Cryptanalysis of the stream cipher FLIP

Séminaire équipe projet SECRET

Yann Rotella
joint work with Sébastien Duval & Virginie Lallemand

Inria Paris, France

31 March 2016

The FLIP story

- JC2
- Accepted in Eurocrypt 2016
- Pierrick Méaux, Anthony Journault, François-Xavier Standaert and Claude Carlet, *Towards Stream Ciphers for Efficient FHE with Low-Noise Ciphertexts*, EUROCRYPT 2016.
- Attack submitted at CRYPTO 2016
- Sébastien Duval, Virginie Lallemand, Yann Rotella, *Cryptanalysis of the FLIP family of stream ciphers*,

Results of our attack

Security claim

- key size $= 192$ bits, security : 80
- key size $= 400$ bits, security : 128

Results of our attack

Security claim

- key size $= 192$ bits, security : 80
- key size $= 400$ bits, security : 128

Our attack

- Guess-and-determine & Algebraic attack
- 2^{54} for $N = 192$
- 2^{68} for $N = 400$

Results of our attack

Security claim

- key size $=$ 192 bits, security : 80
- key size $=$ 400 bits, security : 128

Our attack

- Guess-and-determine & Algebraic attack
- 2^{54} for $N = 192$
- 2^{68} for $N = 400$

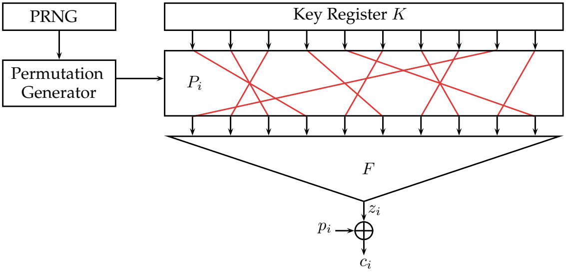
Patch

- $192 \longrightarrow 530$
- $400 \longrightarrow 1394$

Specific aspects

- Stream cipher
- FHE
- The key is stored
- Internal state always the same
- Filter permutator

Filter permutator construction



FLIP

- Key register : size N linear in $\lambda \rightarrow$ Maybe not anymore...
- PRNG : forward secure based on AES 128
- Permutation Generator : Knuth Shuffle
- Filtering function F

The filtering function F

n-th function of type L :

$$L_n(x_0, \cdots, x_{n-1}) = \sum_{i=0}^{n-1} x_i \qquad \text{ex : } L_3 = x_0 + x_1 + x_2$$

n-th function of type Q :

$$Q_n(x_0, \cdots, x_{2n-1}) = \sum_{i=0}^{n-1} x_{2i} x_{2i+1} \qquad \text{ex : } Q_3 = x_0 x_1 + x_2 x_3 + x_4 x_5$$

n-th function of type T :

$$T_k(x_0, \cdots, x_{\frac{k(k+1)}{2}-1}) = \sum_{i=1}^{k} \prod_{j=0}^{i-1} x_{j+\sum_{\ell=0}^{i-1} \ell} \qquad \text{ex : } T_3 = x_0 + x_1 x_2 + x_3 x_4 x_5$$

The filtering function F

n-th function of type L :

$$L_n(x_0,\cdots,x_{n-1}) = \sum_{i=0}^{n-1} x_i \qquad \text{ex : } L_3 = x_0 + x_1 + x_2$$

n-th function of type Q :

$$Q_n(x_0,\cdots,x_{2n-1}) = \sum_{i=0}^{n-1} x_{2i}x_{2i+1} \qquad \text{ex : } Q_3 = x_0x_1 + x_2x_3 + x_4x_5$$

n-th function of type T :

$$T_k(x_0,\cdots,x_{\frac{k(k+1)}{2}-1}) = \sum_{i=1}^{k}\prod_{j=0}^{i-1} x_{j+\sum_{\ell=0}^{i-1}\ell} \qquad \text{ex : } T_3 = x_0 + x_1x_2 + x_3x_4x_5$$

F is given by the **direct sum** of 3 functions :

$$F(x_0,\cdots,x_{n_1+n_2+n_3-1}) = L_{n_1} + Q_{n_2/2} + T_k$$

$$\text{où } n_1 + n_2 + n_3 = N \text{ et } n_3 = \frac{k(k+1)}{2}$$

Preliminary version of FLIP

FLIP (n_1, n_2, n_3)	n_1	n_2	n_3	degré (k)	clef (N)	Sécurité
FLIP (47,40,105)	47	40	105	14	192	80
FLIP (87,82,231)	87	82	231	21	400	128

$$F(x_0, \cdots, x_{191}) =$$

$$x_0 + \ldots + x_{46} + x_{47}x_{48} + \ldots + x_{85}x_{86} + x_{87} + x_{88}x_{89} + \ldots + x_{178}x_{179} \cdots x_{191}$$

Cryptanalysis

Classical attacks

- Algebraic Immunity
- Non Linearity
- Resiliency

Cryptanalysis

Classical attacks

- Algebraic Immunity
- Non Linearity
- Resiliency

Our attack

- Use a Guess-and-determine technique to have a simpler function
- Combine with a classical attack on the reduced boolean function

Our attack

1. Guess ℓ random positions of null bits
2. Keep an equation when there is at least **one** null bit in each monomial of degree at least 3
3. Solve the system of degree 2

