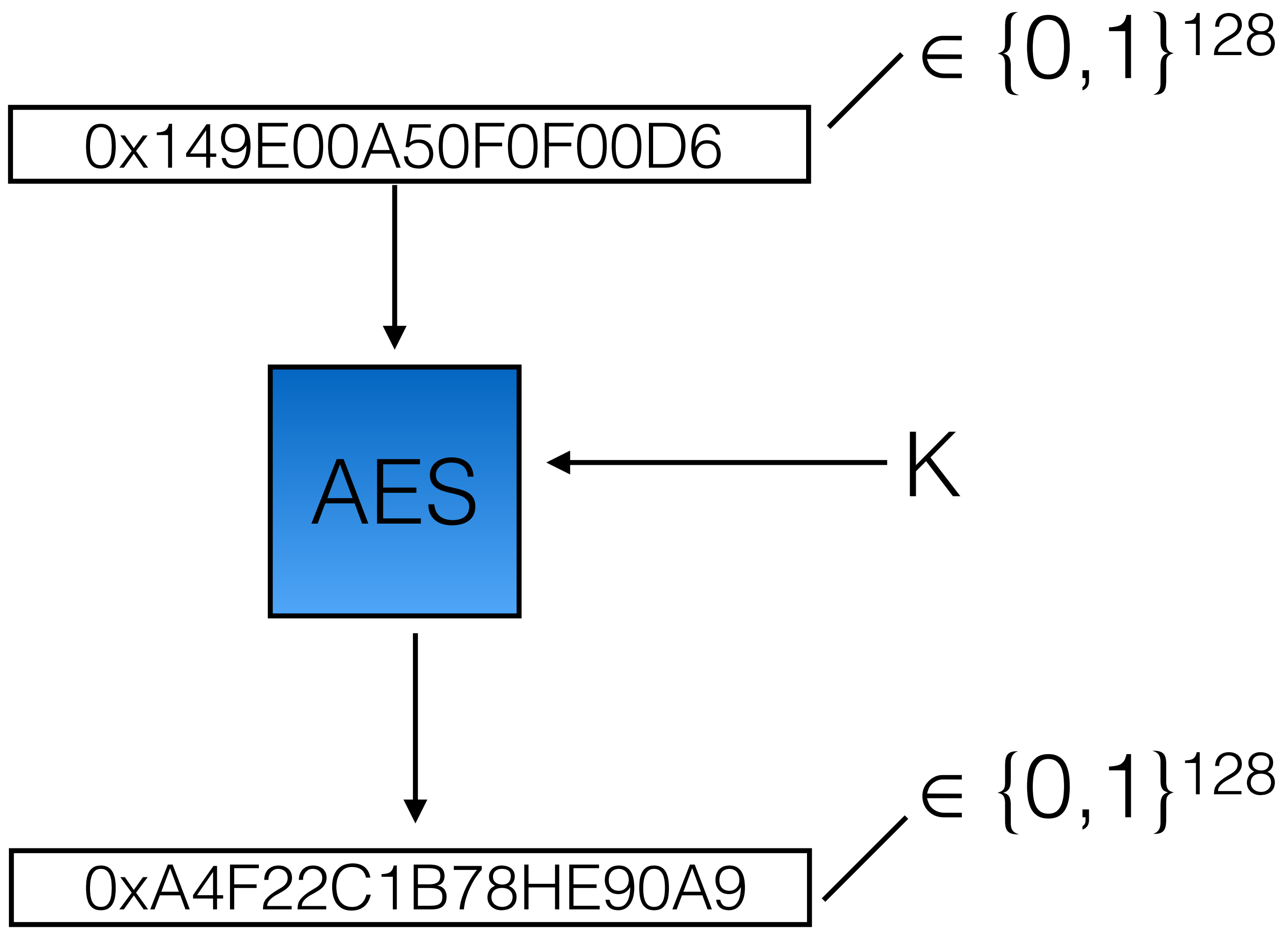
Breaking The FF3 Format-Preserving Encryption Standard Over Small Domains

F. Betül Durak

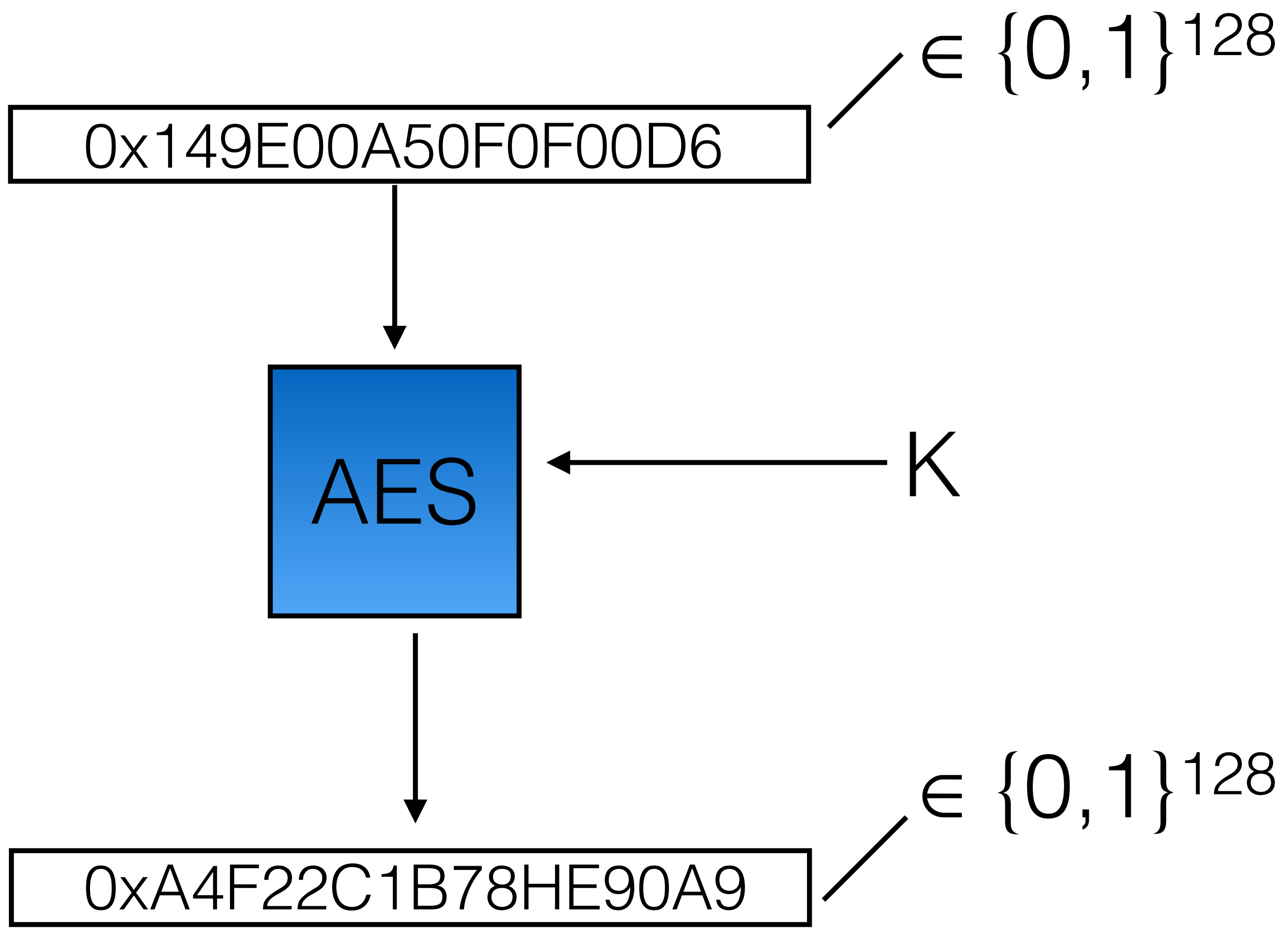
Serge Vaudenay

ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

Block Ciphers

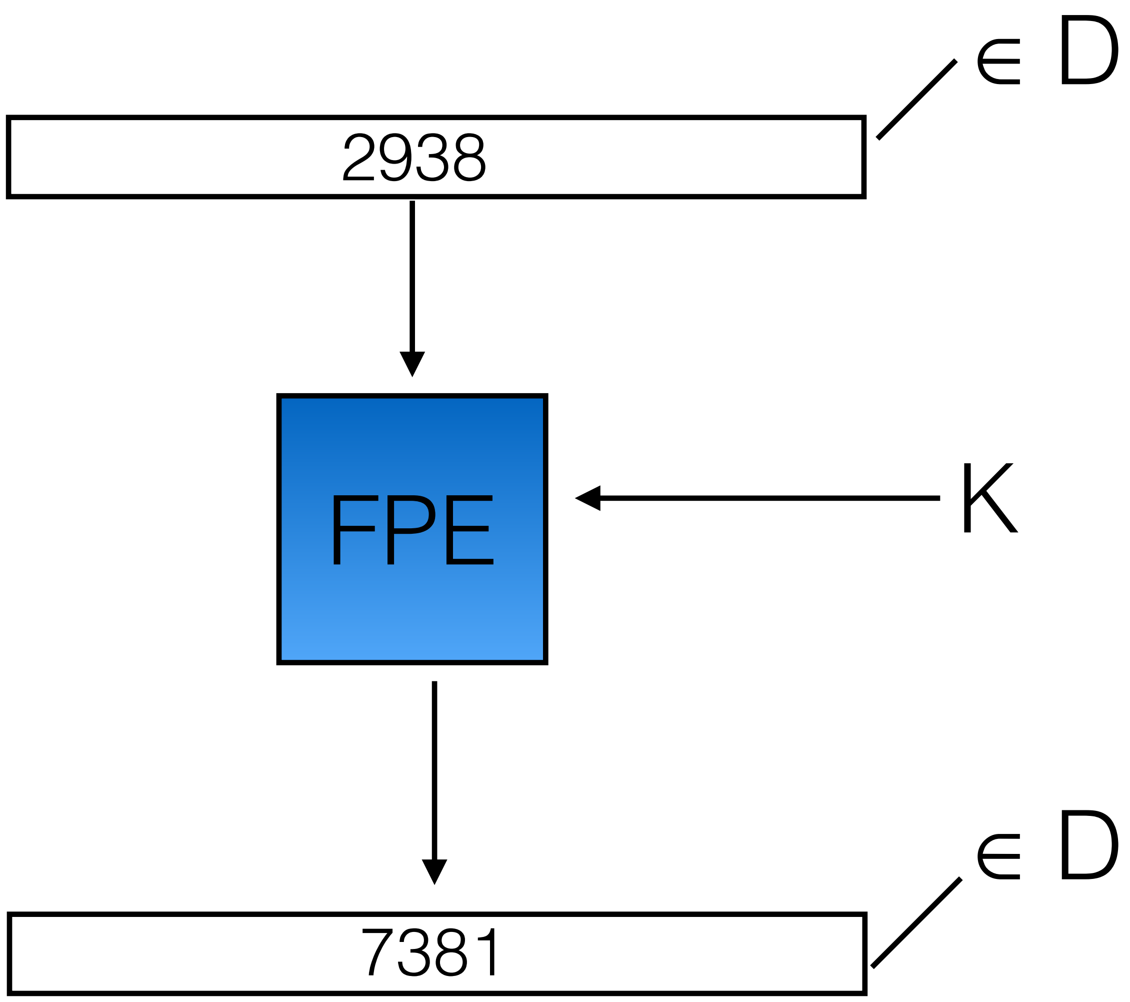


Block Ciphers

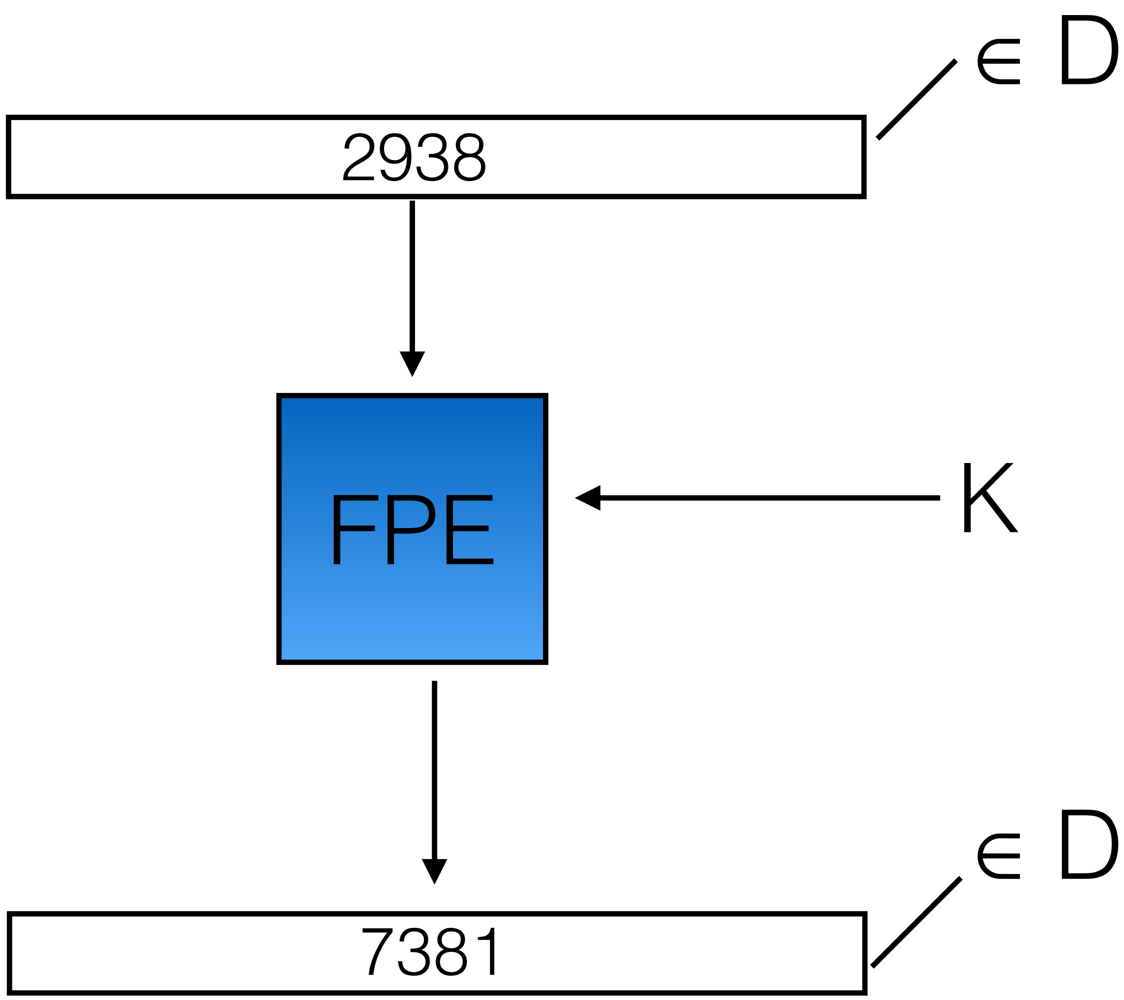


Strict with specific domains: bit-strings of length 128.

Format-Preserving Encryption (FPE) [Brightwell and Smith, 1997], [Black and Rogaway, 2002], [Spies'08],[BRRS'09],…



Format-Preserving Encryption (FPE) [Brightwell and Smith, 1997], [Black and Rogaway, 2002], [Spies'08],[BRRS'09],…



Legacy databases:

- Passcodes
- Social security numbers (SSN) $|D| \approx 2^{30}$
- Credit card numbers (CCN) $|D| \approx 2^{51}$

FPE in Practice: Encrypted Databases

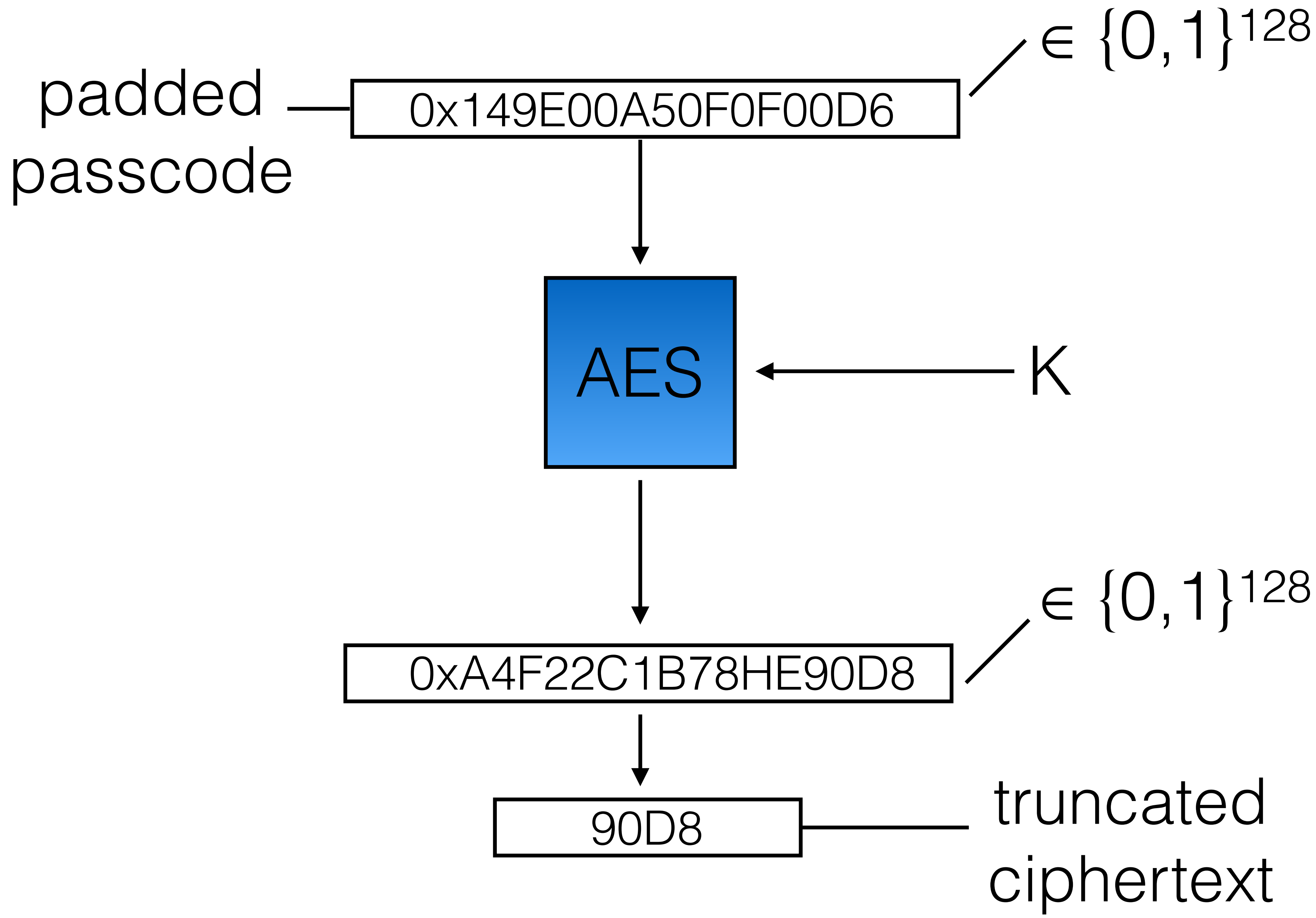
Patients	Passcode	SSN
Alice Yan	2356	34-582-9381
Bob Wu	4567	75-682-8345
…	…	…
Sam Xi	9056	26-734-2108

