Farfalle: parallel permutation-based cryptography

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

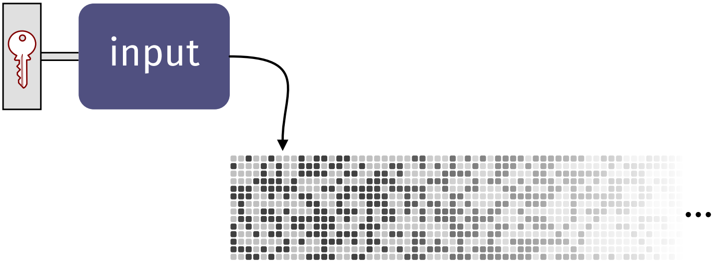
[1]STMicroelectronics
[2]Radboud University

Fast Software Encryption
Bruges, Belgium, March 2018

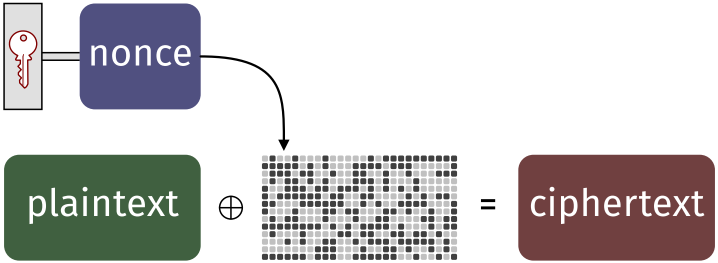
Outline

Outline

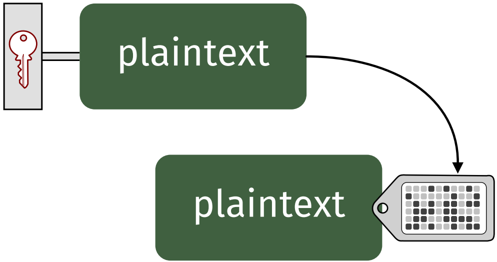
Pseudo-random function (PRF)



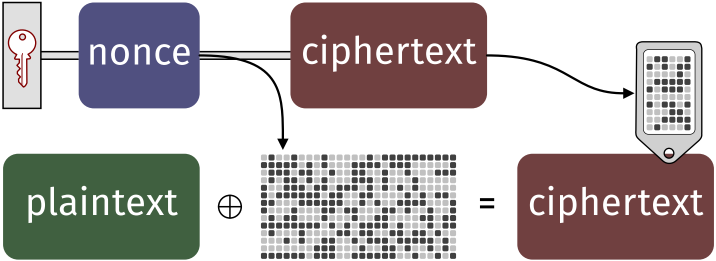
Stream cipher



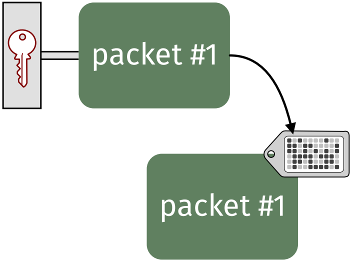
Message authentication code (MAC)



