text{Perm}(n)]}(\mathcal{A}) \leq \mathbf{Adv}^{\text{int-rup}}_{\text{SILC}[\text{Rand}(n)]}(\mathcal{A}) + \dfrac{0.5\sigma^2}{2^n}$
- $\mathbf{Adv}^{\text{int-rup}}_{\text{SILC}[\text{Rand}(n)]}(\mathcal{A}) = \mathbf{Adv}^{\text{int-rup}}_{\text{SILC2}}(\mathcal{A})$
- $\mathbf{Adv}^{\text{int-rup}}_{\text{SILC2}}(\mathcal{A}) \leq \mathbf{Adv}^{\text{int-rup}}_{\text{SILC3}}(\mathcal{A}) + \dfrac{0.5\sigma^2}{2^n}$
- $\mathbf{Adv}^{\text{int-rup}}_{\text{SILC3}}(\mathcal{A}) \leq \mathbf{Adv}^{\text{int-rup}}_{\text{SILC4}}(\mathcal{A}) + \dfrac{0.5(2q+q'+q'')^2}{2^n} + \dfrac{\left((2q+q'+q'')+(2\sigma_A+\sigma_{A'}+\sigma_{A''})\right)^2}{2^n}$
- $\mathbf{Adv}^{\text{int-rup}}_{\text{SILC4}}(\mathcal{A}) \leq \mathbf{Adv}^{\text{int-rup}}_{\text{SILC5}}(\mathcal{A}) + \dfrac{0.5(q+q'')^2}{2^n} + \dfrac{\left((q+q'')+(\sigma_M+\sigma_{C''})\right)^2}{2^n}$
- $\sigma = (3q+\sigma_A+2\sigma_M)+(q'+\sigma_{A'}+\sigma_{C'})+(3q''+\sigma_{A''}+\sigma_{C''})$

SILC Is INT-RUP Secure

Theorem

For any INT-RUP adversary $\mathcal{A}$ that makes q encryption queries (σ_A blocks and σ_M blocks), q' decryption queries ($\sigma_{A'}$ blocks and $\sigma_{C'}$ blocks), and q'' verification queries ($\sigma_{A''}$ blocks and $\sigma_{C''}$ blocks), we have

$$\mathbf{Adv}^{\text{int-rup}}_{\text{SILC}[\text{Perm}(n),\ell_N,\tau]}(\mathcal{A}) \leq \frac{5\sigma^2}{2^n} + \frac{q''}{2^\tau},$$

where $\sigma = (3q + \sigma_A + 2\sigma_M) + (q' + \sigma_{A'} + \sigma_{C'}) + (3q'' + \sigma_{A''} + \sigma_{C''})$

Summary

- SILC is INT-RUP secure against nonce-reusing adversaries up to the birthday bound
  - insecure in terms of privacy in RUP setting/nonce-reuse setting
- We expect that a similar proof is possible for CLOC (still in the process of verification)