FPE in Practice: Encrypted Databases

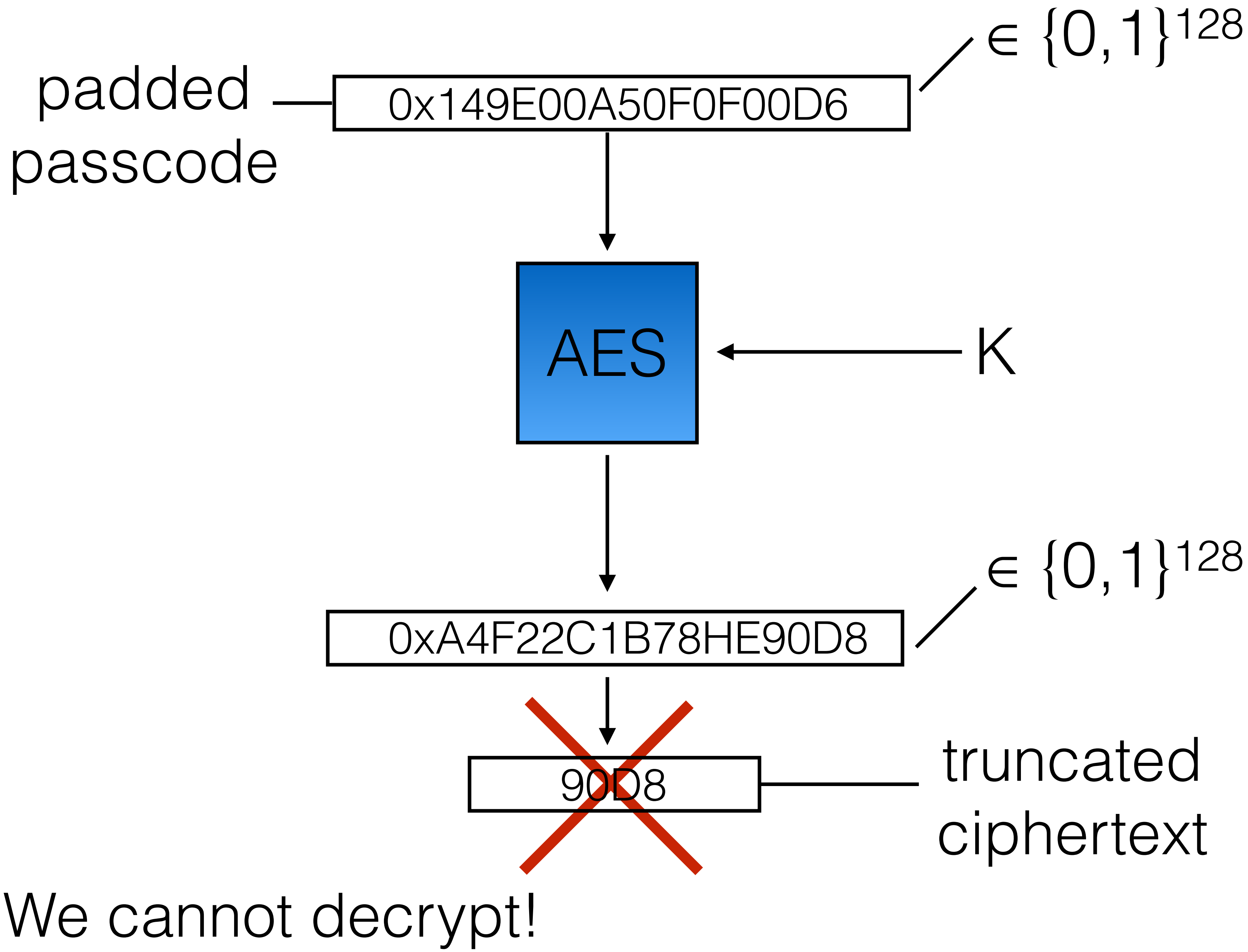
Patients	Passcodes	SSNs
Alice Yan	xxxx	xxxxx-9381
Bob Wu	xxxx	xxxxx-8345
…	…	…
Sam Xi	xxxx	xxxxx-2108

- Transparent encryption in legacy databases.

Main FPE Challenge: Domain Mismatch



Main FPE Challenge: Domain Mismatch



FPE Constructions

- Provably secure [HMR'12, RY'13, MR'14]
    - Not fast enough to use in practice.

FPE Constructions

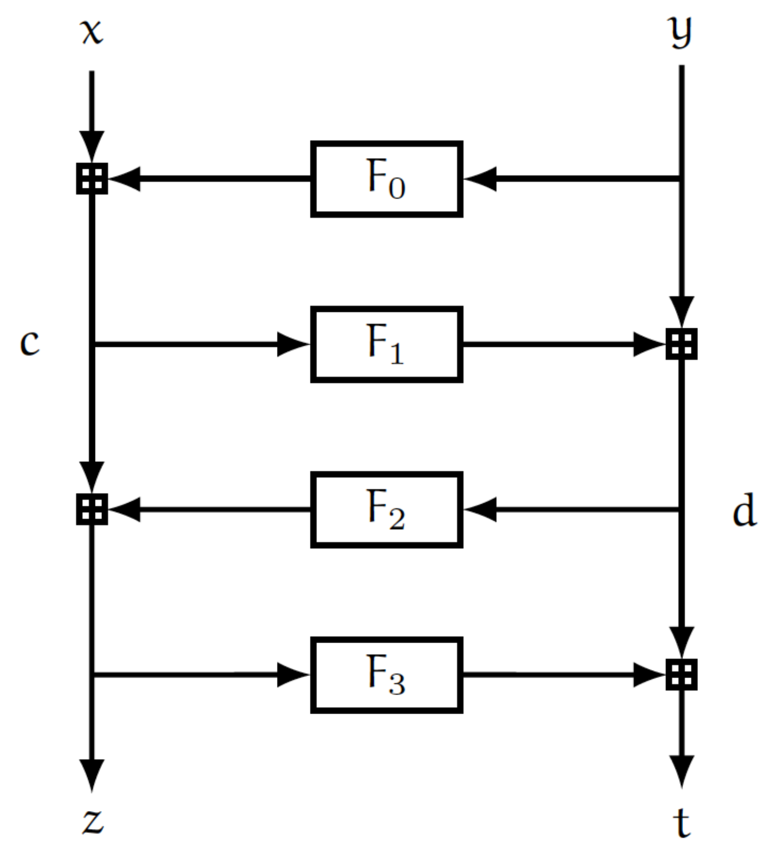
- Provably secure [HMR'12, RY'13, MR'14]
  - Not fast enough to use in practice.

- NIST Special Publications 800-38G:
  - Practical [BRS (FF1), V (~~FF2~~), BPS (FF3)]
  - Security by cryptanalysis (Voilà!).
  - FF1 and **FF3** (somewhat balanced Feistel).

Feistel Network (1973)

$P = x||y$

$$c = x \boxplus F_0(y)$$



$$d = y \boxplus F_1(c)$$

$C = z||t$

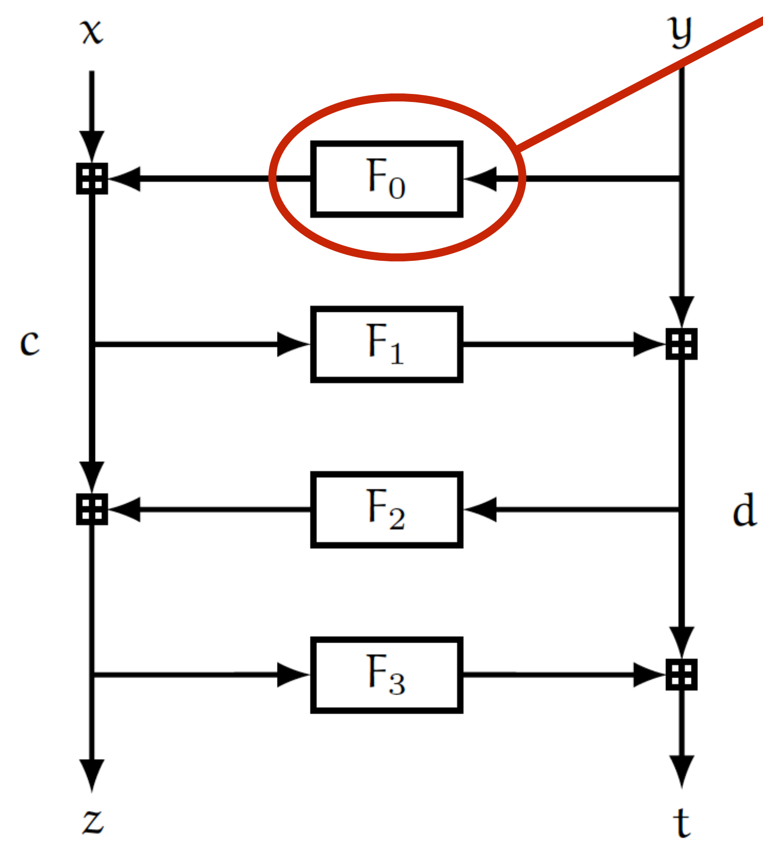
An instance of (balanced) Feistel network on domain D^2

Feistel Network (1973)

any secure PRF onto domain D

P=x||y

$c = x \boxplus F_0(y)$



$d = y \boxplus F_1(c)$

C=z||t

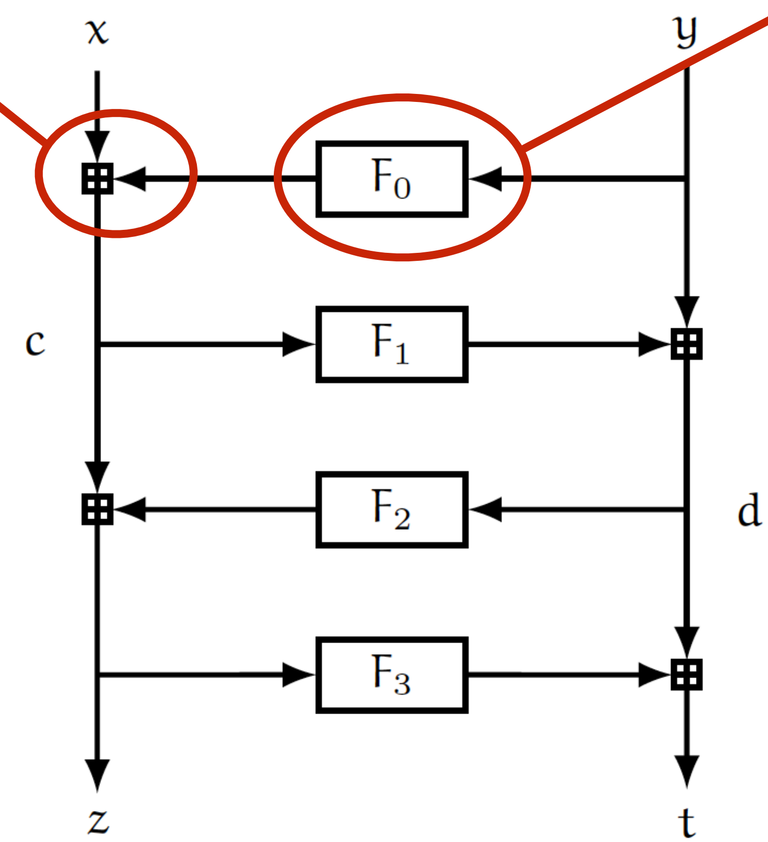
An instance of (balanced) Feistel network on domain D^2

Feistel Network (1973)

group operation
defined on D

any secure PRF
onto domain D

P=x||y



$c = x \boxplus F_0(y)$

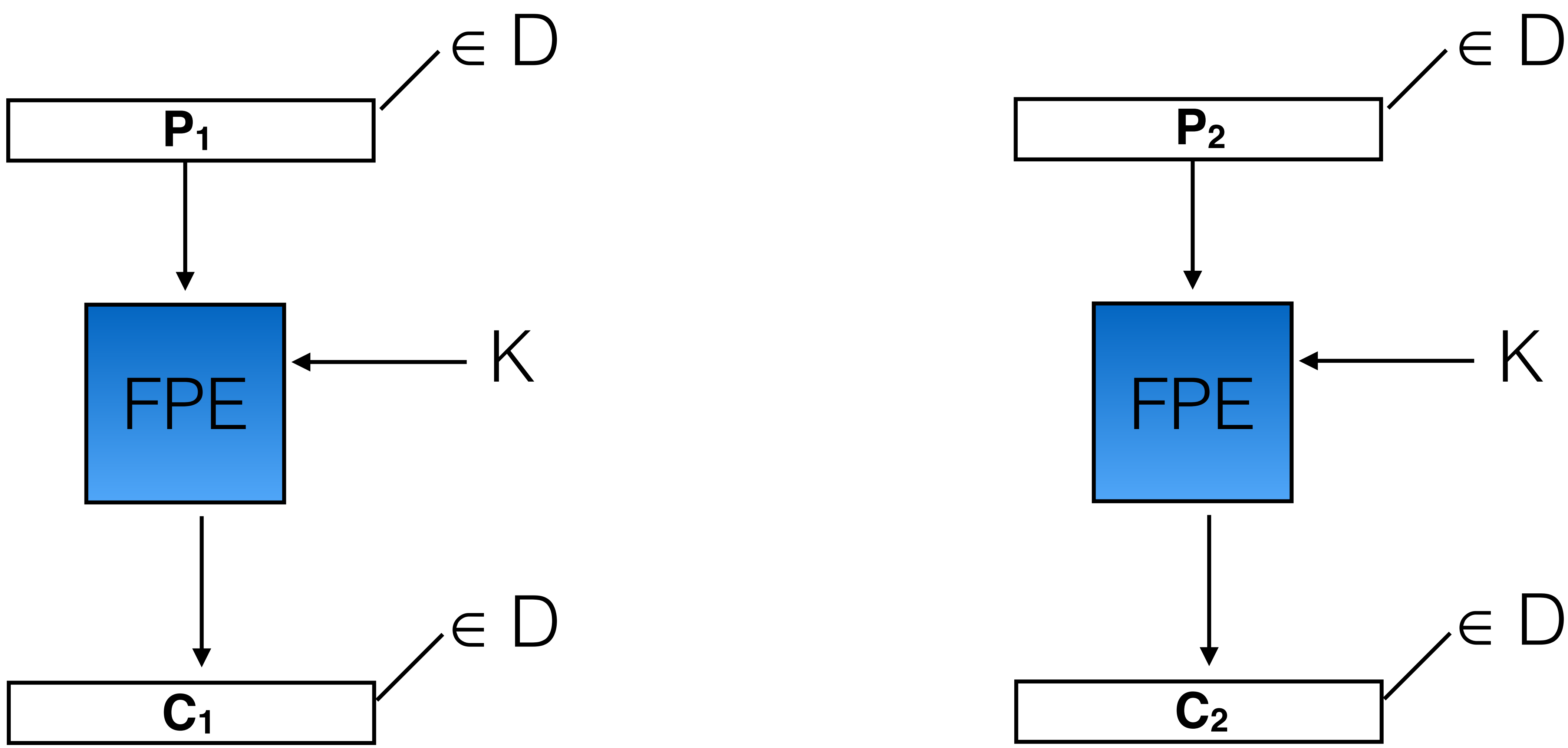
$d = y \boxplus F_1(c)$

C=z||t

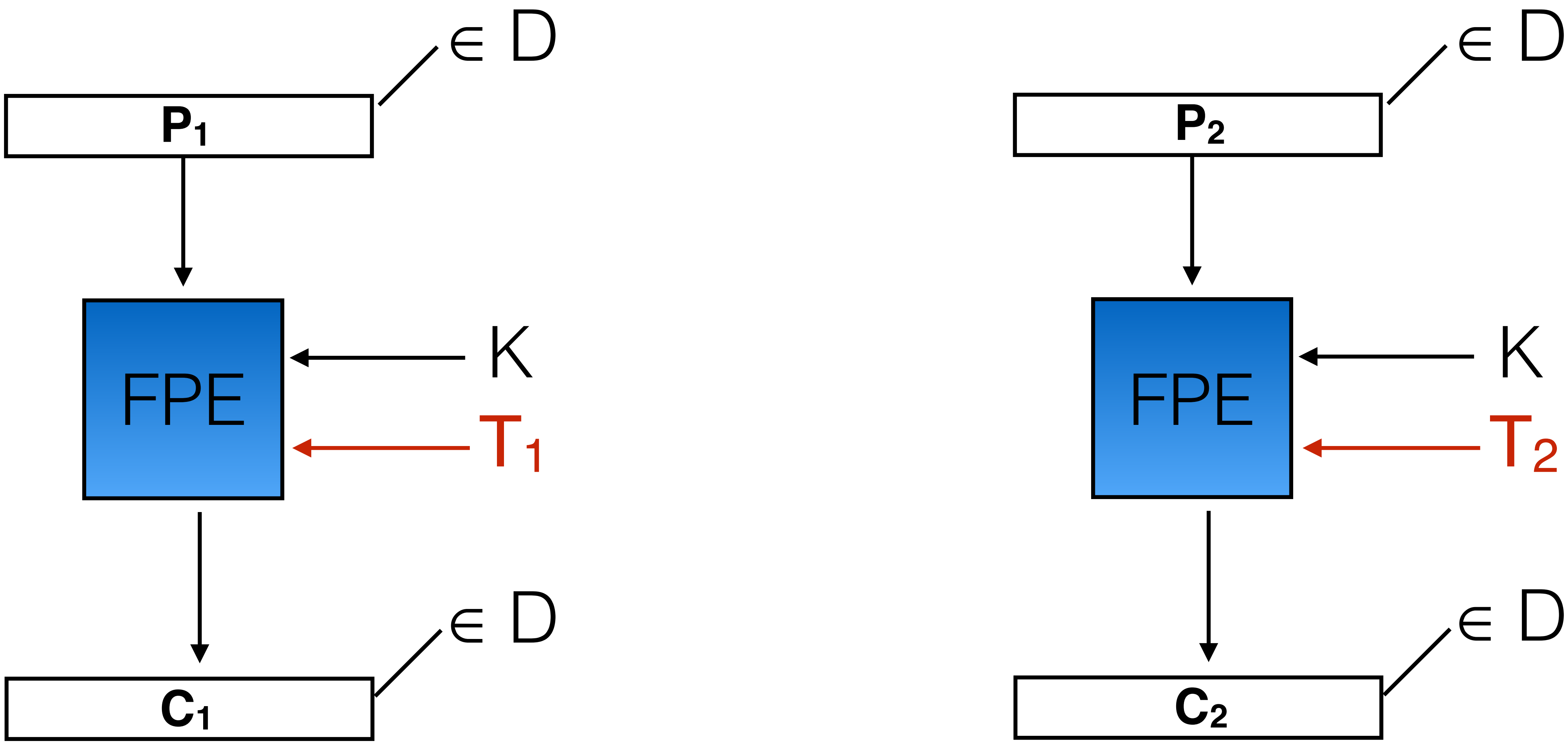
An instance of (balanced) Feistel network on domain D^2

