Cryptanalysis of the FLIP Family of Stream Ciphers

FSE 2016 rump session

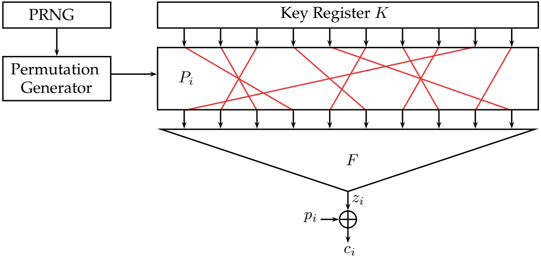
Sébastien Duval, Virginie Lallemand, Yann Rotella

Inria Paris, France

March 22, 2016

The FLIP Family of Stream Ciphers

Pierrick Méaux, Anthony Journault, François-Xavier Standaert and Claude Carlet,
Towards Stream Ciphers for Efficient FHE with Low-Noise Ciphertexts,
EUROCRYPT 2016.



- **Constant** register storing key K (N bits),
- Permutation generator,
- Filtering function F

The Filtering Function F

$$F\ (x_0, .., x_{n_1-1}, x_{n_1}, x_{n_1+1}, .., x_{n_1+n_2-2}, x_{n_1+n_2-1}, x_{n_1+n_2}, x_{n_1+n_2+1}, x_{n_1+n_2+2}, .., x_{n_1+n_2+n_3-k}, .., x_{n_1+n_2+n_3-1})$$

$$\begin{aligned} &= x_0 + \ldots + x_{n_1-1} \\ &+ x_{n_1}x_{n_1+1} + x_{n_1+2}x_{n_1+3} + \ldots + x_{n_1+n_2-2}x_{n_1+n_2-1} \\ &+ x_{n_1+n_2} + x_{n_1+n_2+1}x_{n_1+n_2+2} + \ldots + x_{n_1+n_2+n_3-k} \cdots x_{n_1+n_2+n_3-1} \end{aligned}$$

Preliminary version:

FLIP (n_1, n_2, n_3)	key $(N = n_1 + n_2 + n_3)$	Security	degree (k)
FLIP (47, 40, 105)	192	80	14
FLIP (87, 82, 231)	400	128	21

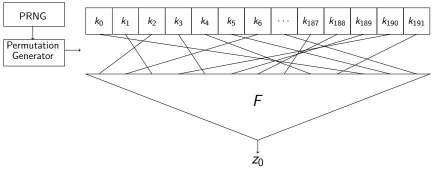
Our Attack

- Known plaintext scenario

Guess-and-determine technique exploiting:

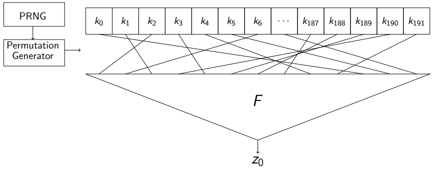
- The **constant** key register
- The **low number** of monomials of degree ≥ 3 in F: $k - 2$

Our Attack



$$z_0 =$$
$$k_{P_0^{-1}(0)} + k_{P_0^{-1}(1)} + k_{P_0^{-1}(2)} + \ldots + k_{P_0^{-1}(45)} + k_{P_0^{-1}(46)} +$$
$$k_{P_0^{-1}(47)} k_{P_0^{-1}(48)} + k_{P_0^{-1}(49)} k_{P_0^{-1}(50)} + \ldots + k_{P_0^{-1}(83)} k_{P_0^{-1}(84)} + k_{P_0^{-1}(85)} k_{P_0^{-1}(86)} +$$
$$k_{P_0^{-1}(87)} + k_{P_0^{-1}(88)} k_{P_0^{-1}(89)} + k_{P_0^{-1}(90)} k_{P_0^{-1}(91)} k_{P_0^{-1}(92)} + \ldots + k_{P_0^{-1}(178)} \cdots k_{P_0^{-1}(191)}$$