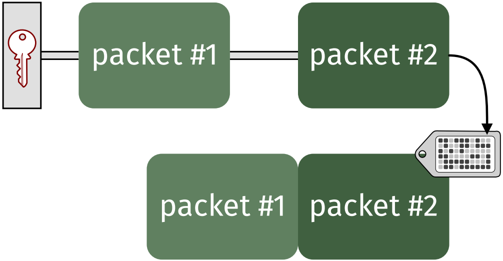
Authenticated encryption



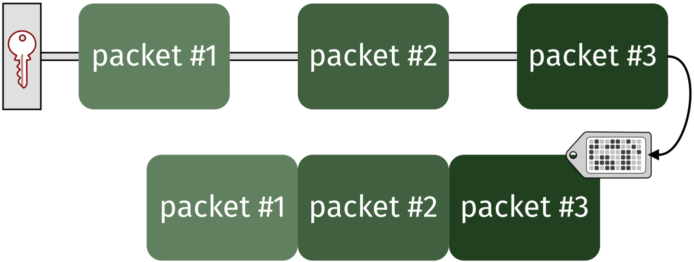
Incrementality



Incrementality

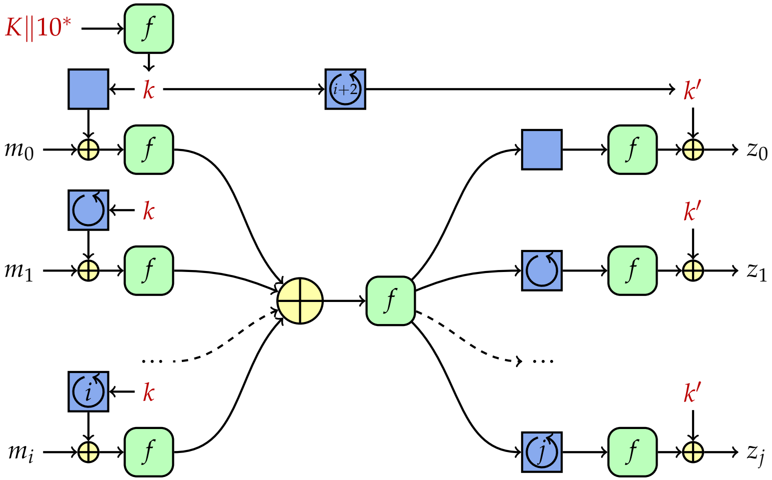


Incrementality

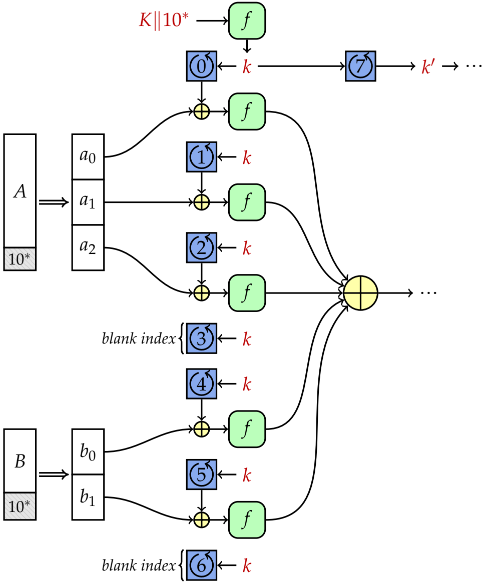


Outline

Farfalle



Multi-string input and incrementality



Outline

Kravatte = Farfalle with Keccak-p

- $f = \text{Keccak-}p[1600, n_r = 6]$
- roll_c: simple linear function on 5×64 bits
- roll_e: simple non-linear function on 10×64 bits
- Target security: ≥ 128 bits (including post-quantum)

KRAVATTE performance

KRAVATTE		
mask derivation	475	cycles
less than 200 bytes	1240	cycles
MAC computation use case:		
long inputs	0.58	cycles/byte
Stream encryption use case:		
long outputs	0.59	cycles/byte
AES-128 counter mode	0.54	cycles/byte
AES-256 counter mode	0.77	cycles/byte

Intel® Core™ i5-6500 (Skylake), single core

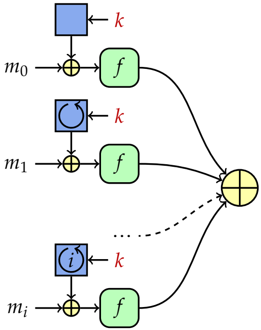
Kravatte modes

Kravatte session-based AE		
long metadata	0.61	cycles/byte
long plaintexts	1.39	cycles/byte
Kravatte-SIV		
long plaintexts	1.43	cycles/byte
Kravatte tweakable wide block cipher		
long block lengths	2.10	cycles/byte