Tweakable Format Preserving Encryption

$Pr[P_1=P_2]$ is high with small domains, hence $C_1=C_2$

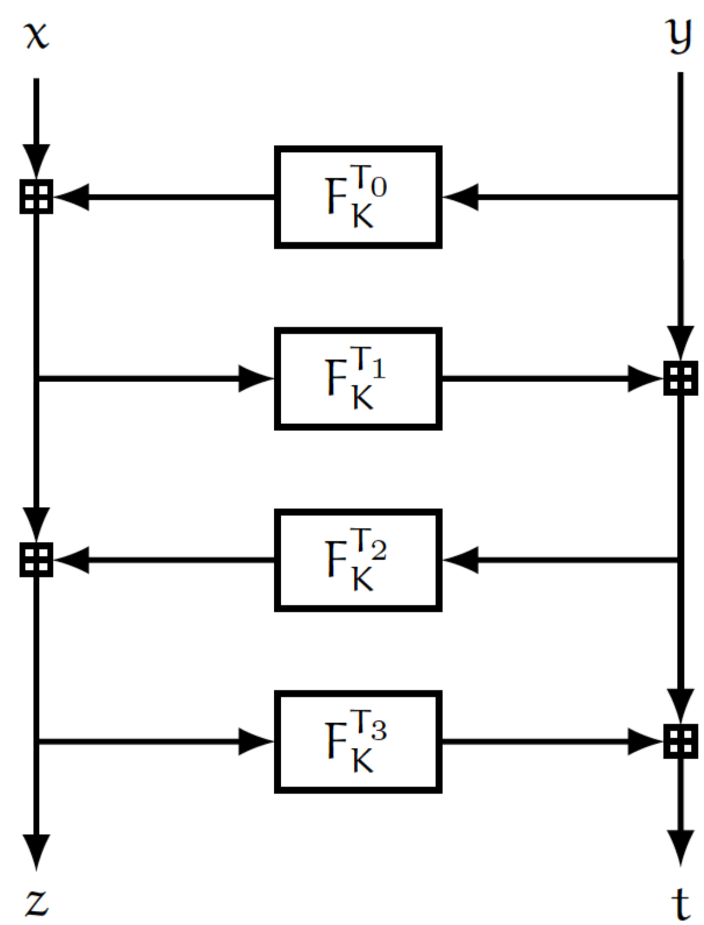


Tweakable Format Preserving Encryption



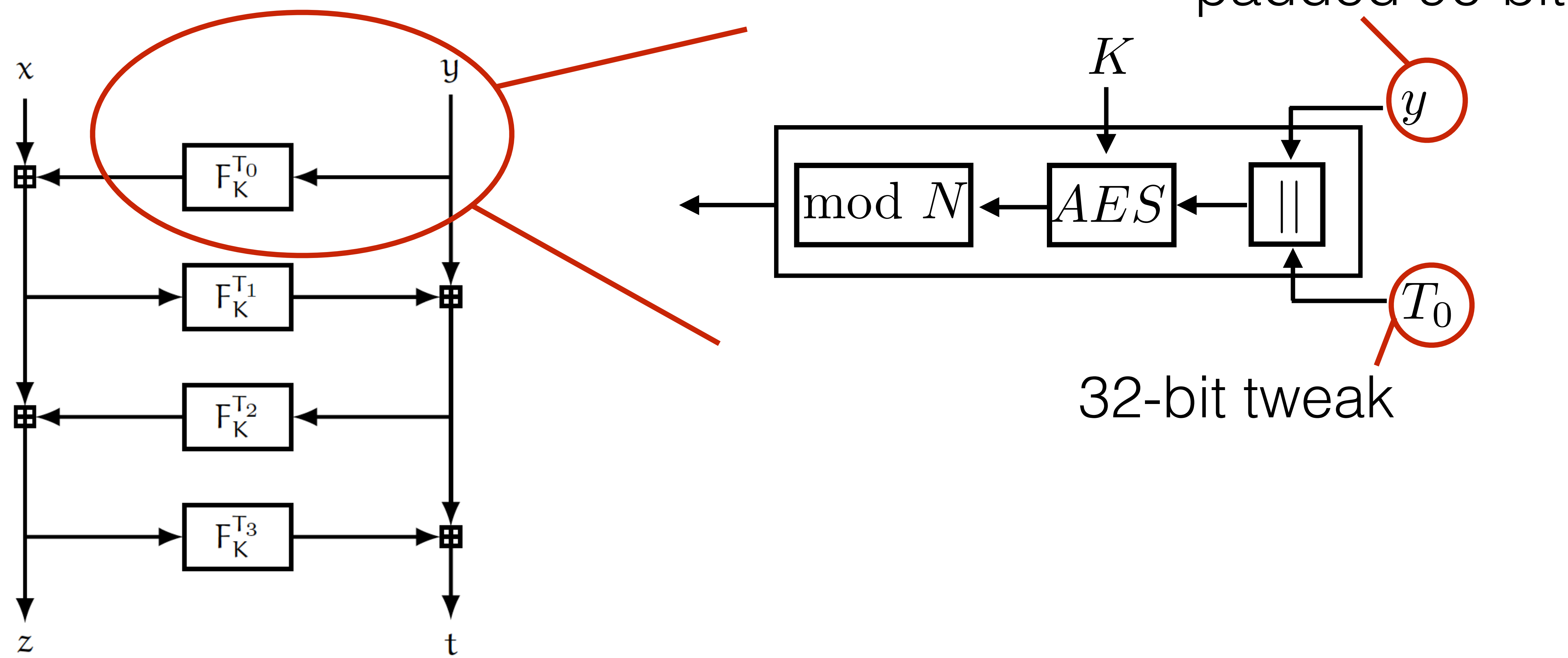
When $P_1 = P_2$ and $T_1 \neq T_2$, $C_1 \neq C_2$

Feistel Networks in FF3



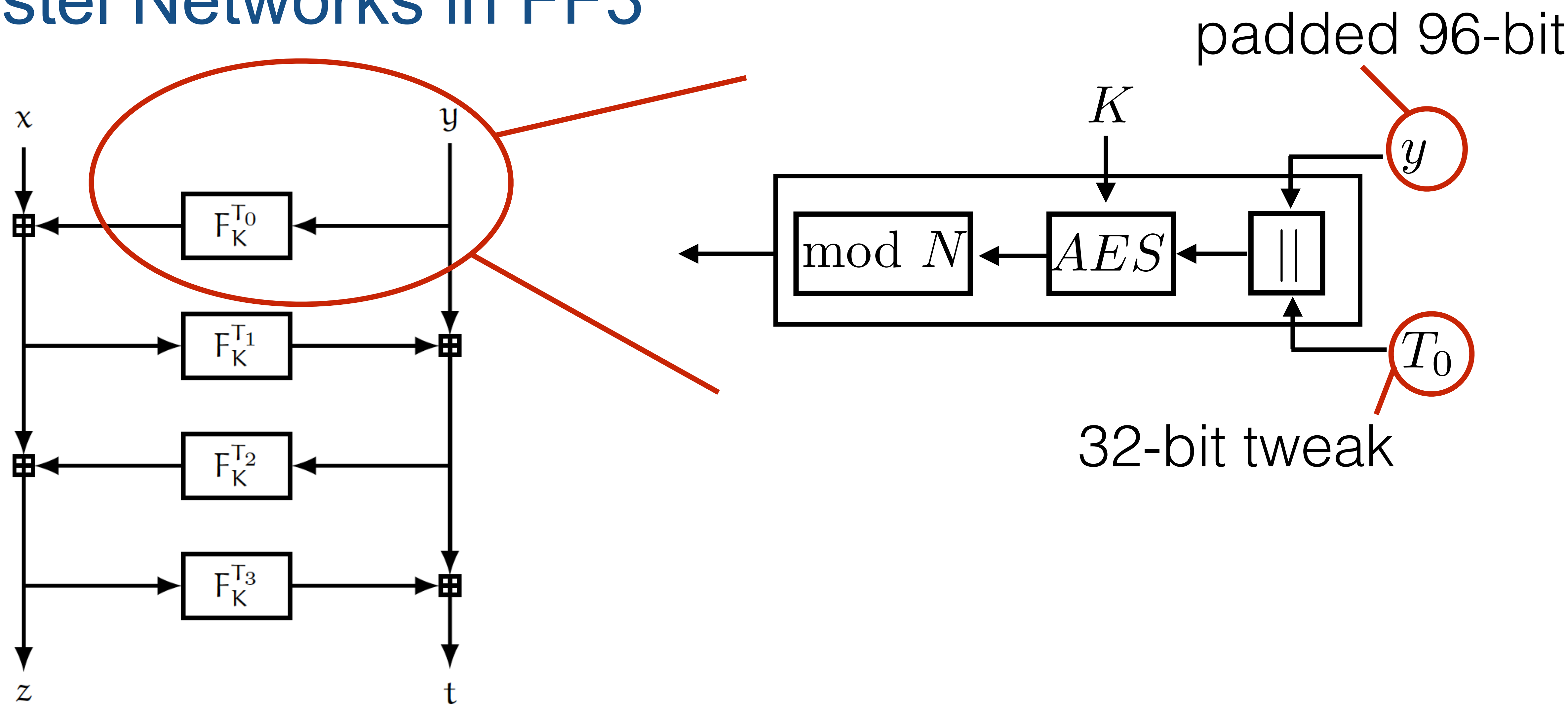
FPE: An encryption scheme on domain $\mathbb{Z}_N \times \mathbb{Z}_N$ (i.e, domain size is N^2) when N is really small, typically defined as $N \ll 2^{128}$.

Feistel Networks in FF3



FPE: An encryption scheme on domain $\mathbb{Z}_N \times \mathbb{Z}_N$ (i.e, domain size is N^2) when N is really small, typically defined as $N \ll 2^{128}$.

Feistel Networks in FF3



FPE: An encryption scheme on domain $\mathbb{Z}_N \times \mathbb{Z}_N$ (i.e, domain size is N^2) when N is really small, typically defined as $N \ll 2^{128}$.

The secret key and tweaks are dropped in notation from now on.

NIST Standard SP-800-38G (2016): **FF3**

- Round number r=8 for **FF3** (r=10 for FF1).
- Domain size is at least 100.
- Security:
  - Targeted security is 128-bit.
  - Security of Feistel networks inherits to **FF3**.
  - **FF3** asserts chosen-plaintext security and even PRP security against chosen-plaintext/-ciphertext attack.

Our Contributions (Briefly)

Part 1: We develop a new generic attack on Feistel networks.

Our Contributions (Briefly)

Part 1: We develop a new generic attack on Feistel networks.

Part 2: We give a total practical break to FF3 standard when the message domain is small.

Our Contributions (Briefly)

Part 1: We develop a new generic attack on Feistel networks.

Part 2: We give a total practical break to FF3 standard when the message domain is small.

- Our attack works with the best known query and time complexity.

Our Contributions (Briefly)

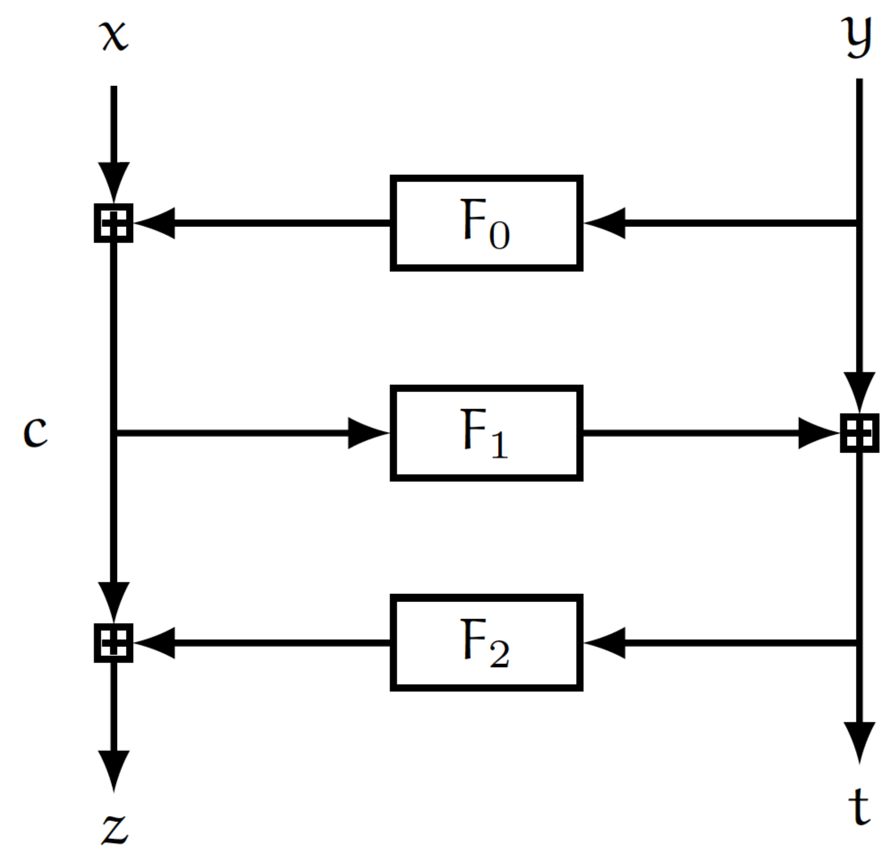
Part 1: We develop a new generic attack on Feistel networks.

Part 2: We give a total practical break to FF3 standard when the message domain is small.

- Our attack works with the best known query and time complexity.
- It is easy fix in order to prevent it from present attack.

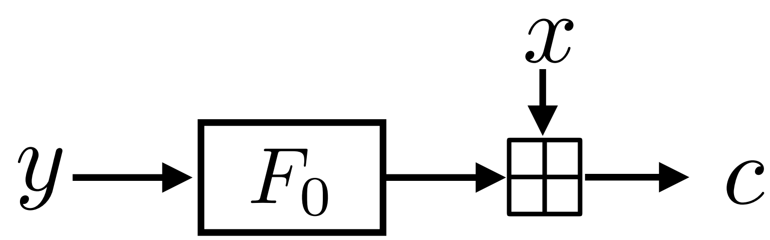
Equivalent Round Functions [BLP'15]

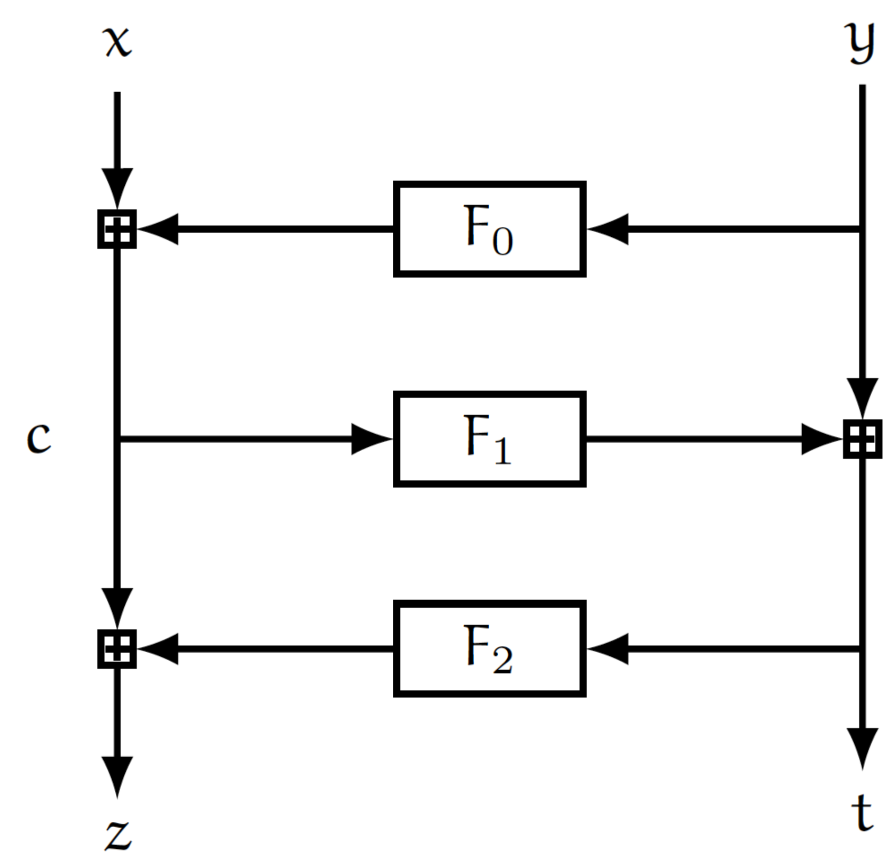
Are the round functions uniquely defined to encrypt messages?



