Farfalle and Kravatte

Parallel permutation-based cryptography

Guido Bertoni[1] Joan Daemen[1,2] Michaël Peeters[1]
Gilles Van Assche[1] Ronny Van Keer[1]

[1]STMicroelectronics
[2]Radboud University

Early Symmetric Crypto 2017

Outline

Outline

Incrementality

$$F_k\left(M^{(0)}\right)$$

Incrementality

$$F_k\left(M^{(1)} \circ M^{(0)}\right)$$

Incrementality

$$F_k\left(M^{(2)} \circ M^{(1)} \circ M^{(0)}\right)$$

Incrementality

$$F_k\left(M^{(m-1)} \circ \cdots \circ M^{(2)} \circ M^{(1)} \circ M^{(0)}\right)$$

Session authenticated encryption (SAE)

Initialization taking nonce $N \in \mathbb{Z}_2^*$
$T \leftarrow 0^t + F_k(N)$
history $\leftarrow N$
return tag $T \in \mathbb{Z}_2^t$

Wrap taking metadata $A \in \mathbb{Z}_2^*$ and plaintext $P \in \mathbb{Z}_2^*$
$C \leftarrow P + F_k(A \circ \text{history})$
$T \leftarrow 0^t + F_k(C \circ A \circ \text{history})$
history $\leftarrow C \circ A \circ$ history
return ciphertext $C \in \mathbb{Z}_2^{|P|}$ and tag $T \in \mathbb{Z}_2^t$

Synthetic initialization value (SIV)

Wrap taking metadata $A \in \mathbb{Z}_2^*$ and plaintext $P \in \mathbb{Z}_2^*$
$T \leftarrow 0^t + F_k(P \circ A)$
$C \leftarrow P + F_k(T \circ A)$
return ciphertext $C \in \mathbb{Z}_2^{|P|}$, tag $T \in \mathbb{Z}_2^t$

Unwrap taking metadata $A \in \mathbb{Z}_2^*$, ciphertext $C \in \mathbb{Z}_2^*$ and tag $T \in \mathbb{Z}_2^t$
$P \leftarrow C + F_k(T \circ A)$
$T' \leftarrow 0^t + F_k(P \circ A)$
if T' = T **then**
  return plaintext $P \in \mathbb{Z}_2^{|C|}$
else
  return error!

Wide block cipher (WBC)

Encipher taking key $k \in \mathbb{Z}_2^*$, tweak $W \in \mathbb{Z}_2^*$ and plaintext $P \in \mathbb{Z}_2^*$

$(L, R) \leftarrow \text{split}(P, r)$

$R_0 \leftarrow R_0 + H_k(L \circ 0)$ (R_0: the first $\min(b, |R|)$ bits of R)