Intel® Core™ i5-6500 (Skylake), single core

Outline

Using one or two blocks



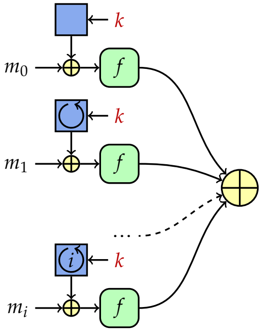
One block: find $f(m_i + \mathrm{roll}_c^i(k)) = 0$

- Equivalent to recovering k

Two blocks: find $m_i + \mathrm{roll}_c^i(k) = m_{i+1} + \mathrm{roll}_c^{i+1}(k)$

- Being able to predict $k + \mathrm{roll}_c^\delta(k)$

Using one or two blocks



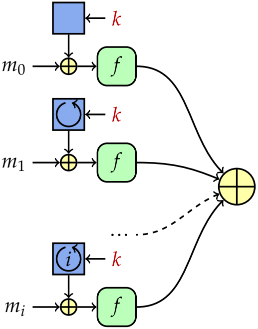
One block: find $f(m_i + \mathrm{roll}_c^i(k)) = 0$

- Equivalent to recovering k

Two blocks: find $m_i + \mathrm{roll}_c^i(k) = m_{i+1} + \mathrm{roll}_c^{i+1}(k)$

- Being able to predict $k + \mathrm{roll}_c^\delta(k)$

Using one or two blocks



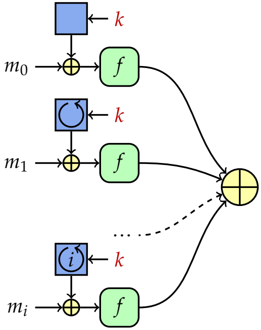
One block: find $f(m_i + \mathrm{roll}_c^i(k)) = 0$

- Equivalent to recovering k

Two blocks: find $m_i + \mathrm{roll}_c^i(k) = m_{i+1} + \mathrm{roll}_c^{i+1}(k)$

- Being able to predict $k + \mathrm{roll}_c^{\delta}(k)$

Using more blocks: affine spaces



Affine space: find

$$\left\{\mathrm{roll}_c^i(k)\right\}_{i\in I} = \mathrm{offset} + \langle \mathrm{basis} \rangle$$

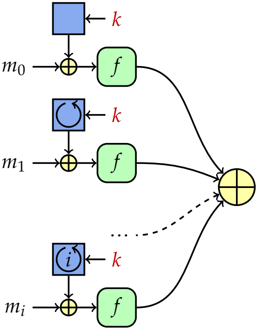
then

$$\sum_i f(m + \mathrm{roll}_c^i(k)) = \Delta^{\mathrm{HO}} f(m)$$

So we studied

$$\min_n : \{\mathrm{roll}_c^i(k) | 0 \le i < n\} \supset \text{affine dim. } d$$

Using more blocks: affine spaces



Affine space: find

$$\left\{\mathrm{roll}_c^i(k)\right\}_{i\in I} = \mathrm{offset} + \langle \mathrm{basis} \rangle$$

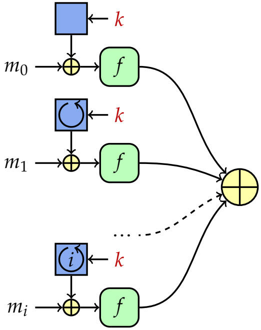
then

$$\sum_i f(m + \mathrm{roll}_c^i(k)) = \Delta^{\mathrm{HO}} f(m)$$

So we studied

$$\min_n \; : \; \{\mathrm{roll}_c^i(k) | 0 \le i < n\} \supset \text{affine dim. } d$$