Equivalent Round Functions [BLP'15]

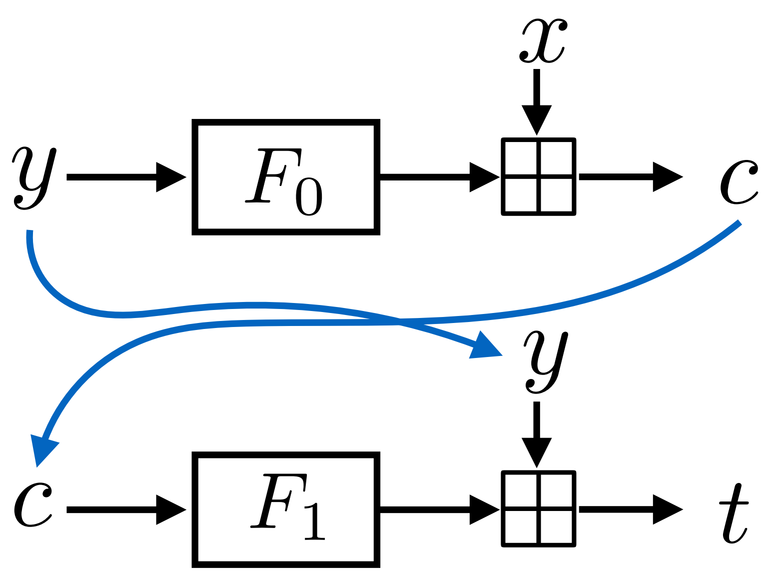
Are the round functions uniquely defined to encrypt messages?

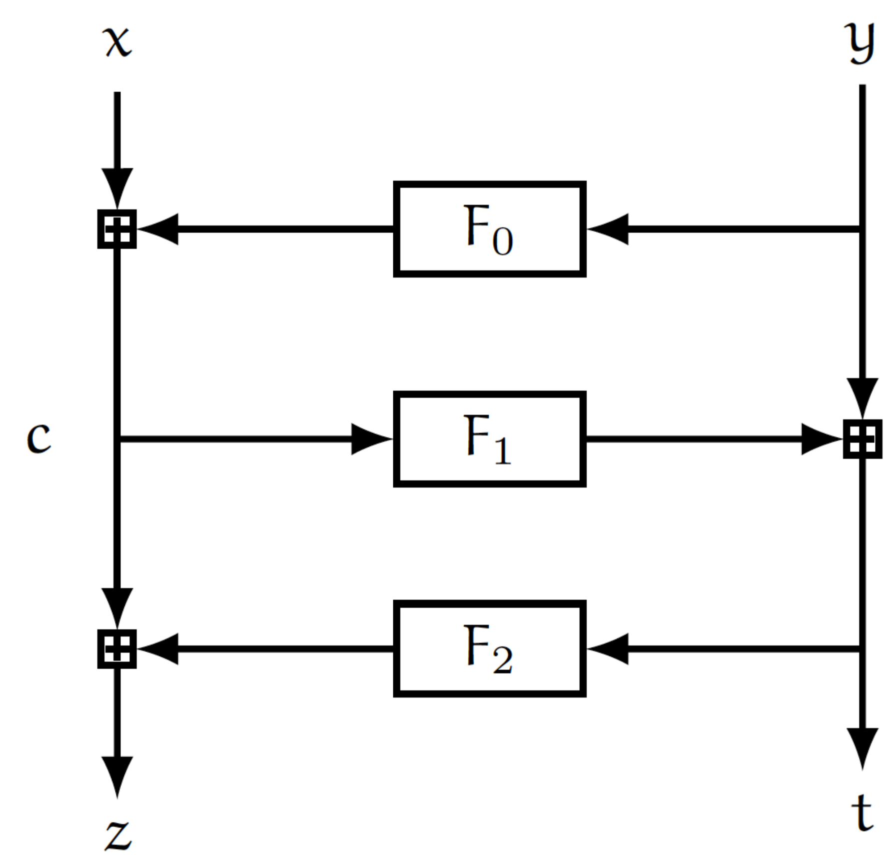




Equivalent Round Functions [BLP'15]

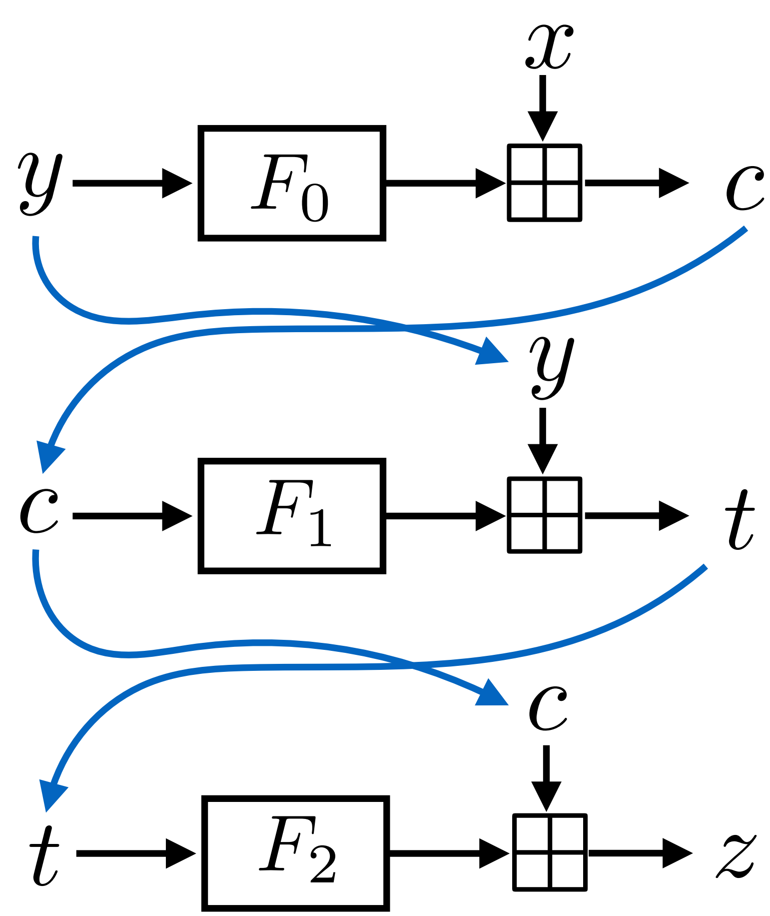
Are the round functions uniquely defined to encrypt messages?

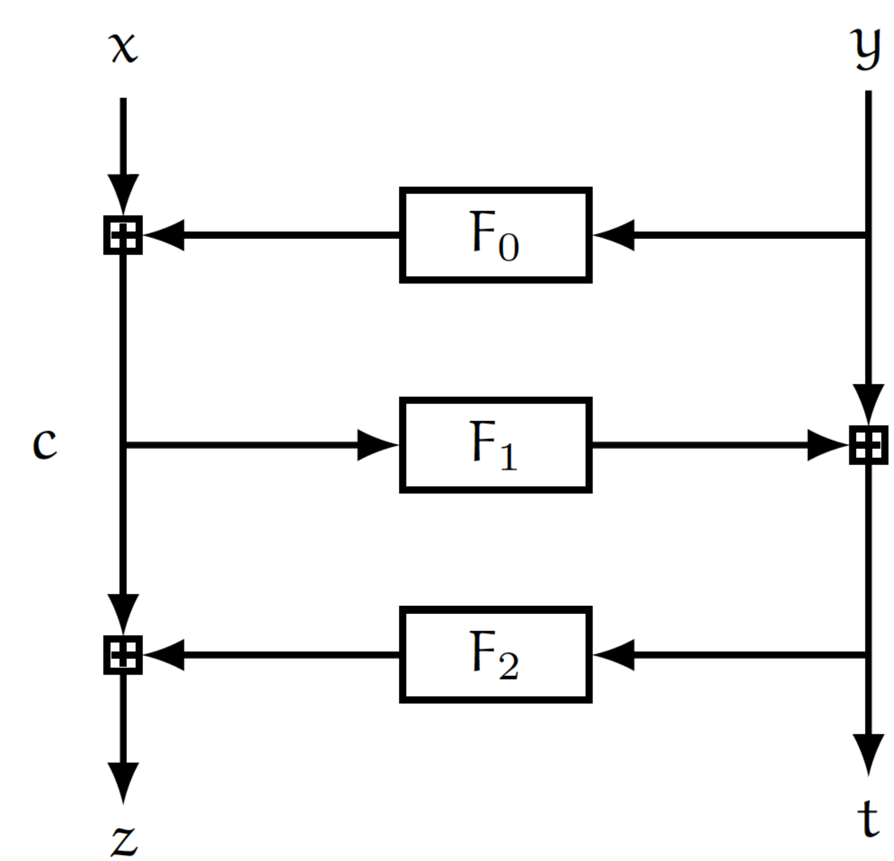




Equivalent Round Functions [BLP'15]

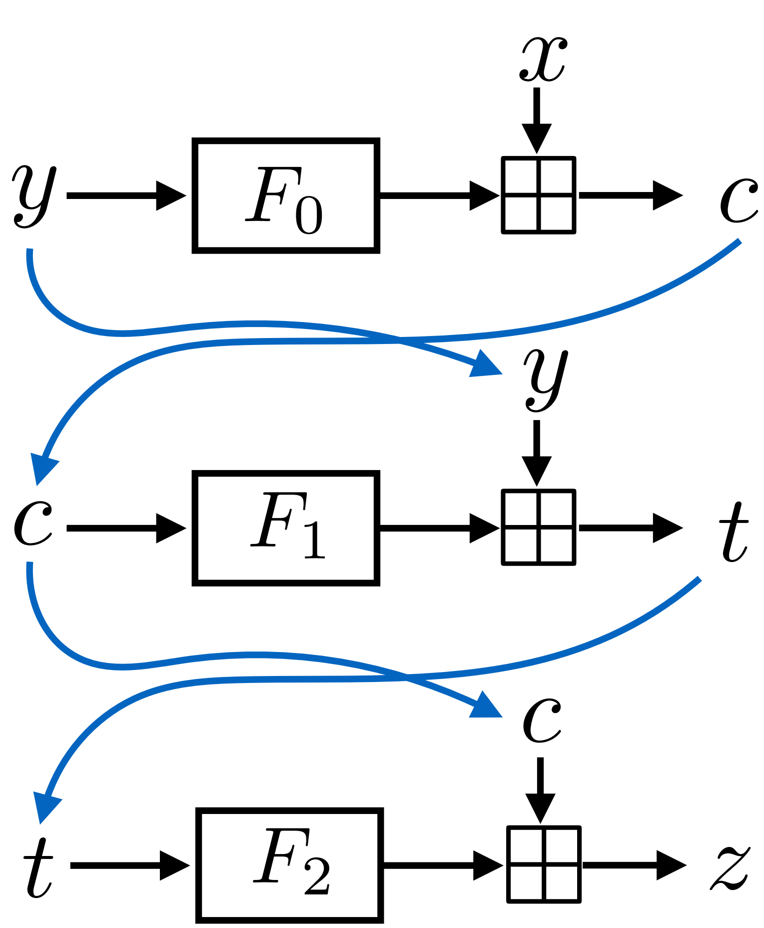
Are the round functions uniquely defined to encrypt messages?

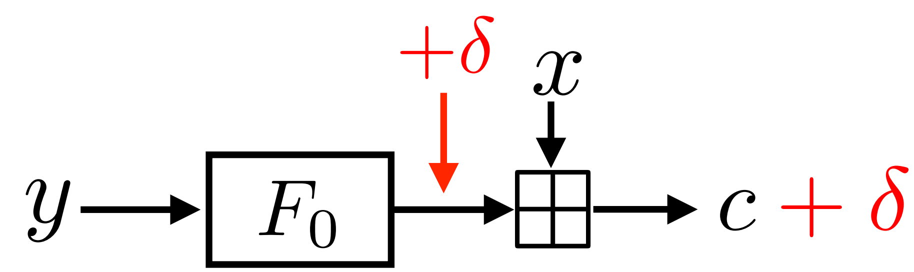




Equivalent Round Functions [BLP'15]

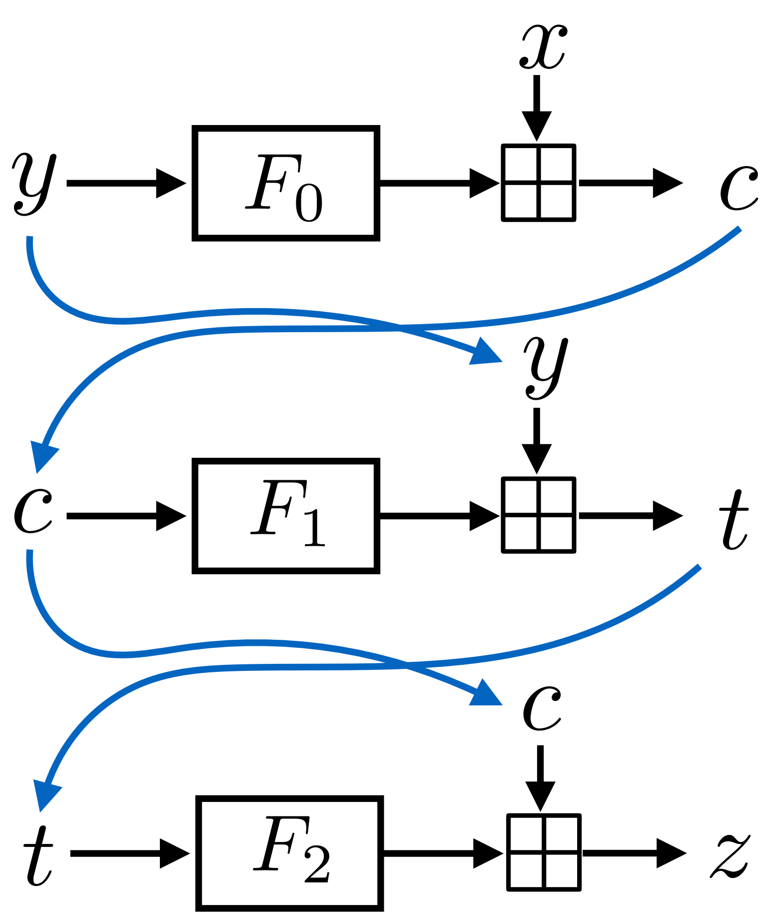
Are the round functions uniquely defined to encrypt messages?

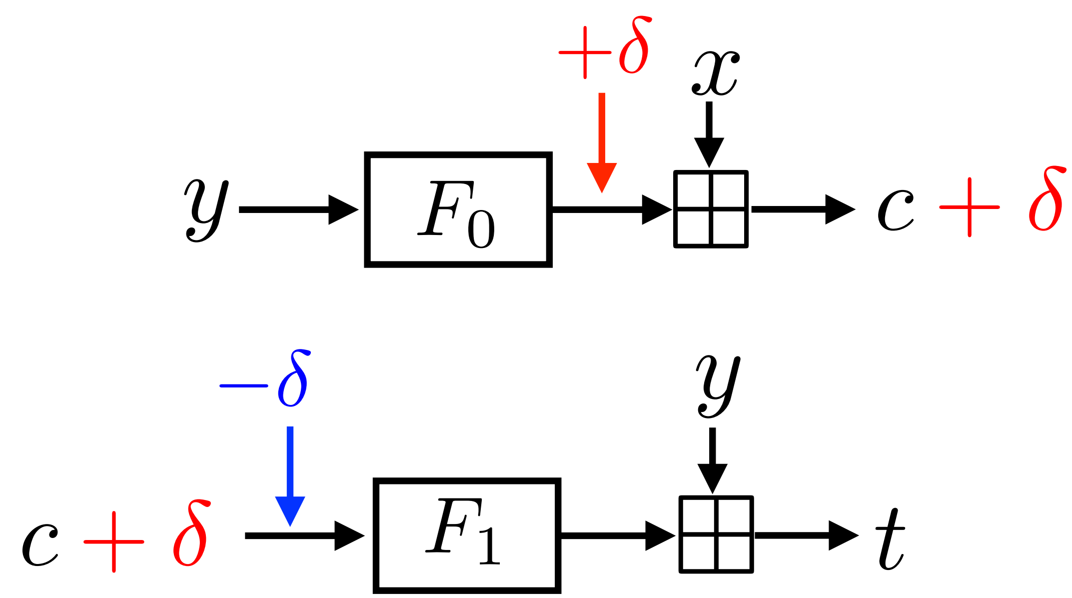




Equivalent Round Functions [BLP'15]

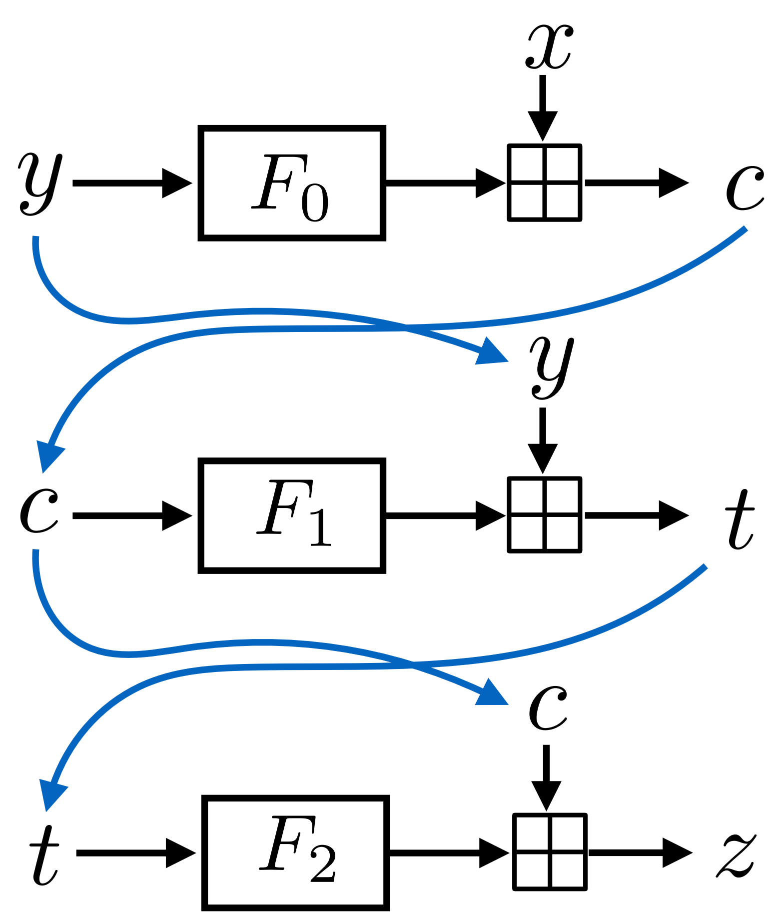
Are the round functions uniquely defined to encrypt messages?

