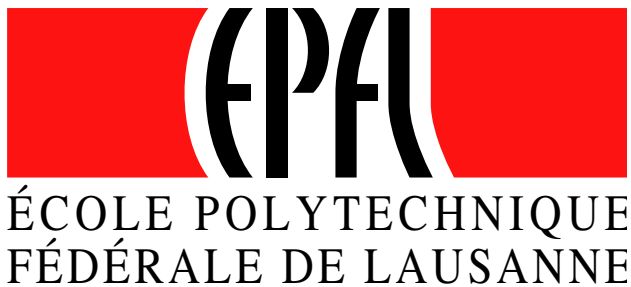
Breaking the FF3 Format Preserving Encryption

F. Betül Durak and Serge Vaudenay



http://lasec.epfl.ch/

LASEC

1. Format Preserving Encryption
2. Round Function Recovery on 4-Round Feistel Schemes
3. Attack on FF3

An Evolution of Encryption

- **block cipher**
  the encryption of a 128-bit block is a 128-bit block
  the encryption of a $128k$-bit string is a $128k$-bit string
- **length-preserving encryption mode**
  the encryption of an ℓ-bit string is an ℓ-bit string
- **format-preserving encryption**
  the encryption of a credit card number is a credit card number
  the encryption of a phone number is a phone number
  the encryption of a zip code is a zip code

Why Format Preserving Encryption?

- companies use expensive software with databases
- they want to encrypt data without rewriting the software

simple approach:
assume an easy 1-to-1 mapping from the plaintext domain to $\mathbf{Z}_N^2$
$\rightarrow$ we need to encrypt on $\mathbf{Z}_N^2$

Wanted

- deterministic encryption from $\mathbf{Z}_N^2$ to itself
- N^2 may be really small
- could add a tweak for more security

input:	**output:**
plaintext$\in \mathbf{Z}_N^2$	ciphertext$\in \mathbf{Z}_N^2$
key+tweak	

tweak can be controled by the adversary

NIST Standard

- NIST SP-800-38G (2016): FF1 and FF3
- tweakable Feistel schemes with modular addition
  balanced, with two branches
- $r = 10$ for FF1 and $r = 8$ for FF3
- security:
  - with $q = \frac{r}{2}N$ known pt, we have enough information to reconstruct the round functions
  - trivial codebook attack with $q = N^2$ pt and one tweak
  - (Patarin 2010) $r = 4$ secure with $q \ll N$ known pt
  - (Patarin 2010) $r = 5$ secure with $q \ll N$ chosen pt
  - (Patarin 2010) $r = 6$ secure with $q \ll N$ chosen pt/ct
  - (Bellare-Hoang-Tessaro 2016) attack with $q > N^2$ (many tweaks)

1 Format Preserving Encryption

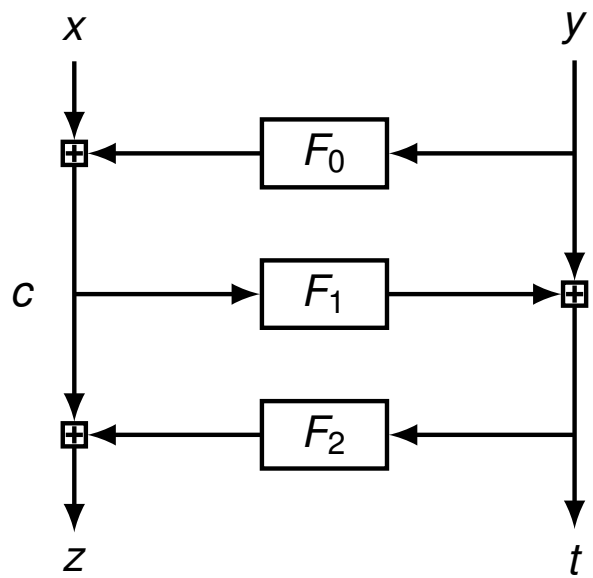
2 **Round Function Recovery on 4-Round Feistel Schemes**

3 Attack on FF3

Round Function Recovery

r	**mode**	**time**	**data**	**ref**
3	known pt	N	N	our 3R attack
4	chosen pt/ct	$N^{\frac{3}{2}}$	$N^{\frac{3}{2}}$	Biryukov-Leuren-Perrin 2015
4	known pt	N^4	$N^{\frac{3}{2}}$	our 4R attack
5	chosen pt/ct	$N^{N^{\frac{3}{4}}}$	N^2	Biryukov-Leuren-Perrin 2015
5	chosen pt	$N^{O(N^{\frac{1}{2}})}$	$N^{\frac{3}{2}}$	our 4R attack extended
≥ 6	chosen pt	$N^{(r-5)N}$	$N^{\frac{3}{2}}$	our 4R attack extended