Using more blocks: affine spaces



Affine space: find

$$\left\{\mathrm{roll}_c^i(k)\right\}_{i\in I} = \mathrm{offset} + \langle \mathrm{basis}\rangle$$

then

$$\sum_i f(m + \mathrm{roll}_c^i(k)) = \Delta^{\mathrm{HO}} f(m)$$

So we studied

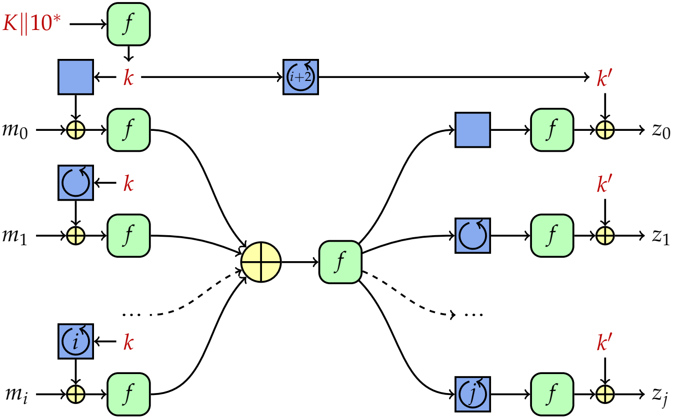
$$\min_n \ : \ \{\mathrm{roll}_c^i(k) | 0 \leq i < n\} \supset \text{affine dim. } d$$

Outline

Expanding the expansion of KRAVATTE

- December 2016: **KRAVATTE initial release**
  - $0 + 6$ rounds in the expansion
  - roll_e linear on 5×64 bits

Simple input structure



$$M = m_0^{0/1} || m_1^{0/1} || \ldots || m_i^{0/1}$$

Expanding the expansion of KRAVATTE

- December 2016: **KRAVATTE initial release**
  - $0 + 6$ rounds in the expansion
  - roll_e linear on 5×64 bits
- July 2017: **KRAVATTE 6644** with $4 + 4$ rounds
- October 2017: contacts with Colin Chaigneau, Thomas Fuhr, Henri Gilbert, Jian Guo, Jérémy Jean, Jean-René Reinhard and Ling Song
  - still susceptible to HO diff. attacks [Guo and Song, ePrint 2017/1026]
  - algebraic attacks, even if increased to $6 + 6$ rounds [This afternoon!]
- December 2017: **KRAVATTE Achouffe**
  - increased to $6 + 6$ rounds
  - roll_e extended to 10×64 bits and becomes non-linear

Expanding the expansion of KRAVATTE

- December 2016: **KRAVATTE initial release**
  - $0 + 6$ rounds in the expansion
  - roll_e linear on 5×64 bits
- July 2017: **KRAVATTE 6644** with $4 + 4$ rounds
- October 2017: contacts with Colin Chaigneau, Thomas Fuhr, Henri Gilbert, Jian Guo, Jérémy Jean, Jean-René Reinhard and Ling Song
  - still susceptible to HO diff. attacks [Guo and Song, ePrint 2017/1026]
  - algebraic attacks, even if increased to $6 + 6$ rounds [This afternoon!]
- December 2017: **KRAVATTE Achouffe**
  - increased to $6 + 6$ rounds
  - roll_e extended to 10×64 bits and becomes non-linear

Expanding the expansion of KRAVATTE

- December 2016: **KRAVATTE initial release**
  - $0 + 6$ rounds in the expansion
  - roll_e linear on 5×64 bits
- July 2017: **KRAVATTE 6644** with $4 + 4$ rounds
- October 2017: contacts with Colin Chaigneau, Thomas Fuhr, Henri Gilbert, Jian Guo, Jérémy Jean, Jean-René Reinhard and Ling Song
  - still susceptible to HO diff. attacks [Guo and Song, ePrint 2017/1026]
  - algebraic attacks, even if increased to $6 + 6$ rounds [This afternoon!]
- December 2017: **KRAVATTE Achouffe**
  - increased to $6 + 6$ rounds
  - roll_e extended to 10×64 bits and becomes non-linear