First step : guess

Size N, **Balanced**

Probability of having a right guess :

$$\mathbb{P}_{rg} = \frac{\binom{\frac{N}{2}}{\ell}}{\binom{N}{\ell}}$$

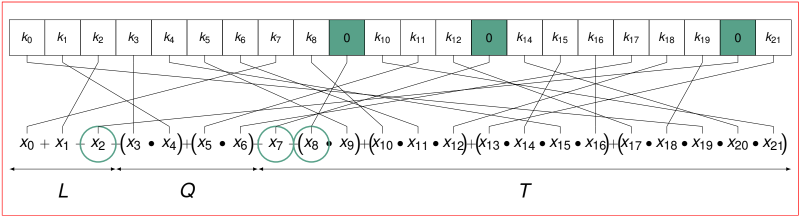
Second step : reach equations of degree ≤ 2

k_0	k_1	k_2	k_3	k_4	k_5	k_6	k_7	k_8	**k_9**	k_{10}	k_{11}	k_{12}	**k_{13}**	k_{14}	k_{15}	k_{16}	k_{17}	k_{18}	k_{19}	**k_{20}**	k_{21}

Second step : reach equations of degree ≤ 2

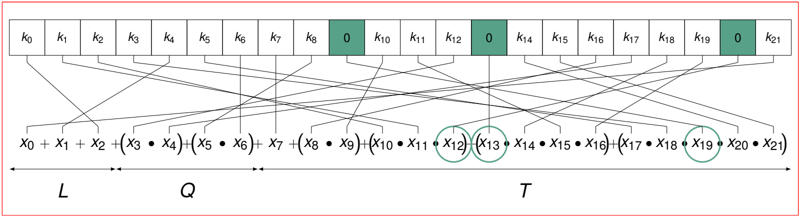
k_0	k_1	k_2	k_3	k_4	k_5	k_6	k_7	k_8	0	k_{10}	k_{11}	k_{12}	0	k_{14}	k_{15}	k_{16}	k_{17}	k_{18}	k_{19}	0	k_{21}

Second step : reach equations of degree ≤ 2



$$z_i = k_7 + k_2 + k_3k_1 + k_{11}k_{17} + 0 + 0 + k_8k_6k_{18} + k_{21}k_{15} + k_{21}k_{15}k_4k_{16} + k_{12}k_{19}k_0k_{14}k_{10}$$

Second step : reach equations of degree ≤ 2



$$z_{i+1} = k_{21} + k_4 + k_0 + k_{12}k_{17} + k_8 k_6 + k_7 + k_{16}k_{10}$$

Second step : reach equations of degree ≤ 2

If $\ell = k - 2$

$$\mathbb{P}_{\ell=k-2} = \frac{k!/2}{\binom{N}{\ell}}$$

General case :

$$\mathbb{P}_{\ell} = \frac{\sum_{i_1+i_2+\cdots+i_{k-2}\leq\ell} \binom{3}{i_1}\binom{4}{i_2}\cdots\binom{k}{i_{k-2}}\binom{N-m}{\ell-l}}{\binom{N}{\ell}}$$

$\rightarrow$ In average, we need $\mathbb{P}_{\ell}^{-1}$ bits of keystream to reach 1 equation of degree 2

Last step : solving the system

$$v_\ell = N - \ell + \binom{N-\ell}{2}$$

1. Reach v_ℓ independant equations
2. Linearization
3. Gauss elimination

Complexity

Time :

$$C_T = \frac{1}{\mathbb{P}_{rg}} \times v_\ell^3$$

Data :

$$C_D = v_\ell \times \frac{1}{\mathbb{P}_\ell}$$

Memory :

$$C_M = v_\ell^2$$

Complexity

Time :

$$C_T = \frac{1}{\mathbb{P}_{rg}} \times v_\ell^3$$

Data :

$$C_D = v_\ell \times \frac{1}{\mathbb{P}_\ell}$$

Memory :

$$C_M = v_\ell^2$$

80-bits securtity claim :

$$C_T = 2^{54.5}, C_D = 2^{40.3}, C_M = 2^{28.0}$$

128-bits security claim :

$$C_T = 2^{68.1}, C_D = 2^{58.5}, C_M = 2^{32.3}$$

Trade-off

FLIP	$\mathbb{P}_l$	v_l	$\mathbb{P}_{rg}$	C_D	C_T
(47,40,105)	**-26.335**	**-13.992**	**12.528**	**40.326**	**54.503**
13	-23.049	-13.976	13.627	37.025	55.554
14	-20.653	-13.960	14.736	34.613	56.615
(87,82,231)	**-42.382**	**-16.151**	**19.647**	**58.533**	**68.100**
20	-38.522	-16.144	20.721	54.666	69.151
21	-35.589	-16.136	21.799	51.725	70.206

Conclusion & Improvements

Conclusion

Security in $\lambda \times \sqrt{N}$

1. Guess regarding permutations
2. Precompute the Gauss-Pivot

Full version of FLIP

	N	λ
$FLIP(42, 128, \Delta_{8,9})$	530	80
$FLIP(82, 224, \Delta_{8,16})$	1394	128

Work in Progress

- Entries of $F \longrightarrow$ constant Hamming weight
  1. Biased ouput ?
  2. Algebraic Immunity ?
  3. Non-linearity ?
- Whitening
- Generalization of this attack

Entries with a constant Hamming weight

Balanced ? $\longrightarrow$ Not so easy...

$$NL_{k,n} = \binom{n}{k} - \frac{1}{2}\sqrt{\binom{n}{k}}$$

$$AI_{k,n} = \binom{n}{\min(k, s, n-k)}$$

Thank You

Thank You

Questions ?