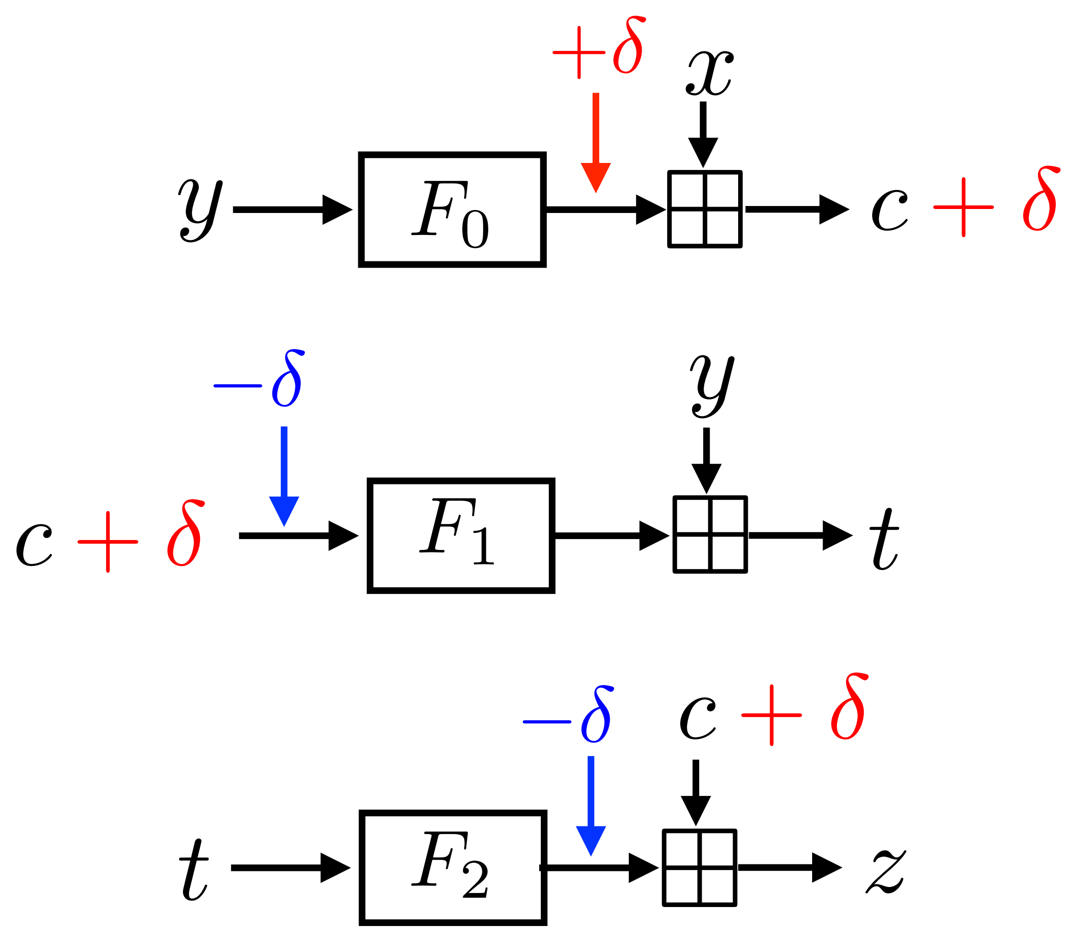




Equivalent Round Functions [BLP'15]

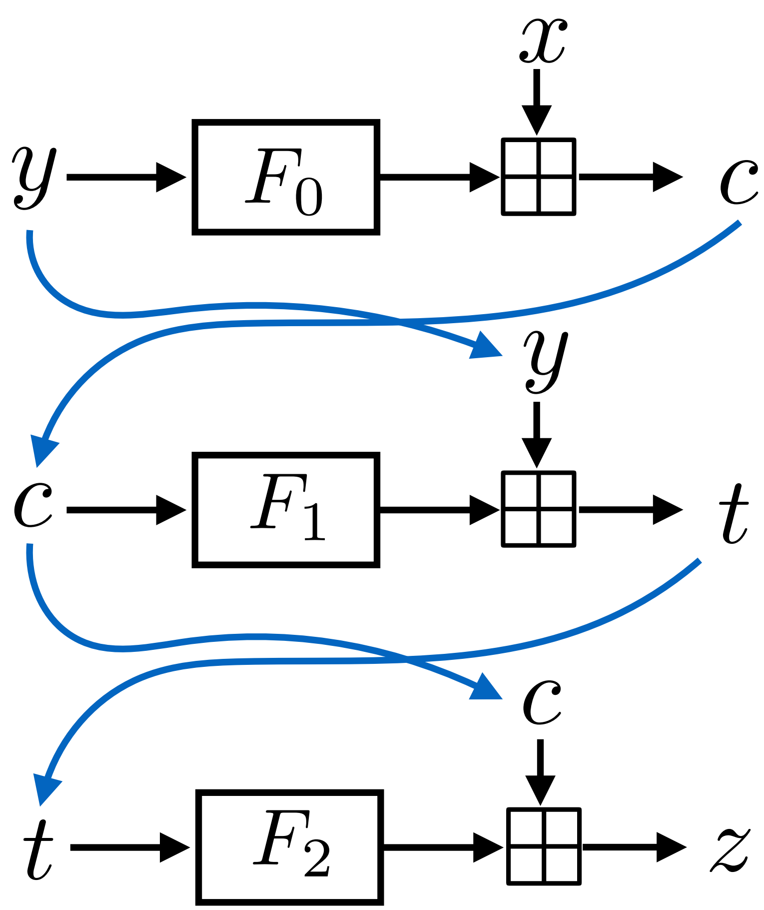
Are the round functions uniquely defined to encrypt messages?



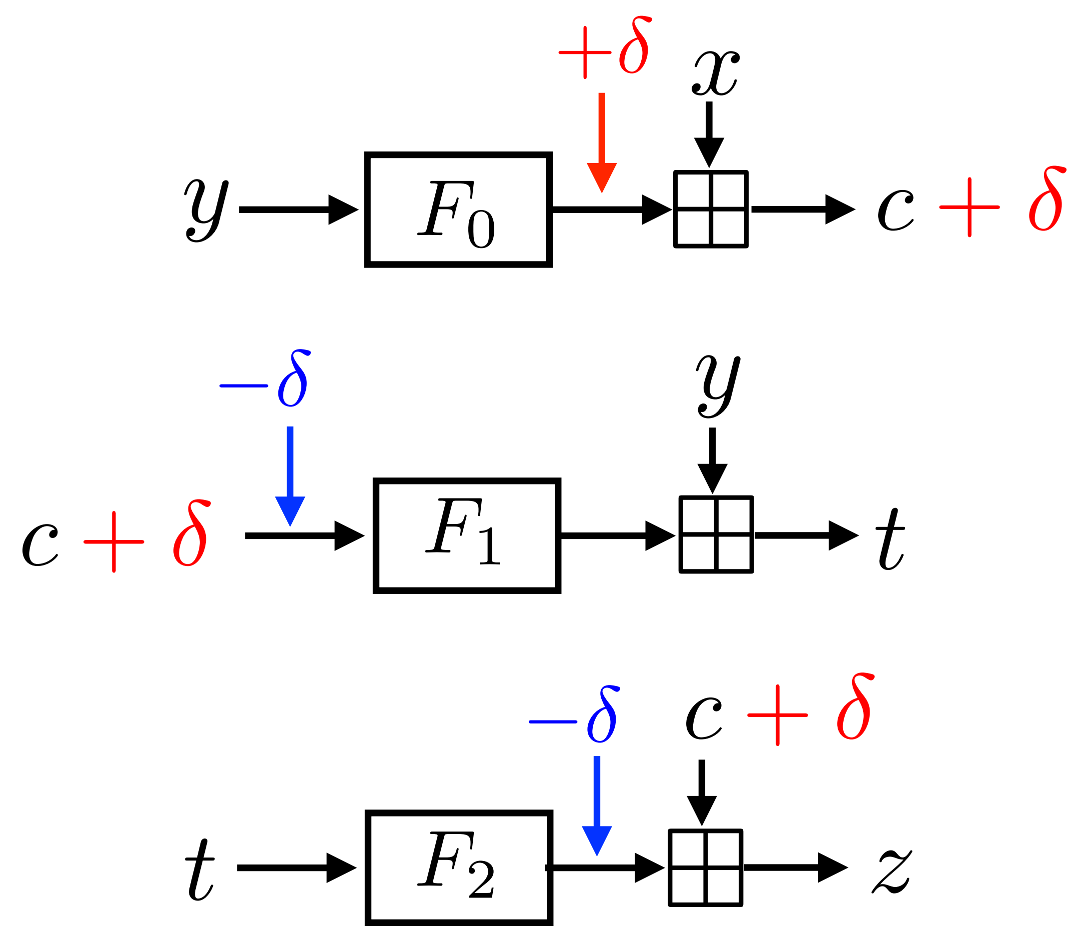


Equivalent Round Functions [BLP'15]

Are the round functions uniquely defined to encrypt messages?



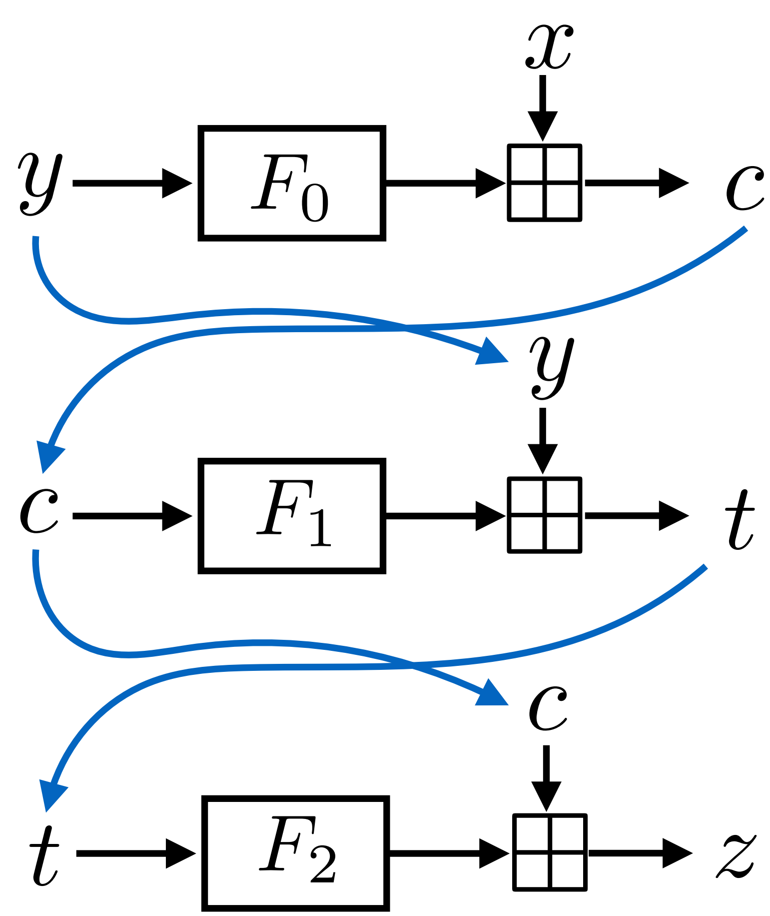
(F_0, F_1, F_2)

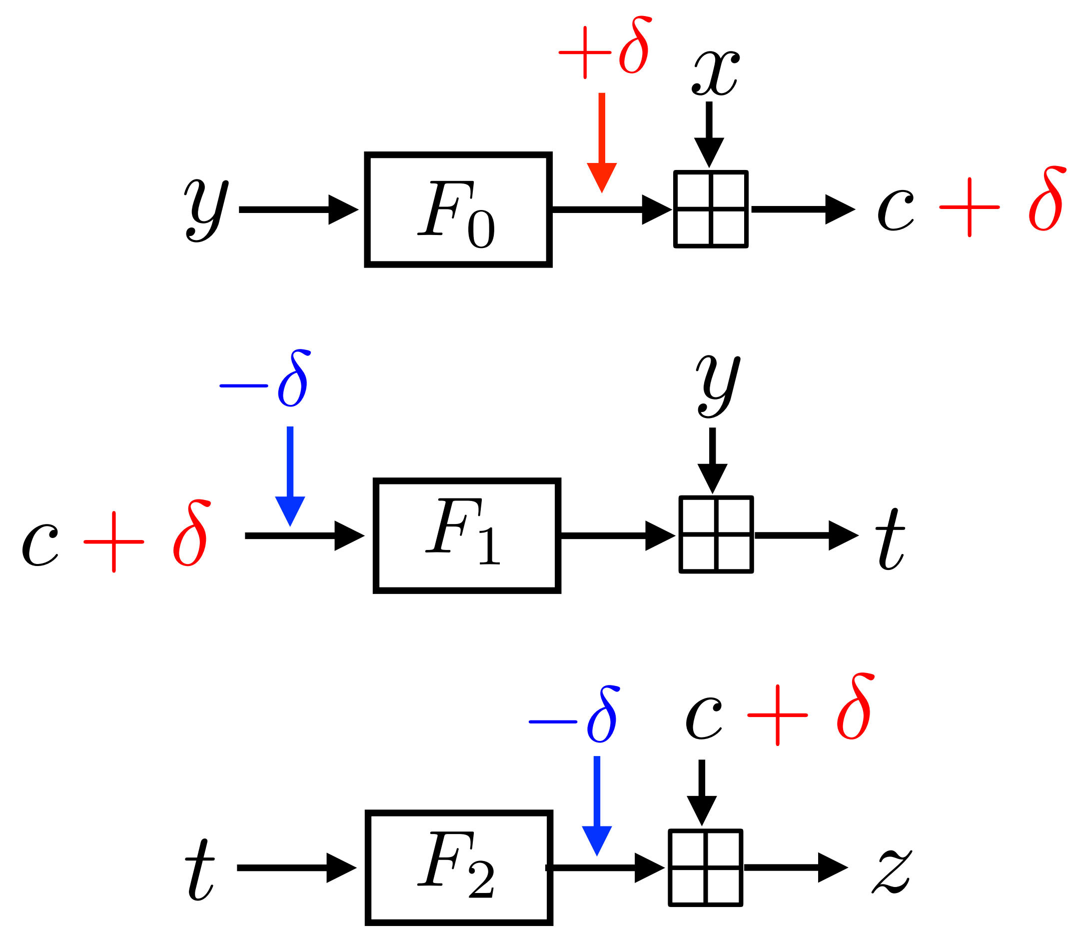


$(F_0(y) + \delta, F_1(c - \delta), F_2(t) - \delta)$

Equivalent Round Functions [BLP'15]

Are the round functions uniquely defined to encrypt messages?





$$(F_0, F_1, F_2)$$

$$(F_0(y) + \delta, F_1(c - \delta), F_2(t) - \delta)$$

The output of one arbitrary input y can be set arbitrarily in F_0, yet it still gives the same input/output behavior of (F_0, F_1, F_2).

Terminology

- attacker goal:
  - **round-function-recovery:** The adversary recovers the round functions or one of the equivalent set of round functions in a Feistel network.
  - **codebook-recovery:** The adversary can recover the mapping of each plaintext to its ciphertext.
  - Both attack goals are as powerful as secret key recovery.

