# Key-Recovery Attacks on Full Kravatte

Colin Chaigneau[1], Thomas Fuhr[2], Henri Gilbert[1,2], Jian Guo[3], Jérémy Jean[2], Jean-René Reinhard[2], Ling Song[3,4]

[1]Université de Versailles, Saint-Quentin-en-Yvelines, France
[2]Agence nationale de la sécurité des systèmes d'information, France
[3]Nanyang Technological University, Singapore
[4]Institute of Information Engineering, Chinese Academy of Sciences, China

FSE 2018 – March 5, 2018

# Farfalle and Kravatte

## Farfalle constuction [BDH+]

- Parallelizable permutation-based PRF of variable input and output length
- Can be used
  - Directly as a MAC, a stream cipher, a KDF
  - Through a mode: as a AEAD, a block cipher of variable block length

## Kravatte: Keccak based instantiation

- Several versions
  - **ePrint**, published on IACR ePrint in July 2017 [2016/1188]
  - **ECC**, outlined at ECC 2017 in November 2017
  - FSE, patched version presented this morning

## Security claim

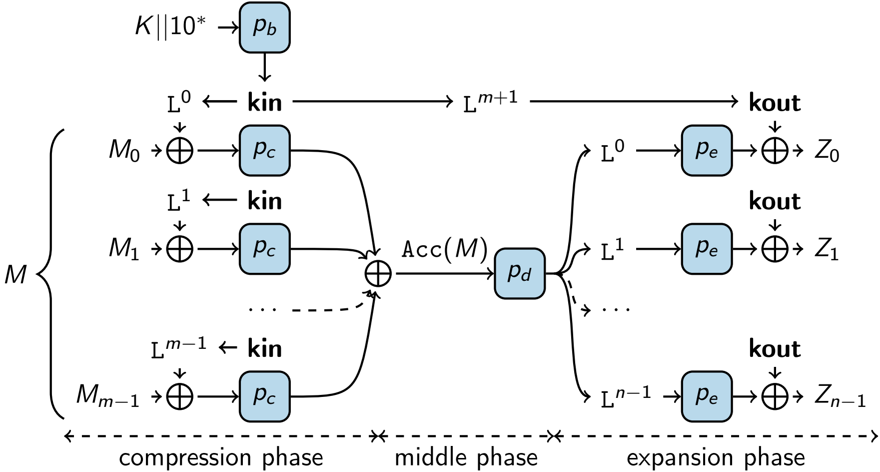
256 bits when $|\text{input} + \text{output blocks}| < 2^{137}$

## Kravatte in a nutshell

**Targeted** Kravatte **properties**

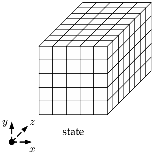
- $p_x$: $r_x$ rounds of `Keccak`-$p$
- Rolling function `L`: linear permutation

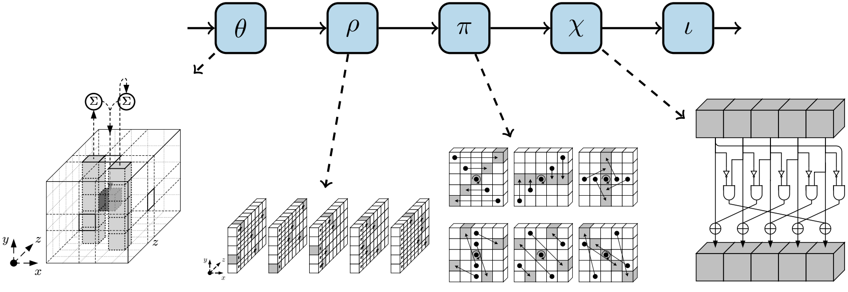
| version | $r_b, r_c, r_d, r_e$ |
|---|---|
| ePrint | 6, 6, 4, 4 |
| ECC | 6, 6, 6, 6 |