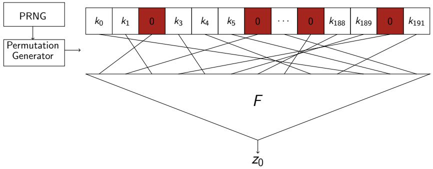
Our Attack



1. Guess $k-2$ null key bit positions

$$
\begin{aligned}
z_0 = \;& k_{P_0^{-1}(0)} + k_{P_0^{-1}(1)} + k_{P_0^{-1}(2)} + \ldots + k_{P_0^{-1}(45)} + k_{P_0^{-1}(46)} + \\
& k_{P_0^{-1}(47)} k_{P_0^{-1}(48)} + k_{P_0^{-1}(49)} k_{P_0^{-1}(50)} + \ldots + k_{P_0^{-1}(83)} k_{P_0^{-1}(84)} + k_{P_0^{-1}(85)} k_{P_0^{-1}(86)} + \\
& k_{P_0^{-1}(87)} + k_{P_0^{-1}(88)} k_{P_0^{-1}(89)} + k_{P_0^{-1}(90)} k_{P_0^{-1}(91)} k_{P_0^{-1}(92)} + \ldots + k_{P_0^{-1}(178)} \cdots k_{P_0^{-1}(191)}
\end{aligned}
$$

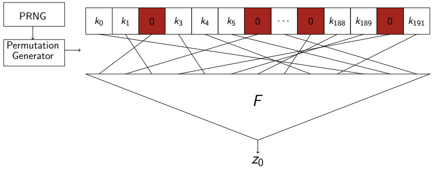
Our Attack



1. Guess $k - 2$ null key bit positions

$$z_0 = k_{P_0^{-1}(0)} + k_{P_0^{-1}(1)} + k_{P_0^{-1}(2)} + \ldots + k_{P_0^{-1}(45)} + k_{P_0^{-1}(46)} + k_{P_0^{-1}(47)} k_{P_0^{-1}(48)} + k_{P_0^{-1}(49)} k_{P_0^{-1}(50)} + \ldots + k_{P_0^{-1}(83)} k_{P_0^{-1}(84)} + k_{P_0^{-1}(85)} k_{P_0^{-1}(86)} + k_{P_0^{-1}(87)} + k_{P_0^{-1}(88)} k_{P_0^{-1}(89)} + k_{P_0^{-1}(90)} k_{P_0^{-1}(91)} k_{P_0^{-1}(92)} + \ldots + k_{P_0^{-1}(178)} \cdots k_{P_0^{-1}(191)}$$

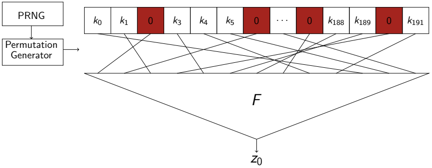
Our Attack



1. Guess $k-2$ null key bit positions
2. Collect quadratic equations

$$z_0 = k_{P_0^{-1}(0)} + k_{P_0^{-1}(1)} + k_{P_0^{-1}(2)} + \dots + k_{P_0^{-1}(45)} + k_{P_0^{-1}(46)} + k_{P_0^{-1}(47)}k_{P_0^{-1}(48)} + k_{P_0^{-1}(49)}k_{P_0^{-1}(50)} + \dots + k_{P_0^{-1}(83)}k_{P_0^{-1}(84)} + k_{P_0^{-1}(85)}k_{P_0^{-1}(86)} + k_{P_0^{-1}(87)} + k_{P_0^{-1}(88)}k_{P_0^{-1}(89)} + k_{P_0^{-1}(90)}k_{P_0^{-1}(91)}k_{P_0^{-1}(92)} + \dots + k_{P_0^{-1}(178)} \cdots k_{P_0^{-1}(191)}$$

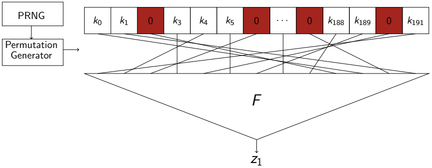
Our Attack



1. Guess $k-2$ null key bit positions
2. Collect quadratic equations

$$z_0 = \cancel{k_{P_0^{-1}(0)}} + \cancel{k_{P_0^{-1}(1)}} + k_{P_0^{-1}(2)} + \dots + k_{P_0^{-1}(45)} + k_{P_0^{-1}(46)} +$$
$$\cancel{k_{P_0^{-1}(47)} k_{P_0^{-1}(48)}} + k_{P_0^{-1}(49)} k_{P_0^{-1}(50)} + \dots + k_{P_0^{-1}(83)} k_{P_0^{-1}(84)} + k_{P_0^{-1}(85)} k_{P_0^{-1}(86)} +$$
$$k_{P_0^{-1}(87)} + \cancel{k_{P_0^{-1}(88)} k_{P_0^{-1}(89)}} + k_{P_0^{-1}(90)} k_{P_0^{-1}(91)} k_{P_0^{-1}(92)} + \dots + k_{P_0^{-1}(178)} \cdots k_{P_0^{-1}(191)}$$