Our Contributions, Part 1:
Generic Attacks on Feistel Networks

cite	r	attack type	attack goal	query	time
this work	3	**known-plaintext**	round-function-recovery	$N \ln N$	$N \ln N$

Our Contributions, Part 1:
Generic Attacks on Feistel Networks

cite	r	attack type	attack goal	query	time
this work	3	**known-plaintext**	round-function-recovery	$N \ln N$	$N \ln N$
this work	4	**known-plaintext**	round-function-recovery	$N^{\frac{3}{2}}$	N^3
[Biryukov-Leurent-Perrin'15]	4	chosen-plaintext and ciphertext	round-function-recovery	$N^{\frac{3}{2}}$	$N^{\frac{3}{2}}$

Our Contributions, Part 1: Generic Attacks on Feistel Networks

cite	r	attack type	attack goal	query	time
this work	3	**known-plaintext**	round-function-recovery	$N \ln N$	$N \ln N$
this work	4	**known-plaintext**	round-function-recovery	$N^{\frac{3}{2}}$	N^3
[Biryukov-Leurent-Perrin'15]	4	chosen-plaintext and ciphertext	round-function-recovery	$N^{\frac{3}{2}}$	$N^{\frac{3}{2}}$
this work	5	**chosen-plaintext**	round-function-recovery	$N^{\frac{3}{2}}$	$N^{O(N^{\frac{1}{2}})}$
[Biryukov-Leurent-Perrin'15]	5	chosen-plaintext and ciphertext	round-function-recovery	N^2	$N^{N^{\frac{3}{4}}}$
this work	≥6	**chosen-plaintext**	round-function-recovery	$N^{\frac{3}{2}}$	$N^{(r-5)N}$

Our Contributions, Part 1:
Generic Attacks on Feistel Networks

cite	r	attack type	attack goal	query	time
this work	3	**known-plaintext**	round-function-recovery	$N \ln N$	$N \ln N$
this work	4	**known-plaintext**	round-function-recovery	$N^{\frac{3}{2}}$	N^3
[Biryukov-Leuren-Perrin'15]	4	chosen-plaintext and ciphertext	round-function-recovery	$N^{\frac{3}{2}}$	$N^{\frac{3}{2}}$
this work	5	**chosen-plaintext**	round-function-recovery	$N^{\frac{3}{2}}$	$N^{O(N^{\frac{1}{2}})}$
[Biryukov-Leurent-Perrin'15]	5	chosen-plaintext and ciphertext	round-function-recovery	N^2	$N^{N^{\frac{3}{4}}}$
this work	≥6	**chosen-plaintext**	round-function-recovery	$N^{\frac{3}{2}}$	$N^{(r-5)N}$

The Sketch of 3-round Attack

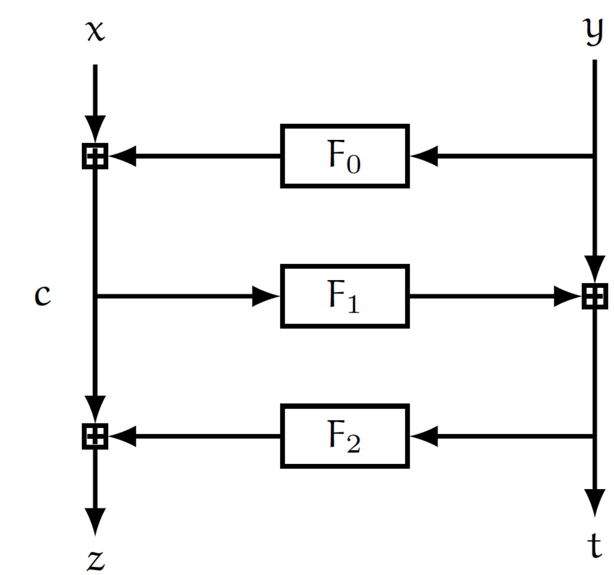
input: The set S that consists of ($x_k y_k z_k t_k$) pairs with unknown intermediate values c_k.

output: (partial) tables for F_0, F_1, F_2.

F_0	
0	
1	
⋮	⋮
y_1	
⋮	⋮
y_0	
⋮	⋮
y_k	
⋮	⋮
N-1	

F_1	
0	
1	
⋮	⋮
c_1	
⋮	⋮
c_2	
⋮	⋮
c_0	
⋮	⋮
N-1	

F_2	
0	
1	
⋮	⋮
t_2	
⋮	⋮
t_0	
⋮	⋮
t_k	
⋮	⋮
N-1	



The Sketch of 3-round Attack

input: The set S that consists of $(x_k y_k z_k t_k)$ pairs with unknown intermediate values c_k.

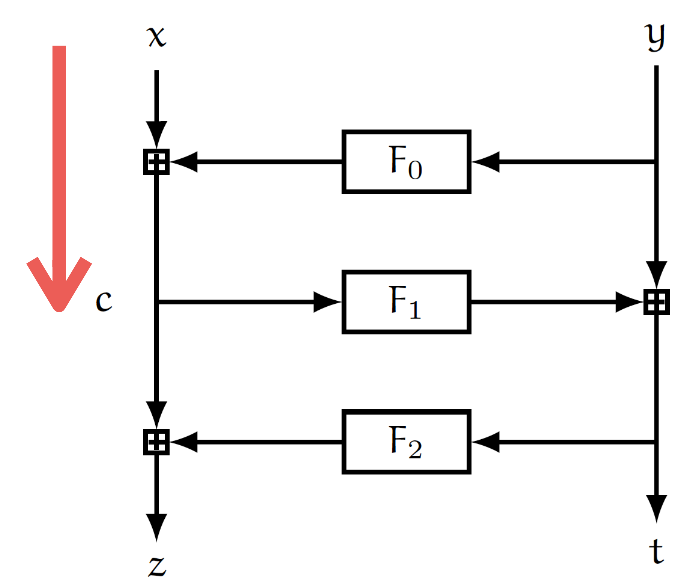
output: (partial) tables for F_0, F_1, F_2.

Pick a pair $(x_0 y_0 z_0 t_0)$ arbitrarily. Set $F_0(y_0)=0$.

F_0	
0	
1	
⋮	⋮
y_1	
⋮	⋮
y_0	0
⋮	⋮
y_k	
⋮	⋮
N-1	

F_1	
0	
1	
⋮	⋮
c_1	
⋮	⋮
c_2	
⋮	⋮
c_0	2
⋮	⋮
N-1	

F_2	
0	
1	
⋮	⋮
t_2	
⋮	⋮
t_0	25
⋮	⋮
t_k	
⋮	⋮
N-1	



$c = x + F_0(y)$

$F_1(c) = t - y$

$F_2(t) = z - c$

The Sketch of 3-round Attack

input: The set S that consists of $(x_k y_k z_k t_k)$ pairs with unknown intermediate values c_k.

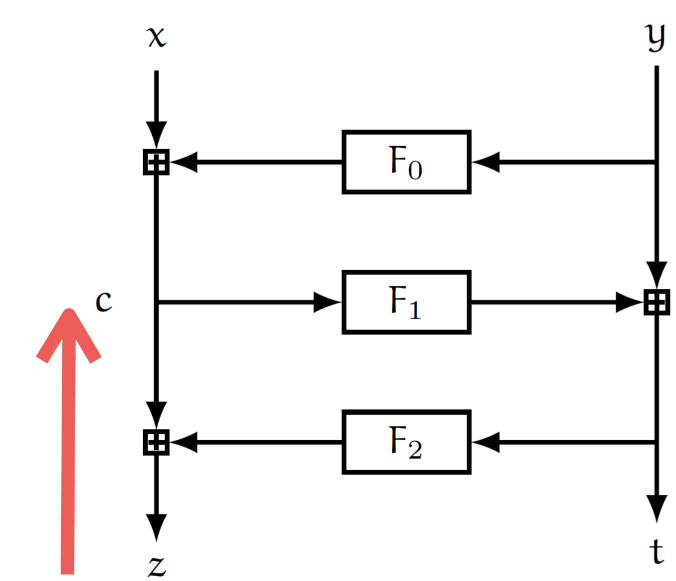
output: (partial) tables for F_0, F_1, F_2.

Pick another pair $(x_1 y_1 z_1 t_1)$ with $t_1 = t_0$

F_0	
0	
1	
⋮	⋮
y_1	32
⋮	⋮
y_0	0
⋮	⋮
y_k	
⋮	⋮
N-1	

F_1	
0	
1	
⋮	⋮
c_1	14
⋮	⋮
c_2	
⋮	⋮
c_0	2
⋮	⋮
N-1	

F_2	
0	
1	
⋮	⋮
t_2	
⋮	⋮
$t_0=t_1$	25
⋮	⋮
t_k	
⋮	⋮
N-1	



$c = x + F_0(y)$

$F_1(c) = t - y$

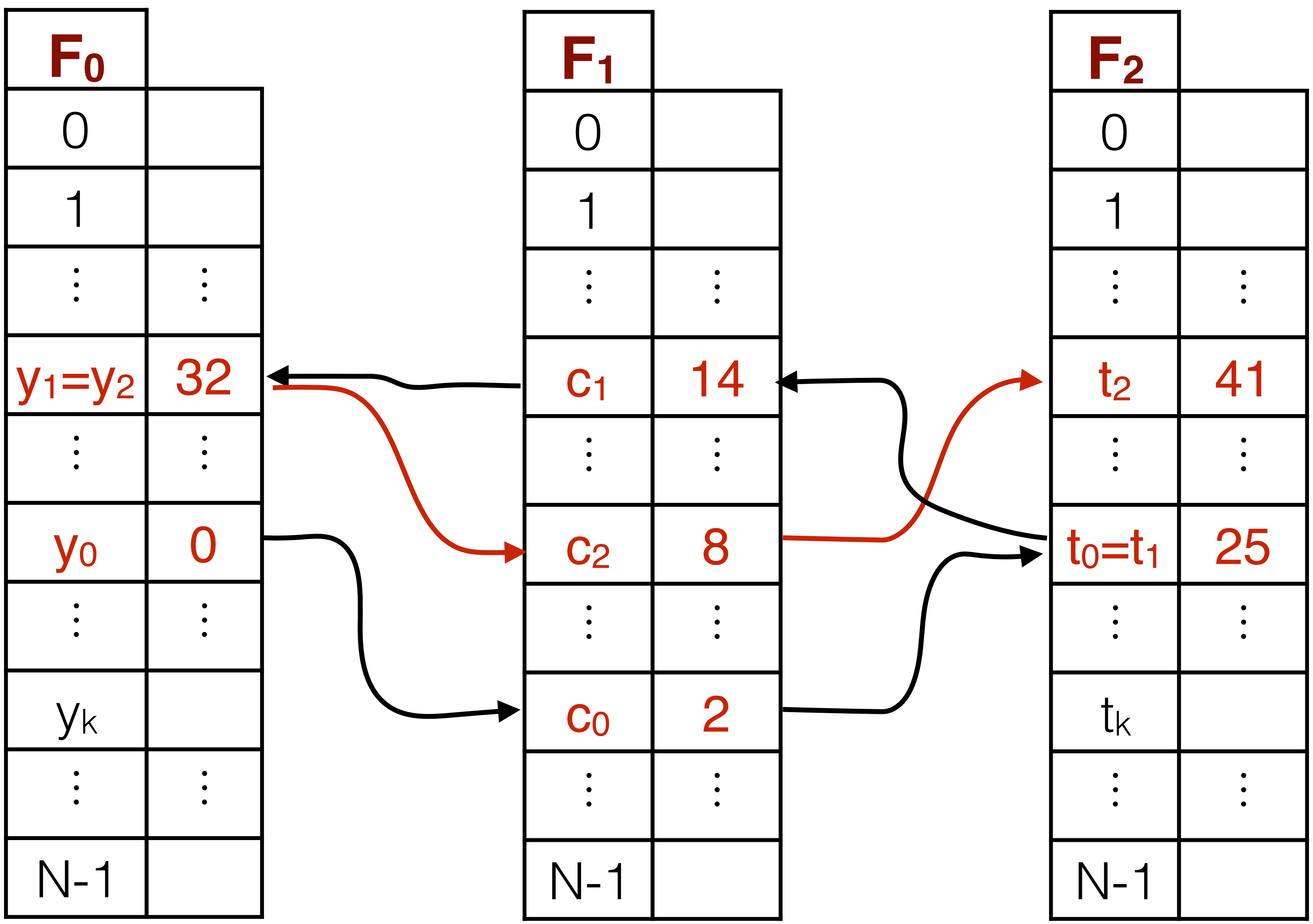
$F_2(t) = z - c$

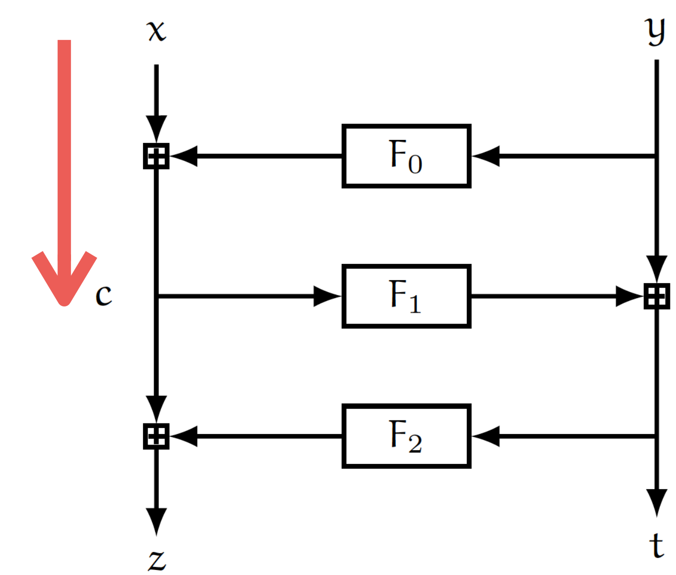
The Sketch of 3-round Attack

input: The set S that consists of $(x_k y_k z_k t_k)$ pairs with unknown intermediate values c_k.

output: (partial) tables for F_0, F_1, F_2.

Pick a third pair $(x_2 y_2 z_2 t_2)$ with $y_2 = y_1$





$c = x + F_0(y)$

$F_1(c) = t - y$

$F_2(t) = z - c$

The Sketch of 3-round Attack

output: (partial) tables for F_0,F_1,F_2.

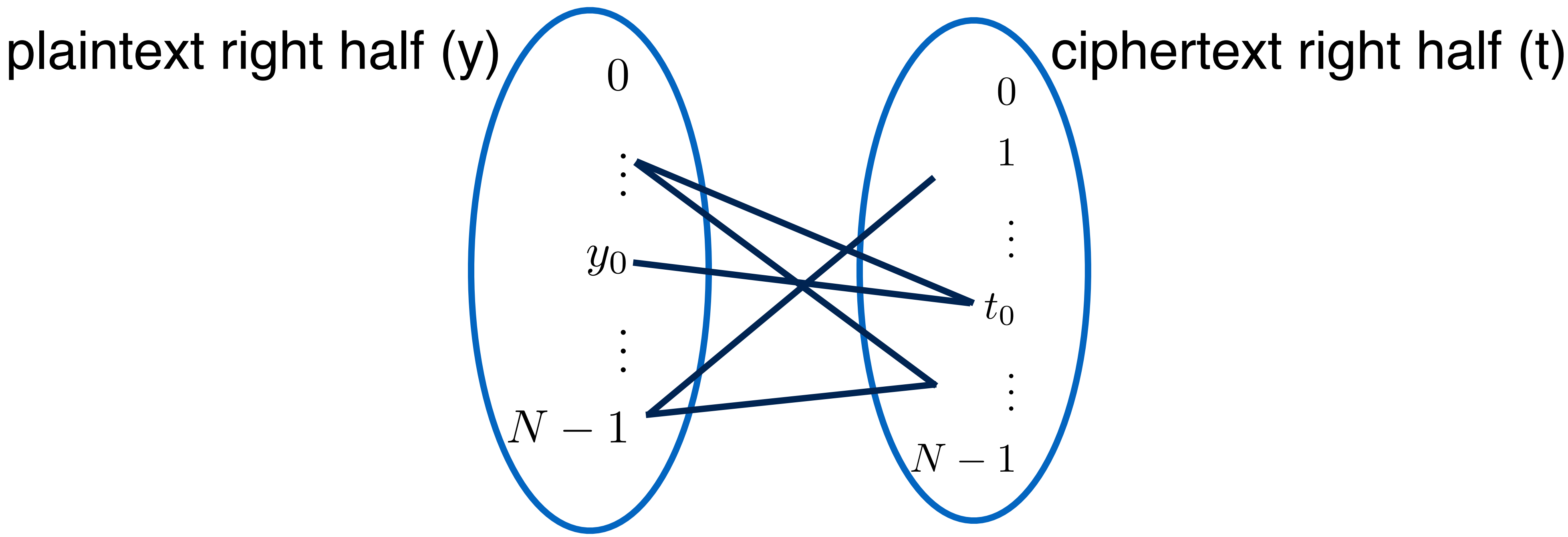
Continue yo-yo game until no more revealed.

F_0	
0	
1	12
⋮	⋮
y_1	32
⋮	⋮
y_0	0
⋮	⋮
y_k	92
⋮	⋮
N-1	6

F_1	
0	56
1	
⋮	⋮
c_1	14
⋮	⋮
c_2	8
⋮	⋮
c_0	2
⋮	⋮
N-1	7

F_2	
0	5
1	87
⋮	⋮
t_2	41
⋮	⋮
t_0	25
⋮	⋮
t_k	1
⋮	⋮
N-1	65

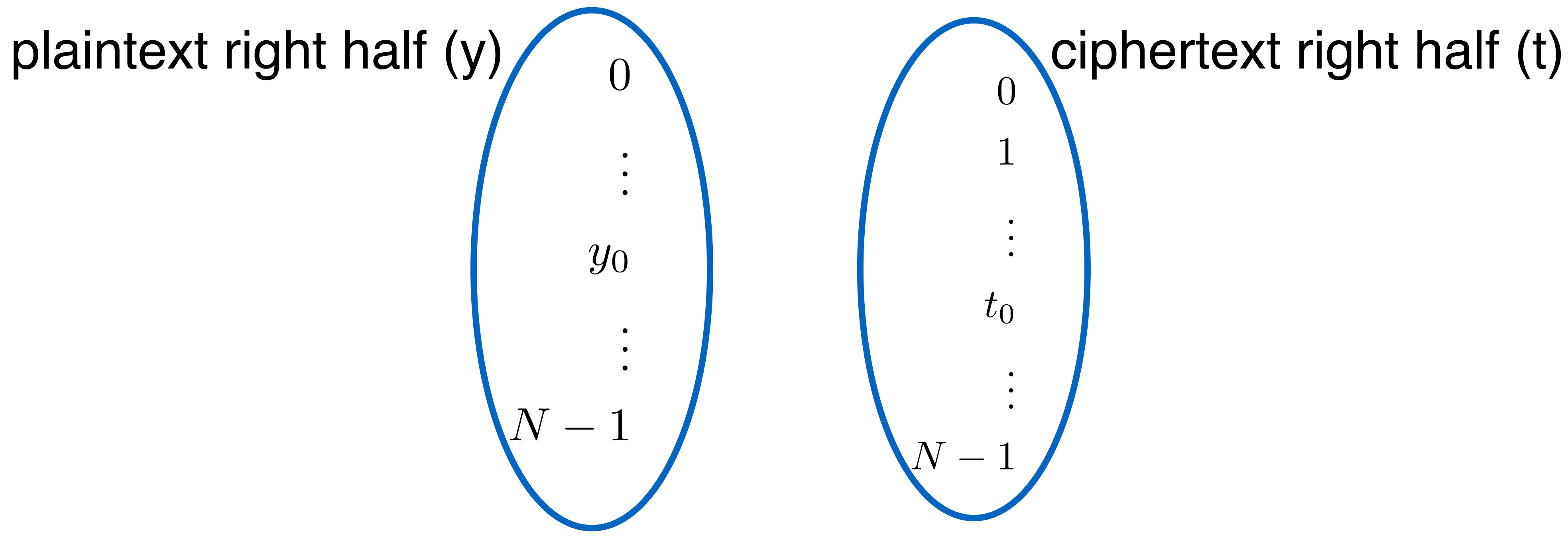
3-round Attack on Feistel Networks



input: The set S that consists of ($x_k y_k z_k t_k$) pairs.