# Reminder: the Keccak-$p$ round function

- Keccak-$p$ state: $5 \times 5 \times 64 = 1600$ bits




linear

linear

linear

non-linear
$\deg(\chi) = 2$
$\deg(\chi^{-1}) = 3$

source of the state, $\theta$, $\rho$, $\pi$, $\chi$ figures: `https://keccak.team/figures.html`

# Outline of our key-recovery attacks

## One attack abusing a property of the compression phase

- Higher order differential attack **(HO)**

## Two attacks on the expansion phase of Kravatte

- Meet-in-the-middle algebraic attack **(MITM)**
- Linear recurrence attack **(LR)**

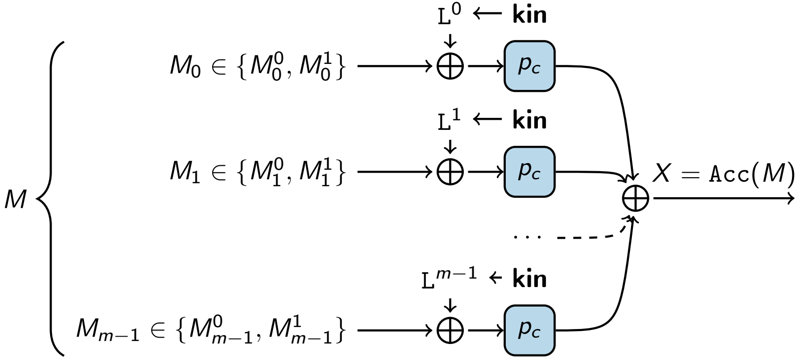
| Attack | version | T | D | M |
|---|---|---|---|---|
| HO | ePrint | $2^{112}$ | $2^{74}$ | $2^{62}$ |
| MITM | ePrint | $2^{115}$ | $2^{28}$ | $2^{76}$ |
| **LR** | **ePrint** | $\mathbf{2^{65}}$ | $\mathbf{2^{51}}$ | $\mathbf{2^{51}}$ |
| **LR** | **ECC** | $\mathbf{2^{134}}$ | $\mathbf{2^{88}}$ | $\mathbf{2^{88}}$ |

# Higher order differential attack

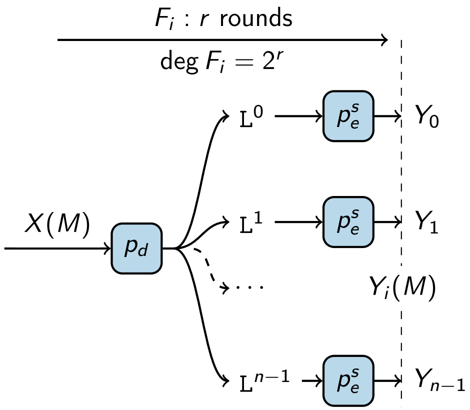
# Main observation

## Building an affine space of accumulator values

- Denote by $\mathcal{S}$ the following structure of $2^m$ $m$-block plaintexts
$$\mathcal{S} = \{M_0^0, M_0^1\} \times \{M_1^0, M_1^1\} \times \ldots \times \{M_{m-1}^0, M_{m-1}^1\}.$$
- $\texttt{Acc}(\mathcal{S})$ is an affine subspace of $\{0,1\}^b$
- if $m \lll b$, $\dim(\texttt{Acc}(\mathcal{S})) = m$ with overwhelming probability



# HO distinguisher



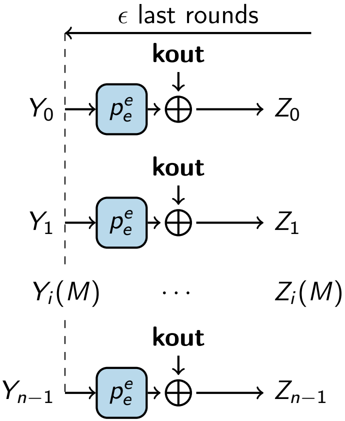

- [Lai94] Summing a function over an affine space of dim. $m \approx$ differentiating $m$ times
- If $m > \deg F_i$, the derivative is 0
- Equation satisfied by $(Y_i(M))_{M \in \mathcal{S}}$ **independently of $\mathbf{k}^{\mathbf{in}}$**

$$m > 2^r \Rightarrow \sum_{X \in \mathtt{Acc}(\mathcal{S})} F_i(X) = \sum_{M \in \mathcal{S}} Y_i(M) = 0$$