3R Attack



input: set S of $(xyzt)$ of size θN

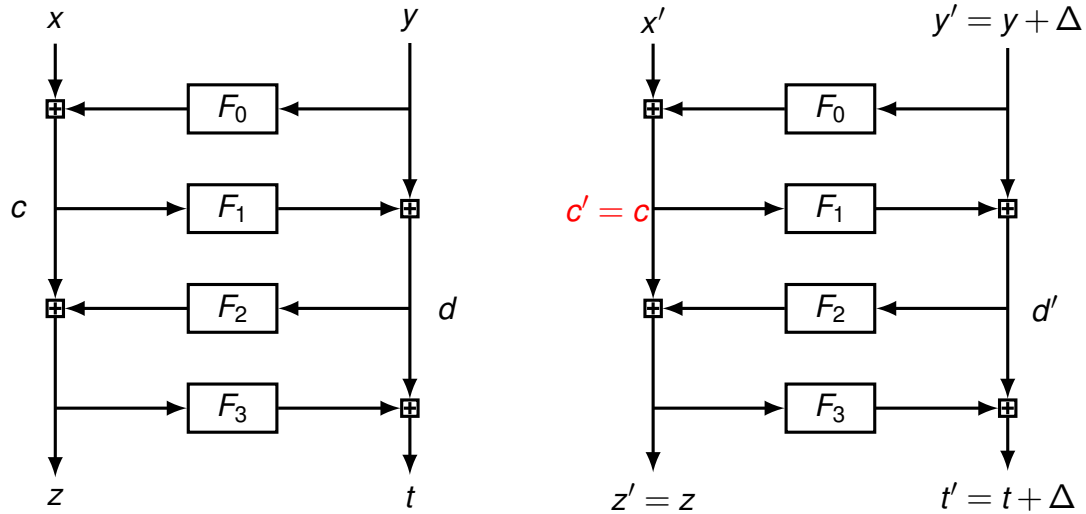
1: take $S_1 \subseteq S$ with y constant (size θ)
2: fix $F_0(y) = 0$ arbitrarily and make a 2R attack on θ tuples $(cyzt)$; collect θ equations $F_2(t) = z - c$
3: take $S_2 \subseteq S$ with t in S_1 (size θ^2)
4: using what is known about F_2, make a 2R attack on θ^2 tuples $(xyct)$; collect θ^2 equations $F_0(y) = c - x$
5: take $S_3 \subseteq S$ with y in S_2 (size θ^3)
6: using what is known about F_0, make a 2R attack on θ^3 tuples $(cyzt)$; collect θ^3 equations $F_2(t) = z - c$
7: play yoyo until nothing new

output: (partial) tables for $F_0 F_1 F_2$

- S defines a random bipartite graph between N values of y and t
- the algorithm looks for the connected component of an arbitrary y
- fully connected if $\theta = \ln N$; with giant component if $\theta = 1$

4R Attack — i

$$V = \{(xyzt, x'y'z't') \mid z' = z, t' - y' = t - y, xy \neq x'y'\}$$
$$V_{\text{good}} = \{(xyzt, x'y'z't') \mid z' = z, c' = c, xy \neq x'y'\} \subseteq V$$