$L \leftarrow L + F_k(R \circ W \circ 1)$

$R \leftarrow R + F_k(L \circ W \circ 0)$

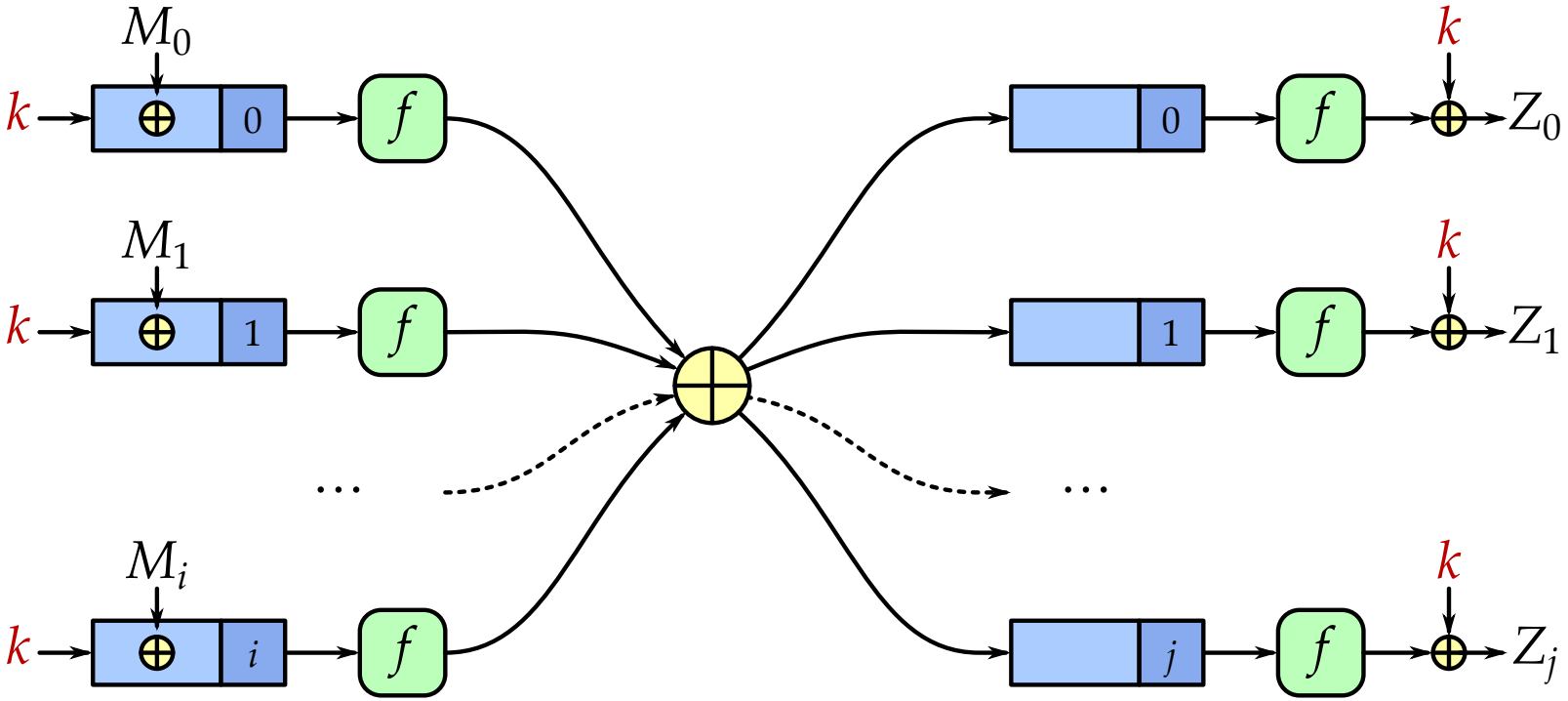
$L_0 \leftarrow L_0 + H_k(R \circ 1)$ (L_0 the first $\min(b, |L|)$ bits of L)

$C \leftarrow L||R$

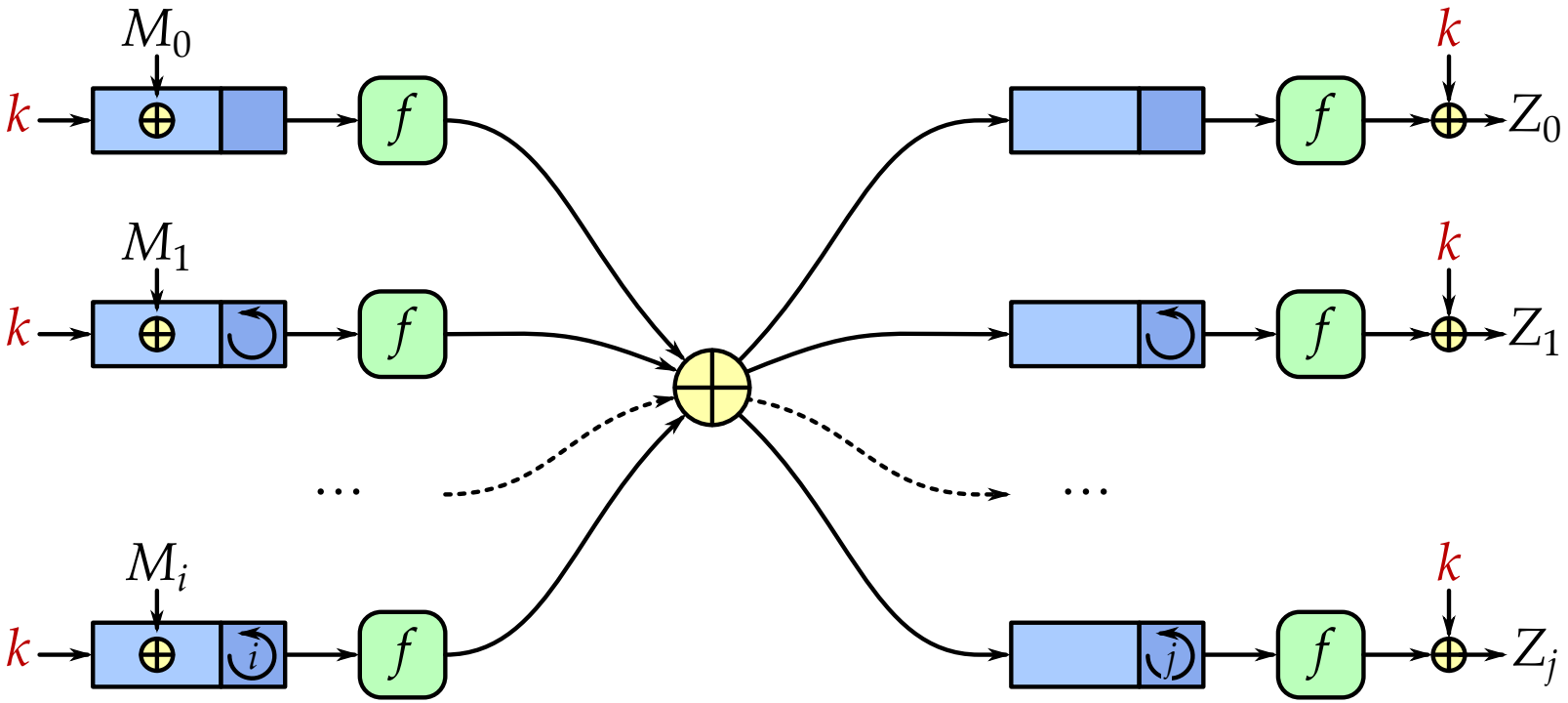
return ciphertext $C \in \mathbb{Z}_2^{|P|}$