Our Attack



1. Guess $k-2$ null key bit positions
2. Collect quadratic equations

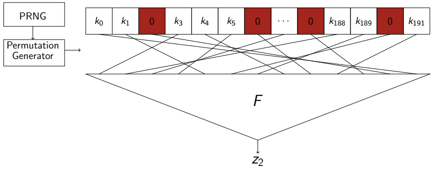
$$z_1 =$$

$$k_{P_1^{-1}(0)} + k_{P_1^{-1}(1)} + k_{P_1^{-1}(2)} + \ldots + k_{P_1^{-1}(45)} + k_{P_1^{-1}(46)} +$$

$$k_{P_1^{-1}(47)}k_{P_1^{-1}(48)} + \cancel{k_{P_1^{-1}(49)}}k_{P_1^{-1}(50)} + \ldots + k_{P_1^{-1}(83)}k_{P_1^{-1}(84)} + \cancel{k_{P_1^{-1}(85)}k_{P_1^{-1}(86)}} +$$

$$\cancel{k_{P_1^{-1}(87)}} + k_{P_1^{-1}(88)}k_{P_1^{-1}(89)} + k_{P_1^{-1}(90)}k_{P_1^{-1}(91)}k_{P_1^{-1}(92)} + \ldots + \cancel{k_{P_1^{-1}(178)} \cdots k_{P_1^{-1}(191)}}$$

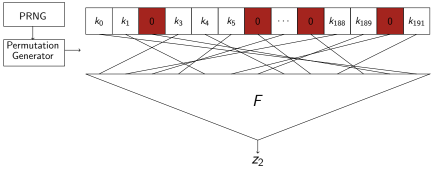
Our Attack



1. Guess $k-2$ null key bit positions
2. Collect quadratic equations

$$z_2 =$$
$$k_{P_2^{-1}(0)} + k_{P_2^{-1}(1)} + k_{P_2^{-1}(2)} + \dots + k_{P_2^{-1}(45)} + k_{P_2^{-1}(46)} +$$
$$k_{P_2^{-1}(47)}k_{P_2^{-1}(48)} + k_{P_2^{-1}(49)}k_{P_2^{-1}(50)} + \dots + k_{P_2^{-1}(83)}k_{P_2^{-1}(84)} + k_{P_2^{-1}(85)}k_{P_2^{-1}(86)} +$$
$$k_{P_2^{-1}(87)} + k_{P_2^{-1}(88)}k_{P_2^{-1}(89)} + \cancel{k_{P_2^{-1}(90)}k_{P_2^{-1}(91)}k_{P_2^{-1}(92)}} + \cancel{\dots} + \cancel{k_{P_2^{-1}(178)} \cdots k_{P_2^{-1}(191)}}$$

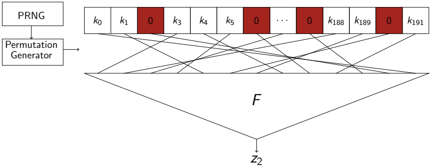
Our Attack



1. Guess $k-2$ null key bit positions
2. Collect quadratic equations
3. Solve the system

$$z_2 = k_{P_2^{-1}(0)} + k_{P_2^{-1}(1)} + k_{P_2^{-1}(2)} + \dots + k_{P_2^{-1}(45)} + k_{P_2^{-1}(46)} +$$
$$k_{P_2^{-1}(47)} k_{P_2^{-1}(48)} + k_{P_2^{-1}(49)} k_{P_2^{-1}(50)} + \dots + k_{P_2^{-1}(83)} k_{P_2^{-1}(84)} + k_{P_2^{-1}(85)} k_{P_2^{-1}(86)} +$$
$$k_{P_2^{-1}(87)} + k_{P_2^{-1}(88)} k_{P_2^{-1}(89)} + \cancel{k_{P_2^{-1}(90)} k_{P_2^{-1}(91)} k_{P_2^{-1}(92)}} + \cancel{\dots} + \cancel{k_{P_2^{-1}(178)} \cdots k_{P_2^{-1}(191)}}$$