Property

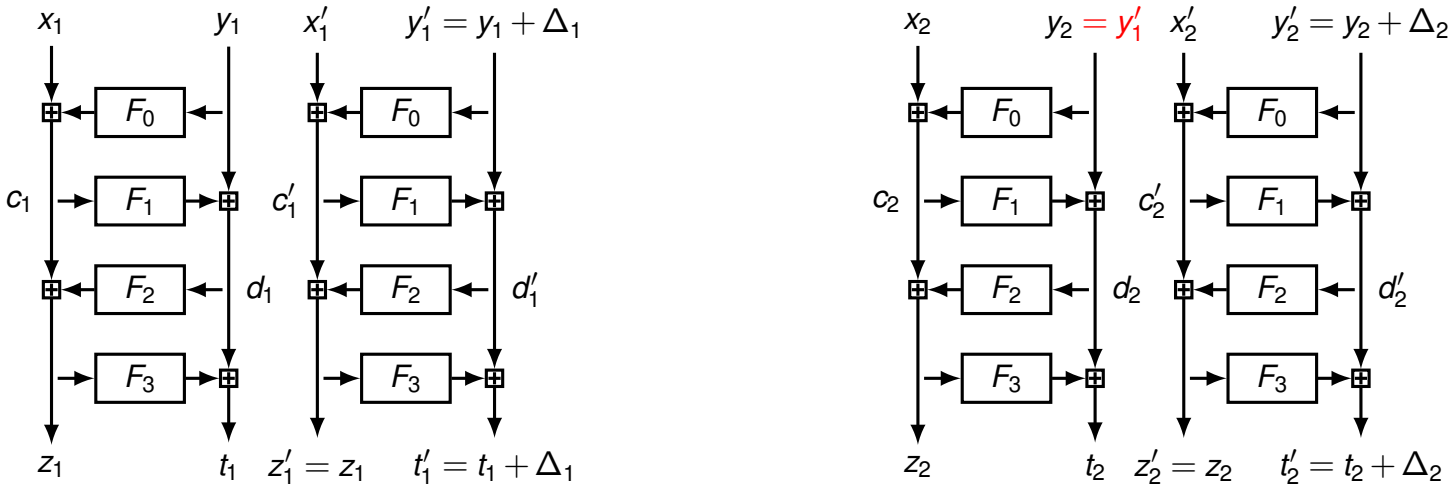
if in V_{good}, then $x - x' = F_0(y') - F_0(y)$

$$\text{define label}(xyzt, x'y'z't') = x - x'$$

4R Attack — ii

define a graph $G = (V, E)$ with

$$E = \{(x_1 y_1 z_1 t_1 x_1' y_1' z_1' t_1', x_2 y_2 z_2 t_2 x_2' y_2' z_2' t_2') | y_1' = y_2\}$$



Property

if $v_1 v_2 \cdots v_L$ is a cycle with all v_i in V_{good}, then

$$\sum_{i=1}^{L} \text{label}(v_i) = 0$$

4R Attack — iii

Lemma

$$E_{F_0 F_1 F_2 F_3}\left(\frac{\#V_{\text{good}}}{\#V}\right) = \frac{1-\frac{1}{N}}{2-\frac{1}{N}} \approx \frac{1}{2}$$

Lemma

$$\Pr[v_1 v_2 \in V_{\text{good}} | v_1 v_2 \text{ non trivial cycle}, \textstyle\sum_{i=1}^{2} \text{label}(v_i) = 0] \geq \frac{1}{1+\frac{10}{N-5}}$$

(trivial cyle: v_1 and v_2 are permutation of each other)

Conjecture

$$\Pr[v_1 \cdots v_L \in V_{\text{good}} | v_1 \cdots v_L \text{ acceptable cycle}, \textstyle\sum_{i=1}^{L} \text{label}(v_i) = 0] \approx 1$$

(acceptable: with $2L$ non-repeating plaintexts)

4R Attack — iv

input: M tuples $(xyzt)$

1: create $G = (V, E)$
2: collect non-trivial cycles of length L with zero label sum
3: deduce M^{2L}/N^{3L} relations $\text{label}(v_i) = F_0(y') - F_0(y)$
4: create the graph G' of all y values connected by these relations
5: find a big connected component C in G' $\{\text{works for } M \geq N^{\frac{3}{2}+\frac{1}{2L}}\}$
6: assign $F_0(y)$ arbitrarily for one $y \in C$, deduce F_0 on C
7: we have $(M/N) \times \#C$ tuples with known $F_0(y)$
8: do a 3R attack for all tuples with known $F_0(y)$
$\{\text{works since } (M/N) \times \#C > N\}$
9: do a yoyo game on 4 rounds with the results from 3R attack