Outline

A first attempt



Far + Falle



Farfalle-PRF

- **Key schedule:**

$$K \in \mathbb{Z}_2^* \quad \text{gets mapped to} \quad k \leftarrow H_{0^b}(K)$$

- **Then:**

$$F_k(M^{(m-1)} \circ \cdots \circ M^{(1)} \circ M^{(0)}, n)$$

with **Far:** $H_k(\cdot)$ – **Farfalle:** $F_k(\cdot)$

Outline

The caracolle rolling function

- LFSR on last e bits of the state

$$\text{caracolle}(k, i) = \left(k(x) \times x^i\right) \bmod p(x)$$

- Goal: avoid affine spaces of high dimension

How long before an affine space appears?

$$L_{\min}(p(x), d) = \min_n \ : \ \{\text{caracolle}(k, i) | 0 \leq i < n\} \supset \text{affine dim. } d$$

d	2	3	4	5	6	7
$e = 13$, est.	$2^{5.2}$	$2^{8.5}$	$2^{10.5}$	$2^{11.7}$	$2^{12.3}$	$2^{12.7}$
$e = 13$, meas.	$2^{5.5}$	$2^{8.5}$	$2^{10.5}$	$2^{11.6}$	-	-
$e = 17$, est.	$2^{6.5}$	$2^{10.8}$	$2^{13.4}$	2^{15}	$2^{15.9}$	$2^{16.4}$
$e = 17$, meas.	$2^{6.9}$	$2^{10.4}$	$2^{13.3}$	-	-	-
$e = 29$, est.	$2^{10.5}$	$2^{17.6}$	$2^{22.2}$	2^{25}	$2^{26.8}$	$2^{27.8}$
$e = 29$, meas.	$2^{10.2}$	$2^{17.4}$	-	-	-	-
$e = 61$, est.	$2^{21.2}$	2^{36}	$2^{45.7}$	2^{52}	$2^{55.7}$	2^{58}
$e = 61$, meas.	$> 2^{20.0}$	-	-	-	-	-