Our Attack



1. Guess $k-2$ null key bit positions
2. Collect quadratic equations
3. Solve the system
4. A correct guess gives the key

$$z_2 =$$
$$k_{P_2^{-1}(0)} + k_{P_2^{-1}(1)} + k_{P_2^{-1}(2)} + \ldots + k_{P_2^{-1}(45)} + k_{P_2^{-1}(46)} +$$
$$k_{P_2^{-1}(47)}k_{P_2^{-1}(48)} + k_{P_2^{-1}(49)}k_{P_2^{-1}(50)} + \ldots + k_{P_2^{-1}(83)}k_{P_2^{-1}(84)} + k_{P_2^{-1}(85)}k_{P_2^{-1}(86)} +$$
$$k_{P_2^{-1}(87)} + k_{P_2^{-1}(88)}k_{P_2^{-1}(89)} + \cancel{k_{P_2^{-1}(90)}k_{P_2^{-1}(91)}k_{P_2^{-1}(92)}} + \cancel{\ldots} + \cancel{k_{P_2^{-1}(178)} \cdots k_{P_2^{-1}(191)}}$$

Results

Preliminary version:

degree:	1 ⋯ 1	2	⋯	2	1	2	⋯	k

$$F: \underbrace{x_0 + \ldots + x_{n_1-1}}_{n_1} + \underbrace{x_{n_1}x_{n_1+1} + \ldots + x_{n_1+n_2-2}x_{n_1+n_2-1}}_{n_2} + \underbrace{x_{n_1+n_2} + x_{n_1+n_2+1}x_{n_1+n_2+2} + \ldots + x_{n_1+n_2+n_3-k}\cdots x_{n_1+n_2+n_3-1}}_{n_3}$$

variables: n_1, n_2, n_3

FLIP (n_1, n_2, n_3)	key (N)	Security	degree (k)	C_T	C_D	C_M
FLIP (47, 40, 105)	192	80	14	$2^{54.5}$	$2^{40.3}$	$2^{28.0}$
FLIP (87, 82, 231)	400	128	21	$2^{68.1}$	$2^{58.5}$	$2^{32.3}$

Results

Preliminary version:

degree:	1 ⋯ 1	2 ⋯ 2	1 2 ⋯ k
F:	$x_0 + \dots + x_{n_1-1}$	$+ x_{n_1}x_{n_1+1} + \dots + x_{n_1+n_2-2}x_{n_1+n_2-1}$	$+ x_{n_1+n_2} + x_{n_1+n_2+1}x_{n_1+n_2+2} + \dots + x_{n_1+n_2+n_3-k} \cdots x_{n_1+n_2+n_3-1}$
variables:	n_1	n_2	n_3

FLIP (n_1, n_2, n_3)	key (N)	Security	degree (k)	C_T	C_D	C_M
FLIP (47, 40, 105)	192	80	14	$2^{54.5}$	$2^{40.3}$	$2^{28.0}$
FLIP (87, 82, 231)	400	128	21	$2^{68.1}$	$2^{58.5}$	$2^{32.3}$

New version:

degree: 1 ⋯ 1, 2 ⋯ 2, 1 2 ⋯ k

$$F: x_0 + \dots + x_{n_1-1} + x_{n_1}x_{n_1+1} + \dots + x_{n_1+n_2-2}x_{n_1+n_2-1} + x_{n_1+n_2} + x_{n_1+n_2+1}x_{n_1+n_2+2} + \dots + x_{n_1+n_2-k+\frac{(k+1)k}{2}} \cdots x_{n_1+n_2-1+\frac{(k+1)k}{2}}$$

$$\dots \qquad \dots \qquad \dots$$

$$+ x_{N-\frac{(k+1)k}{2}} + \quad \dots \quad + x_{N-k} \cdots x_{N-1}$$

variables: n_1, n_2; nb (rows)

FLIP $(n_1, n_2, {}^{nb}\Delta^k)$	key (N)	Security	degree (k)
FLIP (42, 128, ${}^{8}\Delta^{9}$)	**530**	80	9
FLIP (82, 224, ${}^{8}\Delta^{16}$)	**1394**	128	16

Thank you!

http://eprint.iacr.org/2016/271.pdf