output: (partial) tables for $F_0 F_1 F_2 F_3$

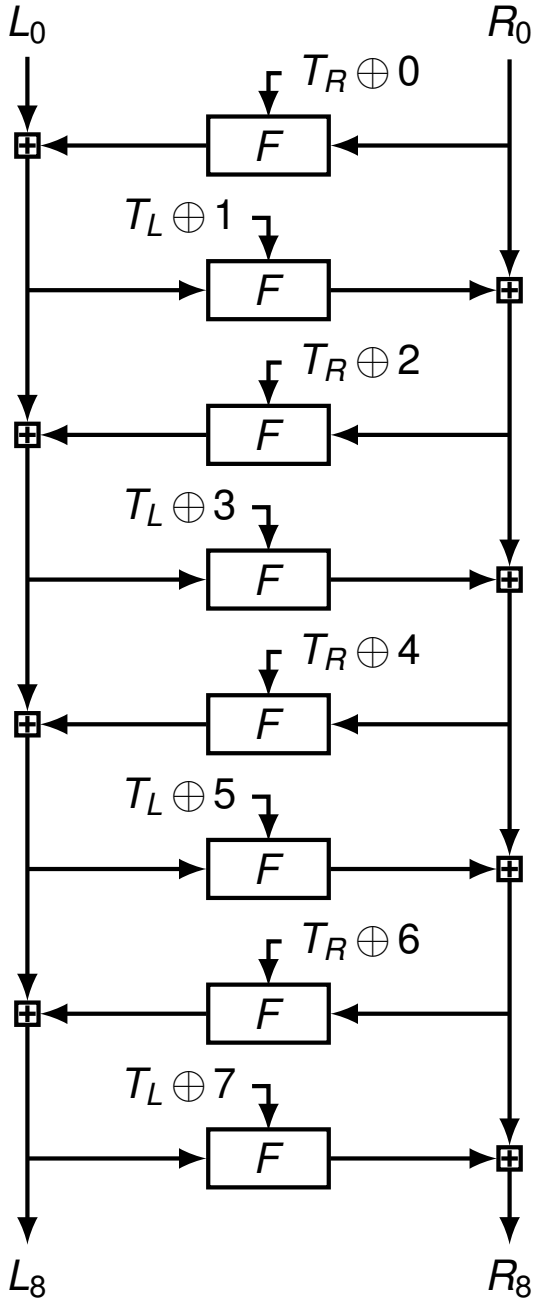
Results

results with $L = 3$ (and $M \approx N^{\frac{3}{2}} \left(\frac{N}{2}\right)^{\frac{1}{2L}}$)

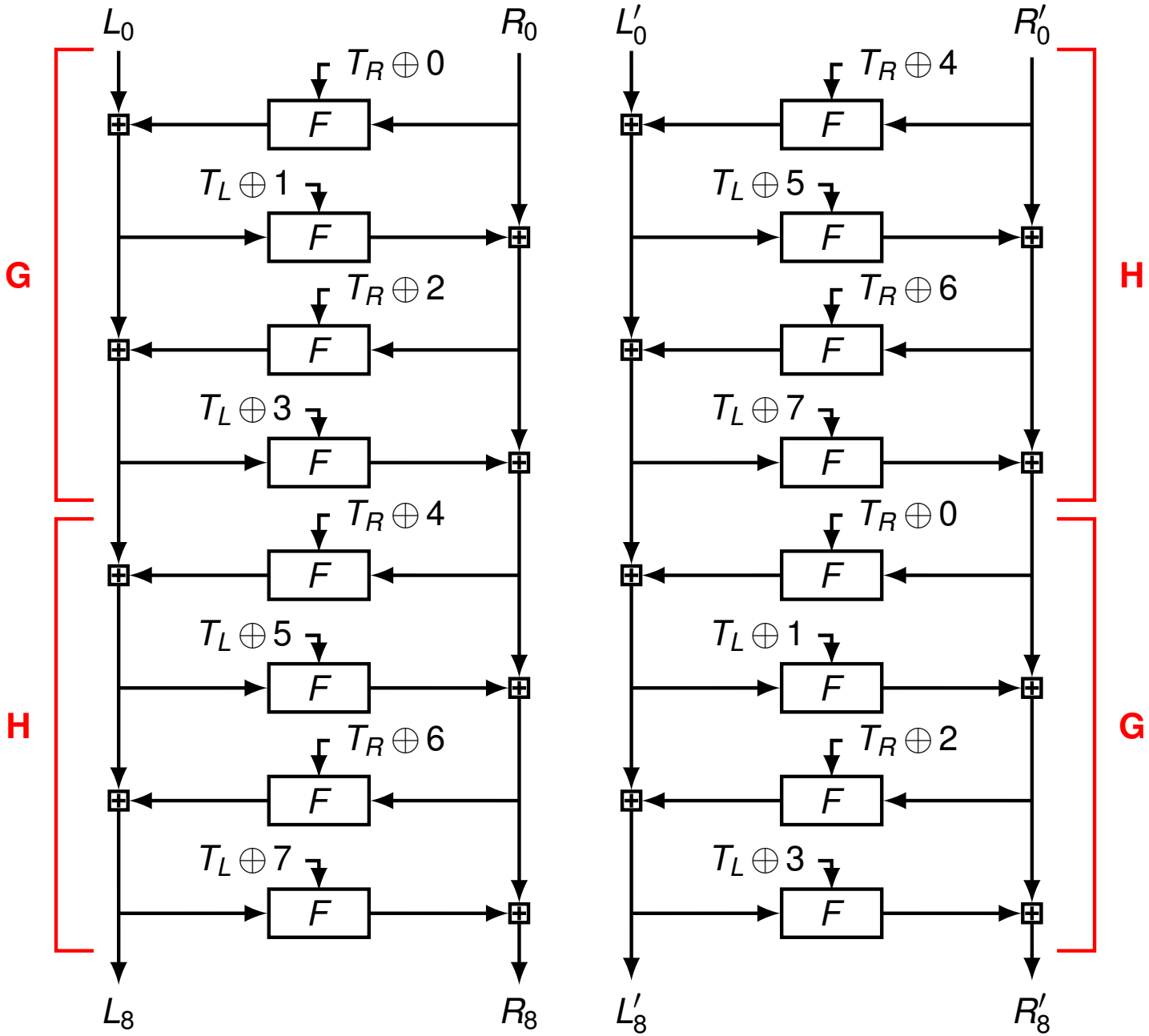
N	M	#trials	Pr[success]	(Pr[S_2])
4	9	3864	3.60%	(88.69%)
8	29	5791	29.11%	(78.62%)
16	91	6585	49.83%	(73.27%)
32	288	6814	62.91%	(71.79%)
64	913	6981	73.80%	(77.14%)
128	2897	6609	83.10%	(83.83%)
256	9196	3154	89.22%	(89.38%)
512	29193	212	92.45%	(92.45%)