$$e = \deg(p(x))$$

Outline

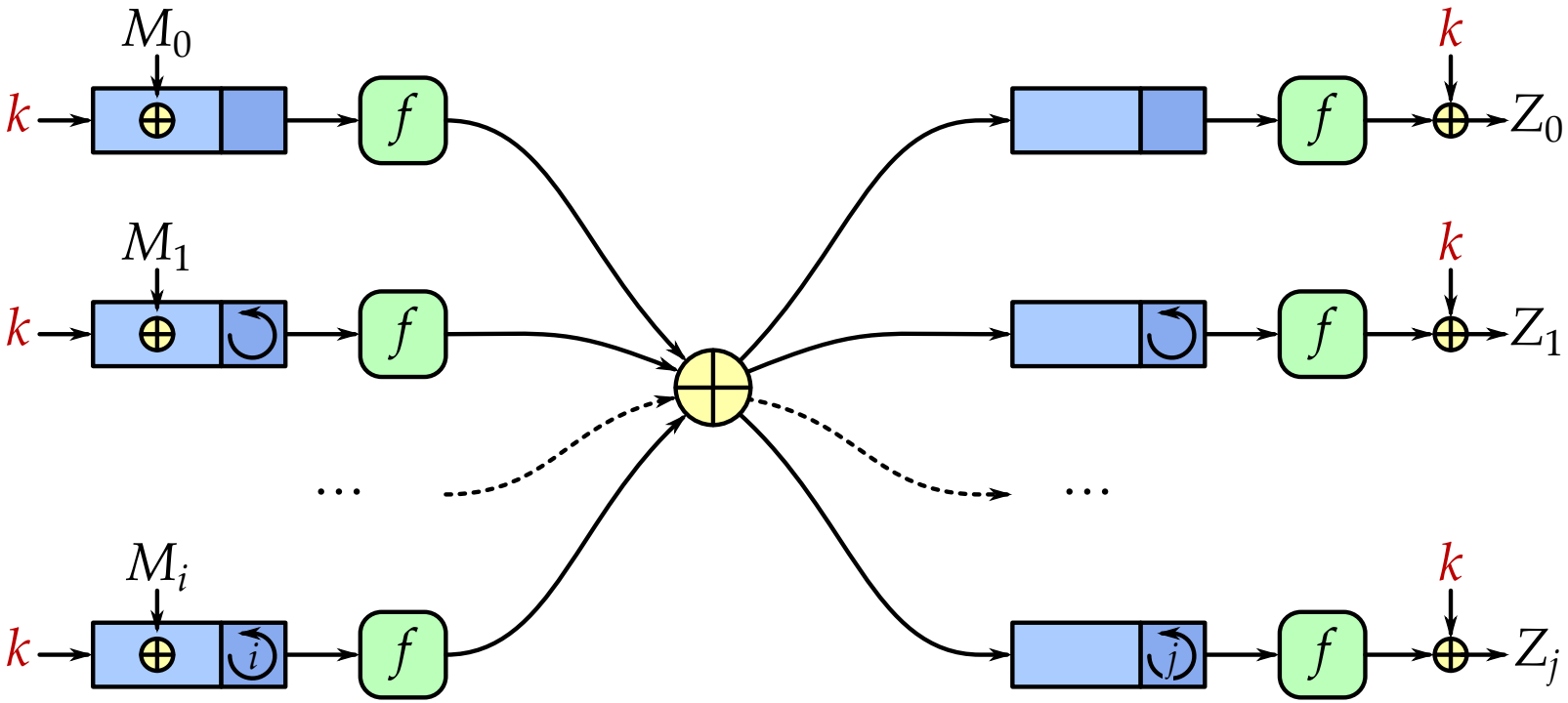
Kravatte = Farfalle with Keccak-p

- $f = \text{Keccak-}p[1600, n_r = 6]$
- $r = 1536$ bits
- caracolle(k, i) with dense $p(x)$ of degree 61
- $i < 2^{56}$
- Target security: 128 bits (claimed capacity of 256 bits)