- Model the set S as a bipartite graph:
  - vertices: two parties of N values of **all** possible **y** and **t**.
  - edges: each (x**y**z**t**) pair from pairs in S that forms an edge.

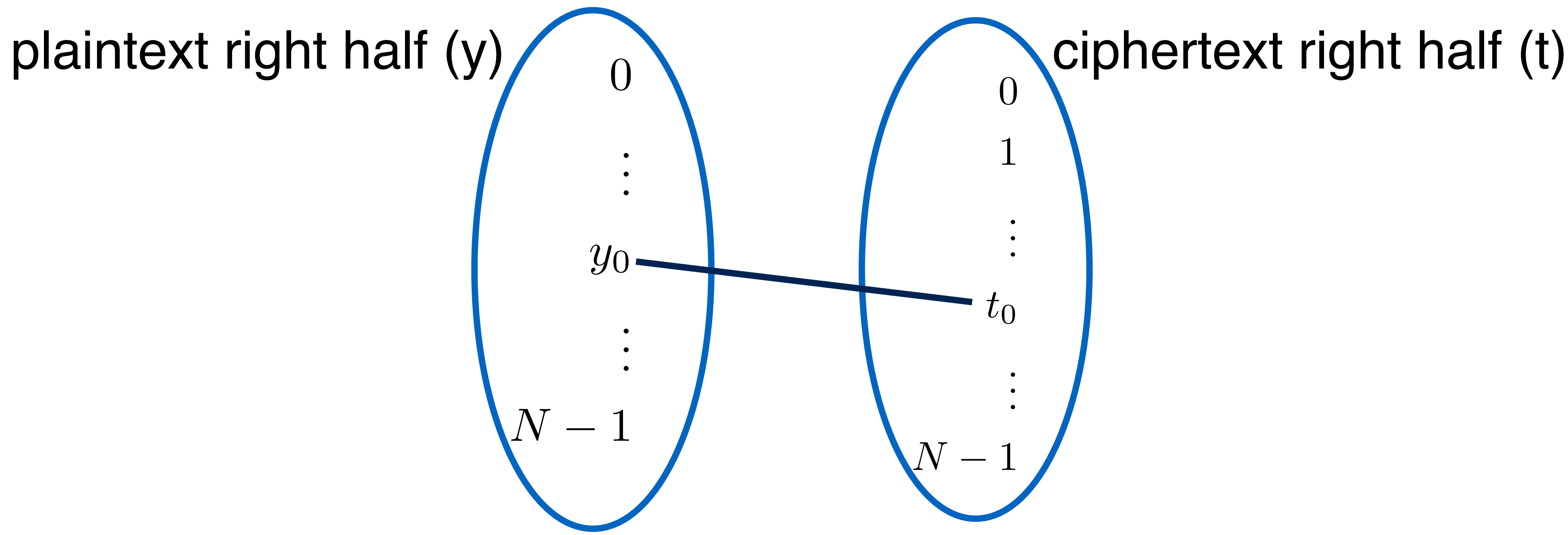
3-round Attack on Feistel Networks



input: The set S that consists of ($x_k y_k z_k t_k$) pairs.

- Model the set S as a bipartite graph:
  - vertices: two parties of N values of **all** possible **y** and **t**.
  - edges: each (x**y**z**t**) pair from pairs in S that forms an edge.
- The algorithm looks for the connected component starting from an arbitrary vertex y_0 that the algorithm starts with.

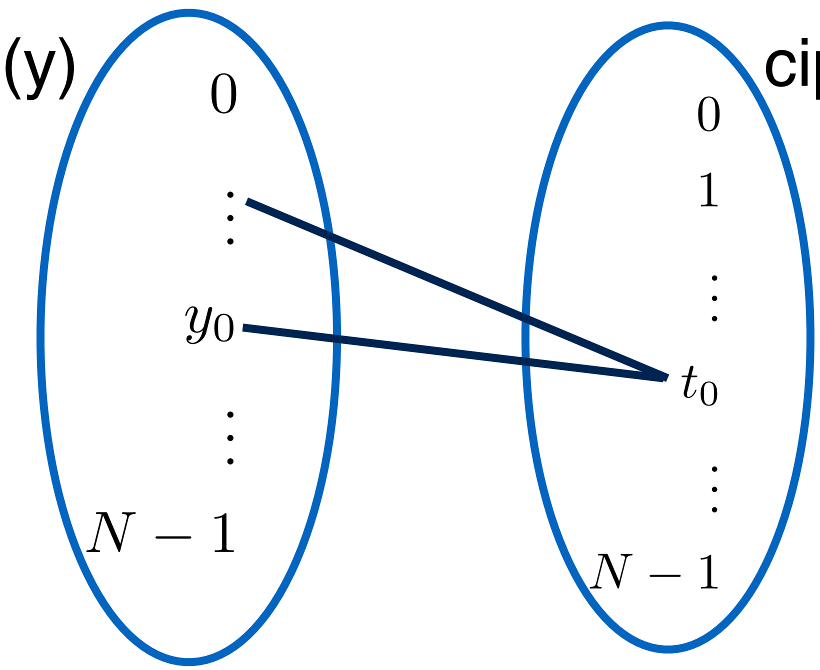
3-round Attack on Feistel Networks



input: The set S that consists of ($x_k y_k z_k t_k$) pairs.

- Model the set S as a bipartite graph:
  - vertices: two parties of N values of **all** possible **y** and **t**.
  - edges: each (x**y**z**t**) pair from pairs in S that forms an edge.
- The algorithm looks for the connected component starting from an arbitrary vertex y_0 that the algorithm starts with.

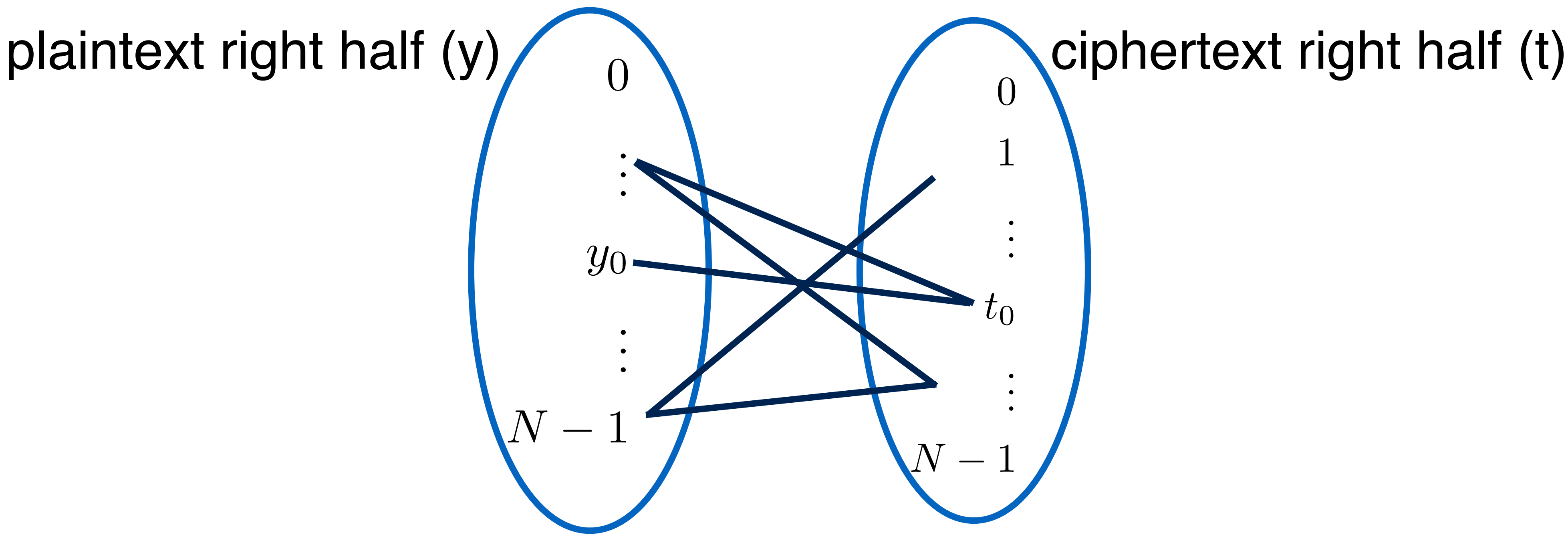
3-round Attack on Feistel Networks



input: The set S that consists of ($x_k y_k z_k t_k$) pairs.

- Model the set S as a bipartite graph:
  - vertices: two parties of N values of **all** possible **y** and **t**.
  - edges: each (x**y**z**t**) pair from pairs in S that forms an edge.
- The algorithm looks for the connected component starting from an arbitrary vertex y_0 that the algorithm starts with.

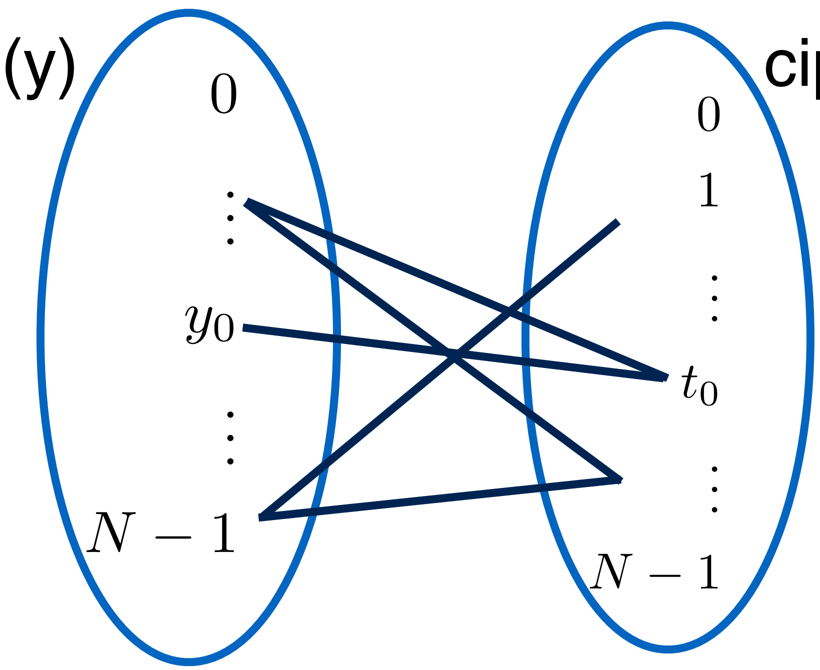
3-round Attack on Feistel Networks



input: The set S that consists of ($x_k y_k z_k t_k$) pairs.

- Model the set S as a bipartite graph:
  - vertices: two parties of N values of **all** possible **y** and **t**.
  - edges: each (x**y**z**t**) pair from pairs in S that forms an edge.
- The algorithm looks for the connected component starting from an arbitrary vertex y_0 that the algorithm starts with.

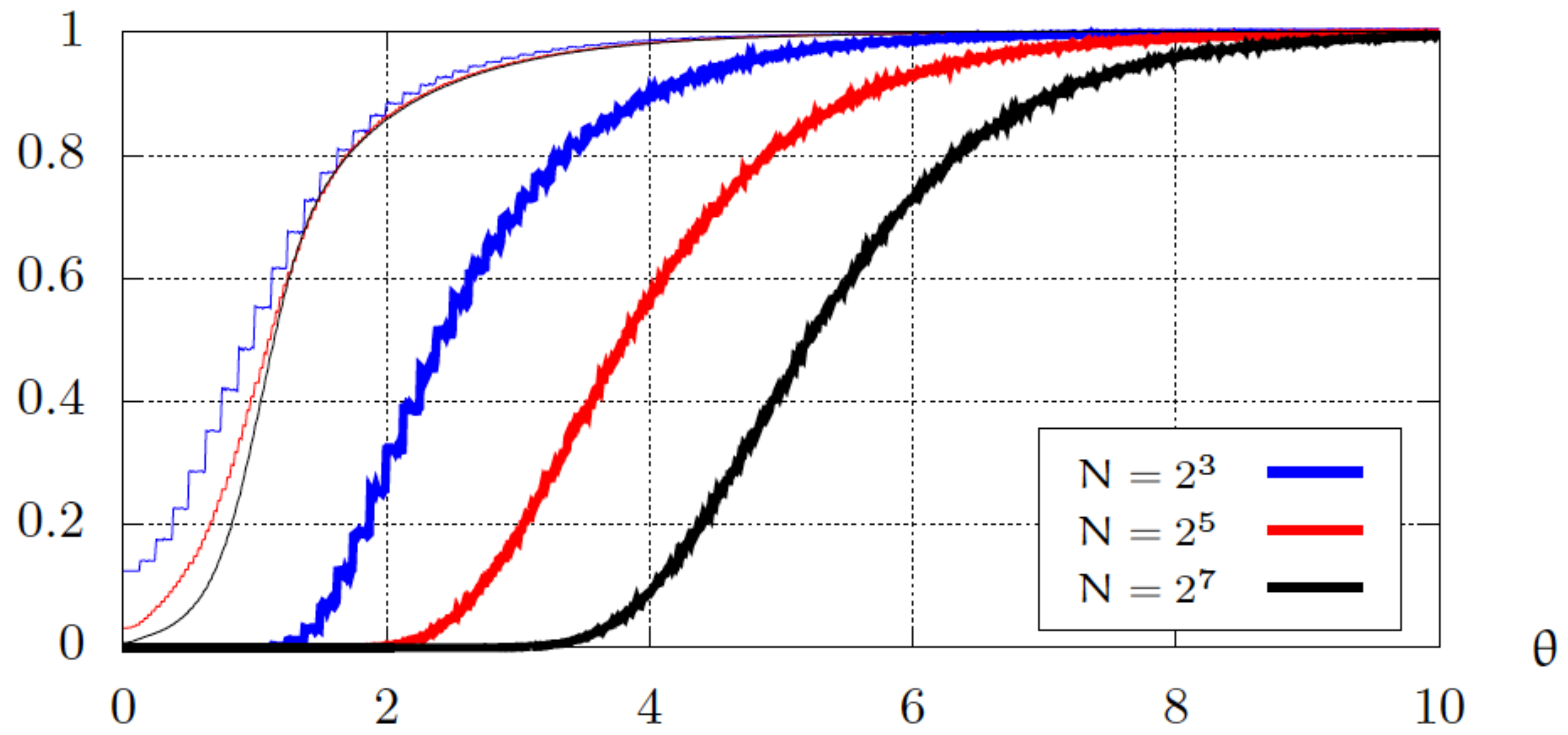
3-round Attack on Feistel Networks



input: The set S that consists of ($x_k y_k z_k t_k$) pairs.

- Model the set S as a bipartite graph:
  - vertices: two parties of N values of **all** possible **y** and **t**.
  - edges: each (x**y**z**t**) pair from pairs in S that forms an edge.
- The algorithm looks for the connected component starting from an arbitrary vertex y_0 that the algorithm starts with.
- The graph is fully connected if the size of S is $N \ln N$.
- The graph has a giant connected component if the size of S is N

Experimental Results



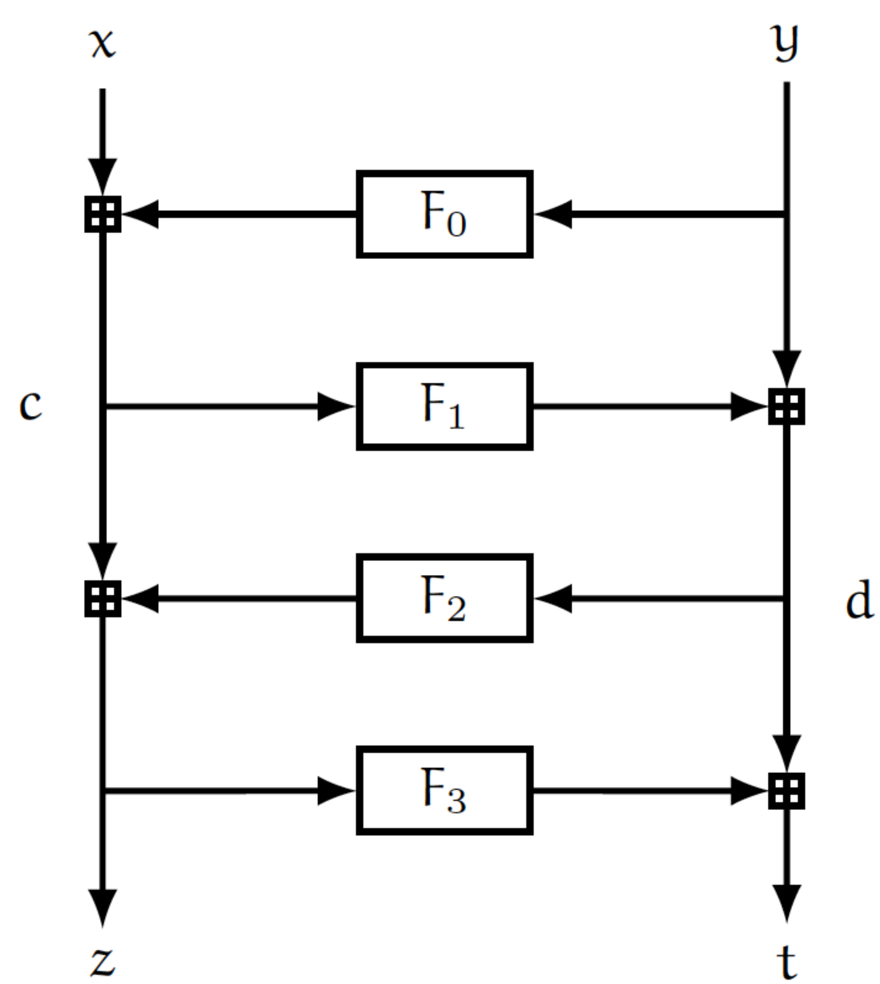
Let $|S| = \theta N$.

thin: The fraction of recovered F_0 depending on θ.

thick: The fraction of experiments which fully recovers all functions over 10,000 independent runs.