S_2: no bad vertices have been collected

FF3 (BPS by Brier-Peyrin-Stern)



XORing 4 to T_L and T_R



Consequence

- given a tweak T, for any key

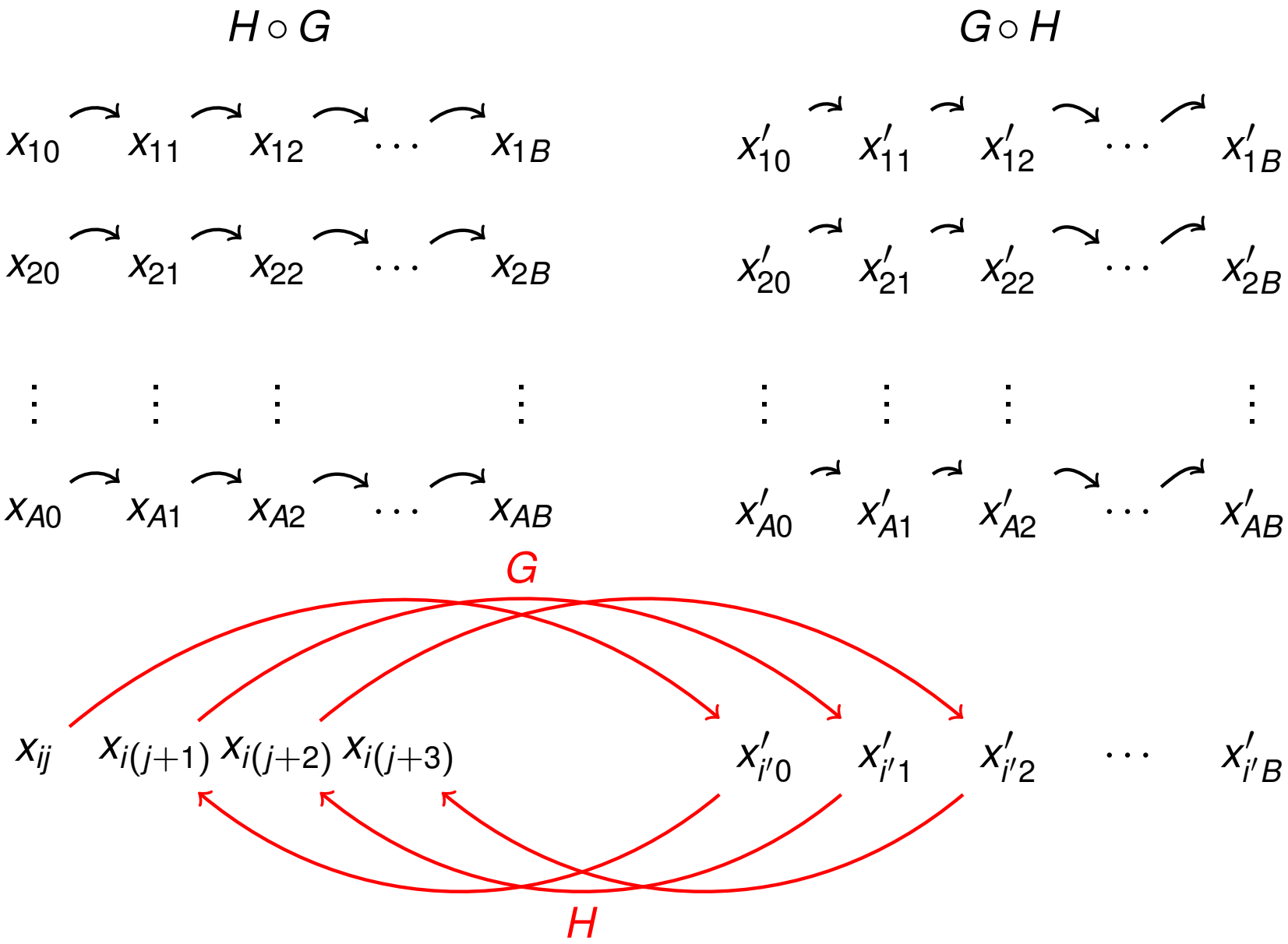
$$\mathrm{Enc}^{T} = H \circ G \qquad \mathrm{Enc}^{T \oplus (4,4)} = G \circ H$$