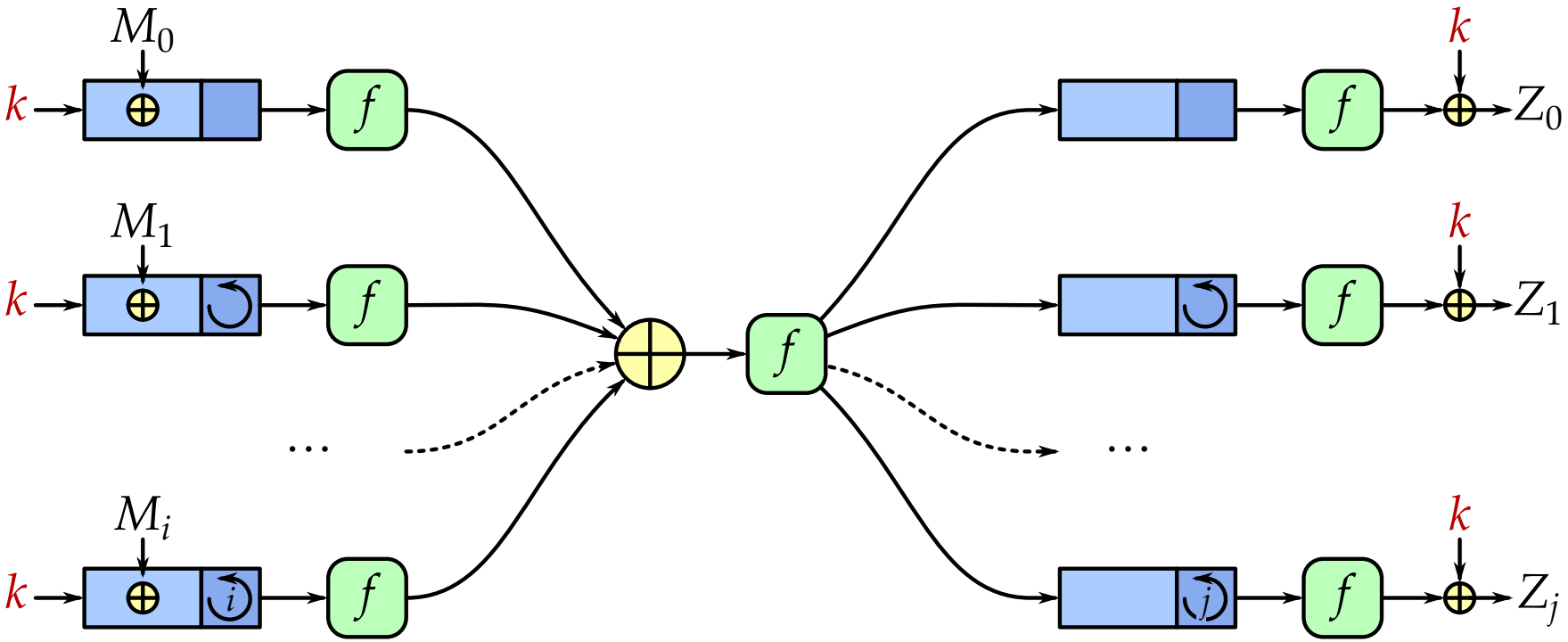
But...

Outline

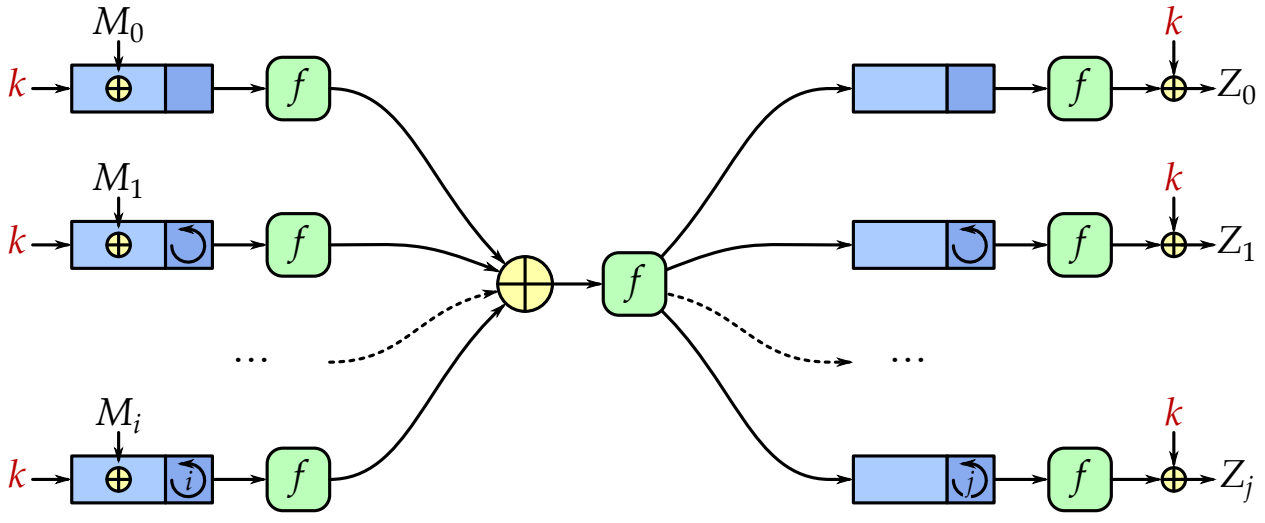
Far + Falle



Far ++ Falle (work in progress)



Plan for KRAVATTE



$$f_{\text{Far}} = \text{KECCAK-}p[1600, n_r = 6]$$
$$f_{\text{f}} = \text{KECCAK-}p[1600, n_r = 4]$$
$$f_{\text{alle}} = \text{KECCAK-}p[1600, n_r = 4]$$

Thanks for your attention!

See

IACR ePrint **2016/1188**

for more details and references.