# HO attacks

## Last $\epsilon$-round attacks

- Express $Y_i(M)$ as a function of **kout**, and $Z_i(M)$
- For one structure, combine using the HO distinguisher to get equations in **kout**
- Consider outputs long enough to collect enough equations to solve for **kout**



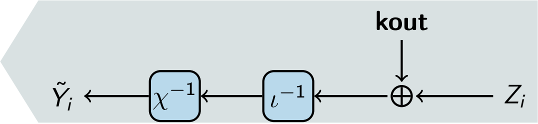

$$\sum_{M \in \mathcal{S}} \texttt{Keccak-}p^{-\epsilon}(\mathbf{kout} \oplus Z_i(M)) = 0$$

# HO attack with one final round ($\epsilon = 1$)

## Attacking Kravatte-**ePrint by local exaustive search**

- $F$ has $4 + 4 - 1 = 7$ `Keccak-`$p$ rounds, $\deg F = 128$
- Using a 129-block structure, we can set up an HO distinguisher
- Note: the linear part of the last round can be ignored
- The system can be solved row-by-row, by exhaustive search
- Each block of equation provides a 5-bit condition on each row of **kout**
- With $n = 2$, most **kout** rows are determined

$$T = D = 2^{129}(129 + 2) \approx 2^{136}$$




## Experimental verification

- Attack tested on a round reduced version of Kravatte

# HO attack with two final rounds ($\epsilon = 2$)

## Attacking Kravatte-ePrint by linearization

- $F$ has $4 + 4 - 2 = 6$ `Keccak-`$p$ rounds, $\deg F = 64$
- Using a 65-block structure, we can set up an HO distinguisher

$$\sum_{M \in \mathcal{S}} \texttt{Keccak-}p^{-2}(\mathbf{kout} \oplus Z_i(M)) = 0$$

- **Linearization** by considering every monomial in **kout** as a fresh variable

**III.** By combination through a degree 3 function, every bit is a LC of
$N_2 = \binom{N_1}{1} + \binom{N_1}{2} + \binom{N_1}{3} \approx 2^{36.5}$
monomials $\lll \binom{1600}{9} \approx 2^{77}$

**I.** For each row, only 20 monomials of degree $\leq 3$ in 5 **kout** variables can be formed by $\chi^{-1}$
Total number of **kout** monomials:
$N_1 = 320 \times 20 = 6400 \approx 2^{13}$

$$\tilde{Y}_i \leftarrow \boxed{\chi^{-1}} \leftarrow \boxed{\iota^{-1}} \leftarrow \boxed{\theta^{-1}} \leftarrow \boxed{(\pi \circ \rho)^{-1}} \leftarrow \boxed{\chi^{-1}} \leftarrow \boxed{\iota^{-1}} \leftarrow \overset{\mathbf{kout}}{\oplus} \leftarrow Z_i$$

**II.** Linear diffusion breaks locality: every bit is a LC of up to $N_1$ monomials

# HO attack with two final rounds ($\epsilon = 2$)

## Attacking Kravatte-**ePrint** by linearization

- $F$ has $4 + 4 - 2 = 6$ `Keccak`-$p$ rounds, $\deg F = 64$
- Using a 65-block structure, we can set up an HO distinguisher

$$\sum_{M \in \mathcal{S}} \texttt{Keccak-}p^{-2}(\mathbf{kout} \oplus Z_i(M)) = 0$$

- **Linearization** by considering every monomial in **kout** as a fresh variable
- Complexity: $T = 2^{138}$, $D = 2^{90}$