Expanding the expansion of KRAVATTE

- December 2016: **KRAVATTE initial release**
  - $0 + 6$ rounds in the expansion
  - roll_e linear on 5×64 bits
- July 2017: **KRAVATTE 6644** with $4 + 4$ rounds
- October 2017: contacts with Colin Chaigneau, Thomas Fuhr, Henri Gilbert, Jian Guo, Jérémy Jean, Jean-René Reinhard and Ling Song
  - still susceptible to HO diff. attacks [Guo and Song, ePrint 2017/1026]
  - algebraic attacks, even if increased to $6 + 6$ rounds [This afternoon!]
- December 2017: **KRAVATTE Achouffe**
  - increased to $6 + 6$ rounds
  - roll_e extended to 10×64 bits and becomes non-linear

Any questions?

Thanks for your attention!

Q?

Backup slides

Backup slides

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

Using differential trails in KRAVATTE

$$\Delta \xrightarrow{\chi\circ\pi\circ\rho\circ\theta} q_1 \xrightarrow{\chi\circ\pi\circ\rho\circ\theta} q_2 \xrightarrow{\chi\circ\pi\circ\rho\circ\theta} q_3 \xrightarrow{\chi\circ\pi\circ\rho\circ\theta} q_4 \xrightarrow{\chi\circ\pi\circ\rho\circ\theta} q_5 \xrightarrow{\chi\circ\pi\circ\rho\circ\theta} \gamma$$

$$\mathrm{Pr}(\mathrm{collision}) = \sum_{\gamma} \mathrm{DP}(\Delta, \gamma)\mathrm{DP}(\Delta', \gamma)$$

Using differential trails in KRAVATTE

$$\Delta \xrightarrow{\chi\circ\pi\circ\rho\circ\theta} q_1 \xrightarrow{\chi\circ\pi\circ\rho\circ\theta} q_2 \xrightarrow{\chi\circ\pi\circ\rho\circ\theta} q_3 \xrightarrow{\chi\circ\pi\circ\rho\circ\theta} q_4 \xrightarrow{\chi\circ\pi\circ\rho\circ\theta} q_5 \xrightarrow{\chi\circ\pi\circ\rho\circ\theta} \gamma$$

$$\mathrm{Pr}(\mathrm{collision}) = \sum_{\gamma} \mathrm{DP}^2(\Delta, \gamma)$$

Using differential trails in KRAVATTE

$$\Delta \xrightarrow{\chi\circ\pi\circ\rho\circ\theta} q_1 \xrightarrow{\chi\circ\pi\circ\rho\circ\theta} q_2 \xrightarrow{\chi\circ\pi\circ\rho\circ\theta} q_3 \xrightarrow{\chi\circ\pi\circ\rho\circ\theta} q_4 \xrightarrow{\chi\circ\pi\circ\rho\circ\theta} q_5 \xrightarrow{\chi\circ\pi\circ\rho\circ\theta} \gamma$$

$$\begin{aligned}\Pr(\text{collision}) &= \sum_{\gamma} \mathrm{DP}^2(\Delta, \gamma) \\ &\approx \sum_{\gamma} 2^{-2\mathrm{w}(6\text{ rounds})}\end{aligned}$$

Using differential trails in KRAVATTE

$$\Delta \xrightarrow{\chi\circ\pi\circ\rho\circ\theta} q_1 \xrightarrow{\chi\circ\pi\circ\rho\circ\theta} q_2 \xrightarrow{\chi\circ\pi\circ\rho\circ\theta} q_3 \xrightarrow{\chi\circ\pi\circ\rho\circ\theta} q_4 \xrightarrow{\chi\circ\pi\circ\rho\circ\theta} q_5 \xrightarrow{\chi\circ\pi\circ\rho\circ\theta} \gamma$$

$$\begin{aligned}\Pr(\text{collision}) &= \sum_{\gamma} \mathrm{DP}^2(\Delta, \gamma) \\ &\approx \sum_{\gamma} 2^{-2\mathrm{w}(\text{6 rounds})} \\ &= 2^{\mathrm{w}(q_5)} 2^{-2\mathrm{w}(\text{6 rounds})}\end{aligned}$$