  where both G and H are 4-round Feistel schemes defined by T
- if we collect x and x' such that

$$x_{i+1} = \mathrm{Enc}^{T}(x_i) \qquad x'_{i+1} = \mathrm{Enc}^{T \oplus (4,4)}(x'_i)$$

  and if we guess that $G(x_i) = x'_j$, then $G(x_{i+k}) = x'_{j+k}$ so all (x_{i+k}, x'_{j+k}) are pt/ct pairs for G

Chosen Plaintext Attack on BPS



Chosen Plaintext Attack on BPS

input: T

1: $T' = T \oplus (4,4)$
2: **for** $i = 1$ to N^{α} **do**
3: pick x_{i0} and set $x_{ij} = \mathrm{Enc}^{T}(x_{i(j-1)})$ for $j = 1, \ldots, N^{\beta}$
4: pick x'_{i0} and set $x'_{ij} = \mathrm{Enc}^{T'}(x'_{i(j-1)})$ for $j = 1, \ldots, N^{\beta}$
5: **end for**
6: **for** $i, i' = 1, \ldots, N^{\alpha}$ **do**
7: **for** $j = 0$ to $N^{\beta} - M - 1$ **do**
8: *assume* $G(x_{ij}) = x'_{i'0}$*:*
9: run 4R attack on G with $G(x_{i(j+k)}) = x'_{i'k}$ for $k = 0, \ldots, N^{\beta} - j$
10: if successful, do the same with H and conclude
11: **end for**
12: **for** $j = 0$ to $N^{\beta} - M - 1$ **do**
13: *assume* $G(x_{i0}) = x'_{i'j'}$*:*
14: ...(same)...
15: **end for**
16: **end for**

Results

results with $L = 3$ (and $M \approx N^{\frac{3}{2}} \left(\frac{N}{2}\right)^{\frac{1}{2L}}$)

N	M	N^{α}	N^{β}	#run	Pr[success]
2	3	1	6	10000	0.00%
4	9	1	18	10000	1.40%
8	29	2	58	10000	17.99%
16	91	2	182	10000	35.35%
32	288	2	576	10000	45.89%
64	913	2	1826	10000	54.14%
128	2897	2	5794	10000	56.85%
256	9196	2	18392	5098	56.34%
512	29193	3	58386	256	77.73%

Conclusion

- Feistel schemes over small domains are not well understood yet
- bad domain separation in FF3 (easy to fix)