**III.** By combination through a degree 3 function, every bit is a LC of
$N_2 = \binom{N_1}{1} + \binom{N_1}{2} + \binom{N_1}{3} \approx 2^{36.5}$
monomials $\lll \binom{1600}{9} \approx 2^{77}$

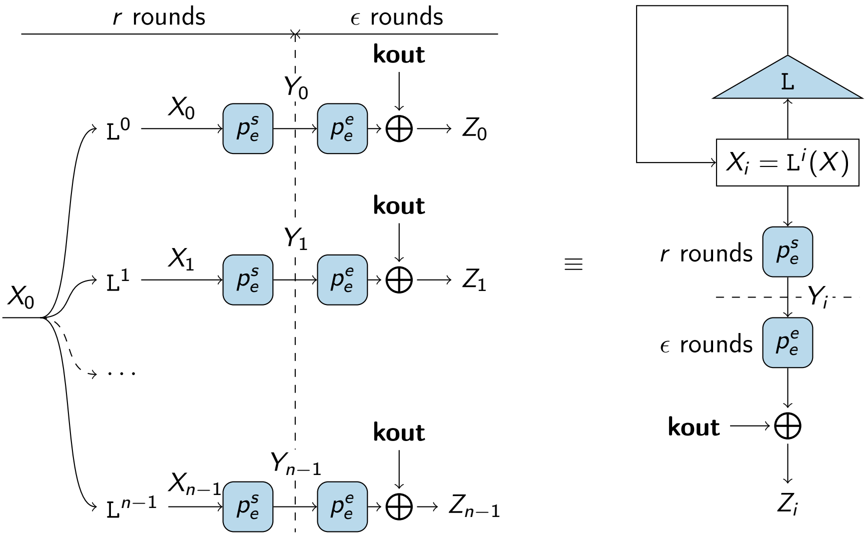
**I.** For each row, only 20 monomials of degree $\leq 3$ in 5 **kout** variables can be formed by $\chi^{-1}$
Total number of **kout** monomials:
$N_1 = 320 \times 20 = 6400 \approx 2^{13}$

$$\tilde{Y}_i \leftarrow \boxed{\chi^{-1}} \leftarrow \boxed{\iota^{-1}} \leftarrow \boxed{\theta^{-1}} \leftarrow \boxed{(\pi \circ \rho)^{-1}} \leftarrow \boxed{\chi^{-1}} \leftarrow \boxed{\iota^{-1}} \leftarrow \overset{\mathbf{kout}}{\oplus} \leftarrow Z_i$$

**II.** Linear diffusion breaks locality: every bit is a LC of up to $N_1$ monomials

# Expansion phase attacks

# Expansion phase seen as a stream cipher



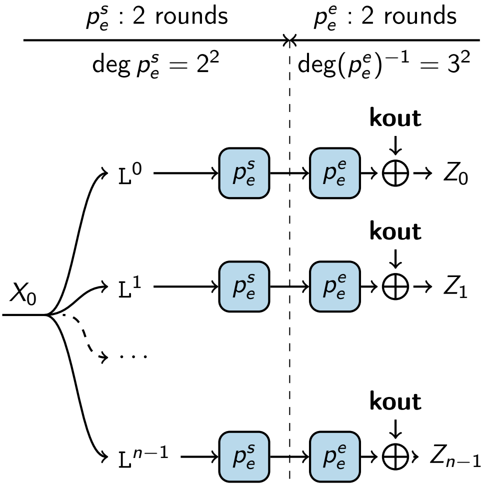
# MITM attack on Kravatte-ePrint

## Linearization

- **Unknowns**: the initial rolling state $X_0$ and **kout**
- Form equations by equating the expressions of $Y_i$ as a function of $X_0$ and as a function of **kout**
- Collect equations and solve