Using differential trails in KRAVATTE

$$\Delta \xrightarrow{\chi\circ\pi\circ\rho\circ\theta} q_1 \xrightarrow{\chi\circ\pi\circ\rho\circ\theta} q_2 \xrightarrow{\chi\circ\pi\circ\rho\circ\theta} q_3 \xrightarrow{\chi\circ\pi\circ\rho\circ\theta} q_4 \xrightarrow{\chi\circ\pi\circ\rho\circ\theta} q_5 \xrightarrow{\chi\circ\pi\circ\rho\circ\theta} \gamma$$

$$\begin{aligned}\Pr(\text{collision}) &= \sum_\gamma \mathrm{DP}^2(\Delta,\gamma)\\ &\approx \sum_\gamma 2^{-2\mathrm{w}(6\text{ rounds})}\\ &= 2^{\mathrm{w}(q_5)}2^{-2\mathrm{w}(6\text{ rounds})}\\ &= 2^{-\mathrm{w}(5\text{ rounds})-\mathrm{w}(6\text{ rounds})}\end{aligned}$$

Using differential trails in KRAVATTE

$$\Delta \xrightarrow{\chi\circ\pi\circ\rho\circ\theta} q_1 \xrightarrow{\chi\circ\pi\circ\rho\circ\theta} q_2 \xrightarrow{\chi\circ\pi\circ\rho\circ\theta} q_3 \xrightarrow{\chi\circ\pi\circ\rho\circ\theta} q_4 \xrightarrow{\chi\circ\pi\circ\rho\circ\theta} q_5 \xrightarrow{\chi\circ\pi\circ\rho\circ\theta} \gamma$$

$$\begin{aligned}
\Pr(\text{collision}) &= \sum_\gamma \mathrm{DP}^2(\Delta, \gamma) \\
&\approx \sum_\gamma 2^{-2\mathrm{w}(6 \text{ rounds})} \\
&= 2^{\mathrm{w}(q_5)} 2^{-2\mathrm{w}(6 \text{ rounds})} \\
&= 2^{-\mathrm{w}(5 \text{ rounds}) - \mathrm{w}(6 \text{ rounds})} \\
&\leq 2^{-50-92} = 2^{-142} \qquad \text{[Mella et al., FSE 2017]}
\end{aligned}$$

Using differential trails in KRAVATTE

$$\Delta \quad \rightarrow q_1 \quad \rightarrow \cdots \rightarrow q_5 \quad \rightarrow \gamma$$

With n inputs and only the first trail:

$$\Pr(\text{collision}) \leq \frac{n}{2} 2^{-142} = n 2^{-143}$$

With n inputs and a structure with 64 times more pairs:

$$\Pr(\text{collision}) \leq 64 \times \frac{n}{2} 2^{-142} = n 2^{-137}$$

Using differential trails in KRAVATTE

$$\begin{array}{l} \Delta \qquad\quad \to q_1 \qquad\quad \to \cdots \to q_5 \qquad\quad \to \gamma \\ \Delta \lll z \to q_1 \lll z \to \cdots \to q_5 \lll z \to \gamma \lll z \end{array}$$

With n inputs and only the first trail:

$$\Pr(\text{collision}) \leq \frac{n}{2} 2^{-142} = n2^{-143}$$

With n inputs and a structure with 64 times more pairs:

$$\Pr(\text{collision}) \leq 64 \times \frac{n}{2} 2^{-142} = n2^{-137}$$