## Complexity

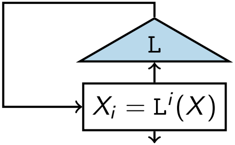
- # of monomials $N \approx 2^{38}$
- $D = N/1600 \approx 2^{28}$
- $T \approx T_{\text{solve}} = N^3 \approx 2^{115}$




$$\texttt{Keccak-}p^2(\mathrm{L}^i(X_0)) = \texttt{Keccak-}p^{-2}(\textbf{kout} + Z_i)$$

# Linear recurrence distinguisher

- Use filtered LFSR cryptanalysis techniques from [Key76, RH07, RGH07]




## Linear recurrence of the rolling state

- The rolling state is updated linearly

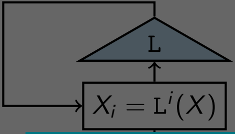
$$X_{i+1} = LX_i$$

- It is a linear recurrence sequence

$$\begin{aligned} (P.X)_i &= \textstyle\sum_j a_j X_{i+j} \\ &= \textstyle\sum_j a_j L^{i+j} X_0 \\ &= (L^i P(L)) X_0 \\ &= 0 \text{ if } P(L) = 0 \end{aligned}$$

# Linear recurrence distinguisher

- Use filtered LFSR cryptanalysis techniques from [Key76, RH07, RGH07]




**Linear recurrence of the rolling state**

**Reminder: Linear recurrence sequence**

- Consider a polynomial $P(x) = \sum_j a_j x^j$, and a sequence $u = (u_i)$
- $(P.u)$ is a sequence obtained by the action of $P$ on $u$

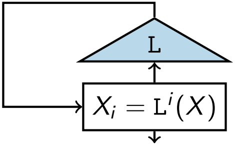
$$(P.u)_i = \sum_j a_j u_{i+j}.$$

- $P$ annihilates $u$ if $P.u = 0$, $u$ is a linear recurrence sequence

$= \quad 0 \text{ if } P(L) = 0$

# Linear recurrence distinguisher

- Use filtered LFSR cryptanalysis techniques from [Key76, RH07, RGH07]



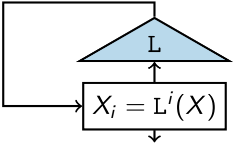

## Linear recurrence of the rolling state

- The rolling state is updated linearly
$$X_{i+1} = LX_i$$
- It is a linear recurrence sequence

$$\begin{aligned}(P.X)_i &= \textstyle\sum_j a_j X_{i+j} \\ &= \textstyle\sum_j a_j L^{i+j} X_0 \\ &= (L^i P(L)) X_0 \\ &= 0 \text{ if } P(L) = 0\end{aligned}$$

# Linear recurrence distinguisher

- Use filtered LFSR cryptanalysis techniques from [Key76, RH07, RGH07]

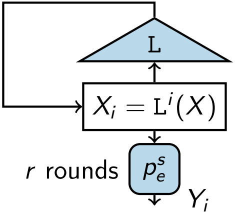



## Linear recurrence of the rolling state

- The rolling state is updated linearly
$$X_{i+1} = LX_i$$
- It is a linear recurrence sequence, **as is any LC $w$ of its components**
$$\begin{aligned}(P.w^T X)_i &= \sum_j a_j w^T X_{i+j} \\ &= w^T \sum_j a_j L^{i+j} X_0 \\ &= \ldots \\ &= 0 \text{ if } P(L) = 0\end{aligned}$$

# Linear recurrence distinguisher

- Use filtered LFSR cryptanalysis techniques from [Key76, RH07, RGH07]

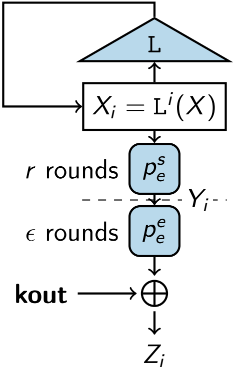



**Case of the filtered linear register**

- The **monomial state** $X^{\leq d}$: vector of monomials of deg $\leq d = 2^r$
- The monomial state is updated linearly
$$X_{i+1}^{\leq d} = L_{\leq d} X_i^{\leq d}$$
- It is a linear recurrence sequence, as is any LC $w$ of its components, **thus** $Y$
$$\begin{aligned}(P.Y)_i &= \textstyle\sum_j a_j w_Y^T X_{i+j}^{\leq d} \\ &= \ldots \\ &= 0 \text{ if } P(L_{\leq d}) = 0\end{aligned}$$

# Linear recurrence distinguisher

- Use filtered LFSR cryptanalysis techniques from [Key76, RH07, RGH07]




## Case of the filtered linear register

- The **monomial state** $X^{\leq d}$: vector of monomials of deg $\leq d = 2^r$
- The monomial state is updated linearly
$$X_{i+1}^{\leq d} = L_{\leq d} X_i^{\leq d}$$
- It is a linear recurrence sequence, as is any LC $w$ of its components, **thus** $Y$
$$\begin{aligned}(P.Y)_i &= \textstyle\sum_j a_j w_Y^T X_{i+j}^{\leq d} \\ &= \dots \\ &= 0 \text{ if } P(L_{\leq d}) = 0\end{aligned}$$

## LR attacks

- Reuse last round attack framework from HO attacks, replacing HO distinguiser by LR distinguisher
$$(P^*.\mathtt{Keccak}\text{-}p^{-\epsilon}(\mathbf{kout} \oplus Z))_i = 0$$

# Linear recurrence polynomial for Kravatte

## Determination of $P^*$

- Kravatte rolling function **only affects 320 bits of the state**
- Restricted update matrix $M$, corresponding monomial update matrix $M_{\leq d}$
- $P_{M_{\leq d}}$ cancels the sequences of all monomials involving the last plane
- The other monomials are constant and cancelled by $x+1$
- $P^* = (x+1)P_{M_{\leq d}}$, deg $P^*$: $\#$ monomials of deg $\leq d$ in 320 variables

## Computation of $P^*$

- Considering $\alpha = x \mod P_M \in GF(2^{320})$,
$$P^* = \prod_{k:HW(k)\leq d} (X + \alpha^k)$$
- Can be computed in time $T_P$ quasilinear in deg $P^*$, using fast polynom multiplication [Sch77]

| $r$ | deg $P^*$ | $T_P$ |
|---|---|---|
| 2 | $2^{28}$ | $2^{40}$ |
| 3 | $2^{51}$ | $2^{65}$ |
| 4 | $2^{88}$ | $2^{104}$ |

Verified for $r = 2$

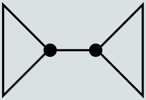
| version | $r+\epsilon$ | $T$ | $D \approx$ deg $P^*$ | $M \approx$ deg $P^*$ |
|---|---|---|---|---|
| ePrint | 3+1 | $2^{65}$ | $2^{51}$ | $2^{51}$ |
| ECC | 4+2 | $2^{134}$ | $2^{88}$ | $2^{88}$ |

# Concluding remarks

| Attack | version | T | D | M |
|---|---|---|---|---|
| HO | ePrint | $2^{112}$ | $2^{74}$ | $2^{62}$ |
| MITM | ePrint | $2^{115}$ | $2^{28}$ | $2^{76}$ |
| **LR** | **ePrint** | $\mathbf{2^{65}}$ | $\mathbf{2^{51}}$ | $\mathbf{2^{51}}$ |
| **LR** | **ECC** | $\mathbf{2^{134}}$ | $\mathbf{2^{88}}$ | $\mathbf{2^{88}}$ |

## Properties leveraged by the attacks

- Low algebraic degree of $\chi$ and $\chi^{-1}$
- Ability to bypass a part of the construction to focus on a reduced number of rounds
- Special points in the `Farfalle` construction
  - The convergence point [HO]
  - The divergence point [MITM, LR]



## Tweaked version of Kravatte (FSE 2018)

- Resisting HO: increase the number of rounds to 6 (versus ePrint version)
- Resisting LR: make the rolling function in expansion phase **non-linear**