The Principle of 4-round Attack on Feistel Networks

- If we characterize F_0, then we can find intermediate c values.
  - If enough intermediate c values are known, we can run our 3-round attack.
- Again: We can set an output of F_0 on an arbitrary point.



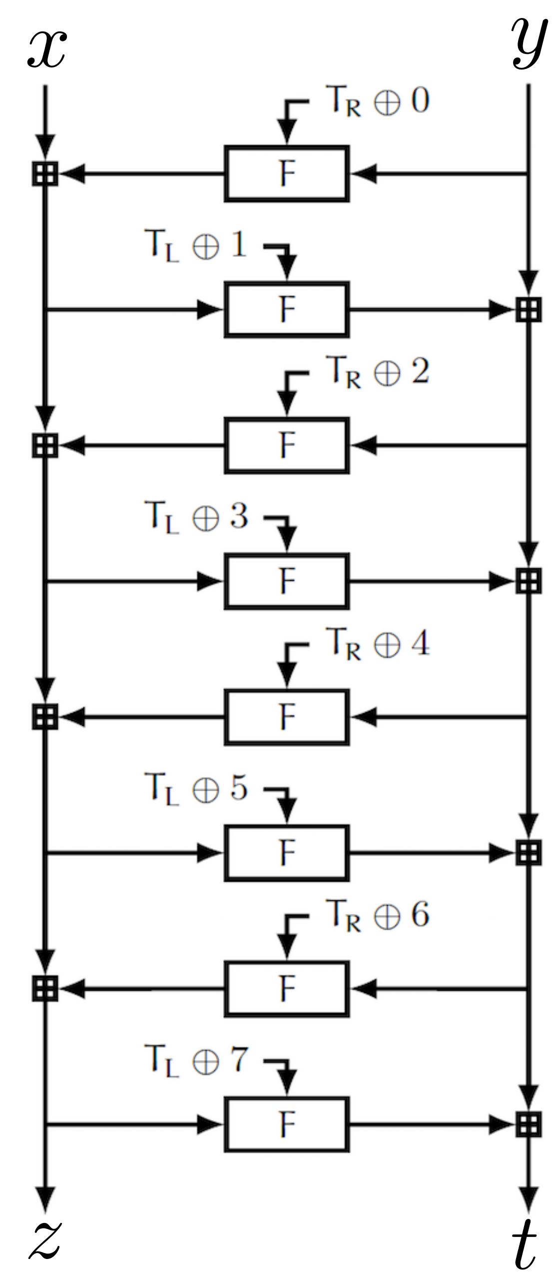
Experimental Results

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

N	M	#trials	Pr[succ]
4	9	3864	3.60%
8	29	5791	29.11%
16	91	6585	49.83%
32	288	6814	62.91%
64	913	6981	73.80%
128	2897	6609	83.10%
256	9196	3154	89.22%
512	29193	212	92.45%

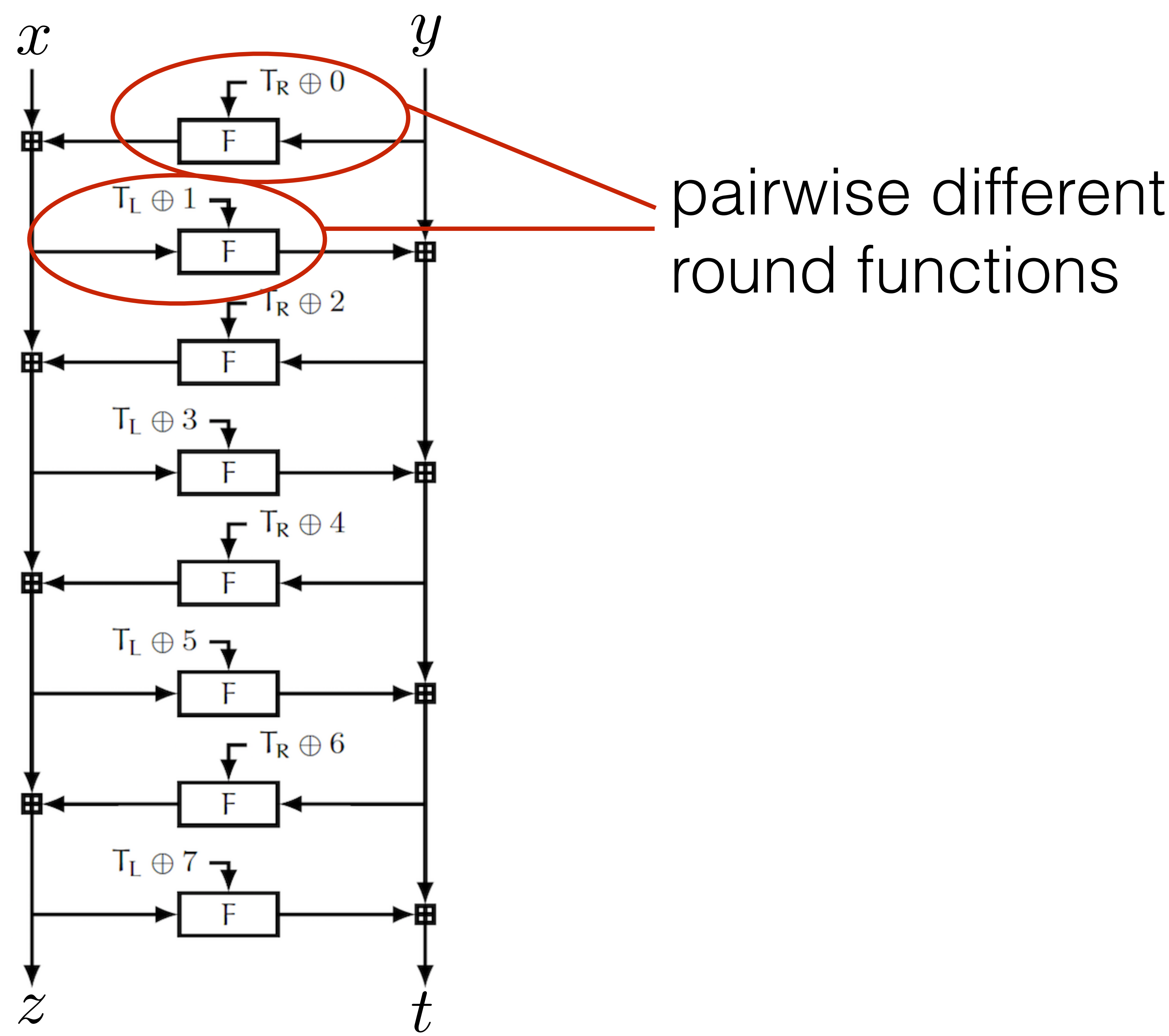
N: the domain size to a round function.
M: query complexity with a parameter **L**.
trials: independent runs of the attack.
succ: entire round functions have been recovered.

Quick Look: FF3 Encryption



FF3 with tweak
$T = (T_L, T_R)$

Quick Look: FF3 Encryption

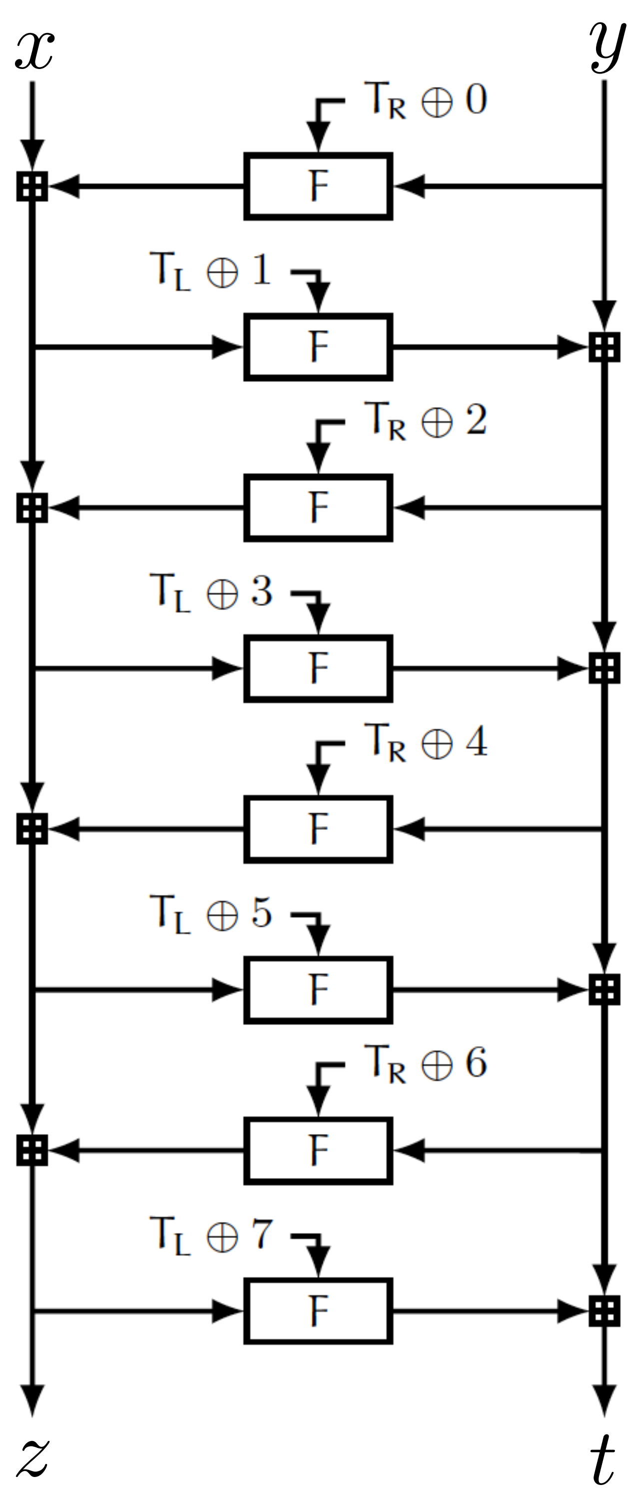


FF3 with tweak
$T = (T_L, T_R)$

Our Contributions, Part 2: Slide Attacks on FF3 Standard

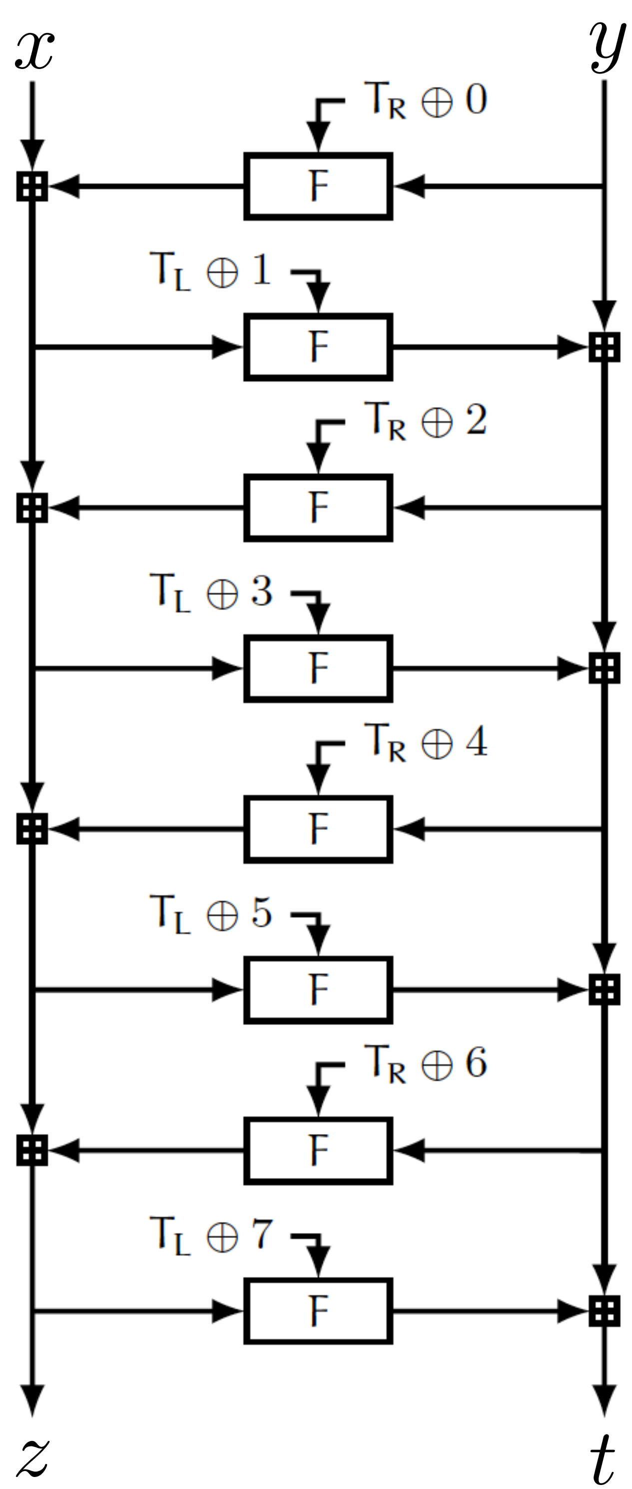
cite	construction	attack type	attack goal	query	time	#tweaks
this work	FF3 (8-round tweakable Feistel Network)	chosen-plaintext	round-function-recovery	$O(N^{\frac{11}{6}})$	$O(N^5)$	2
[Bellare-Hoang-Tessaro'16]	FF3 & FF1 (8 &10-round tweakable Feistel Network)	chosen-plaintext	partial-message-recovery (left half)	3	$O(\log(N)N^{r-3})$	

Slide Attack

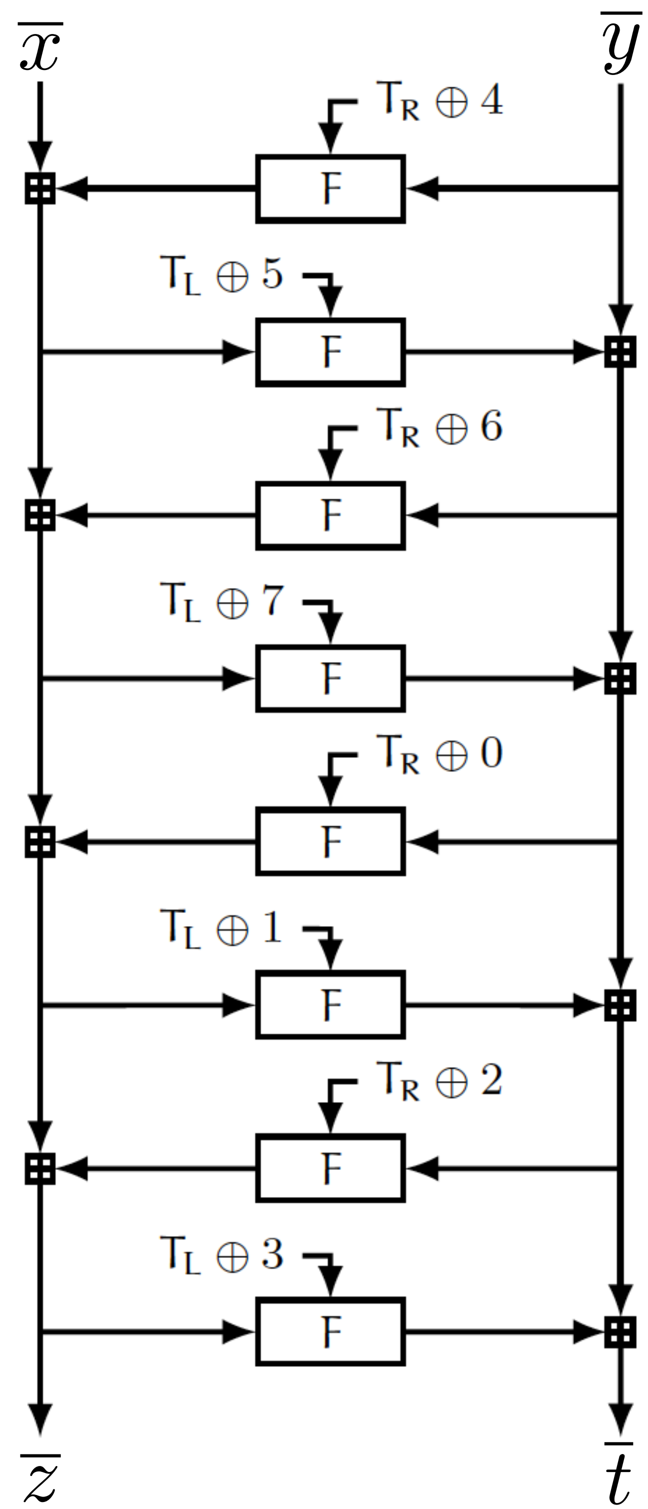


FF3 with tweak
$T = (T_L, T_R)$

Slide Attack

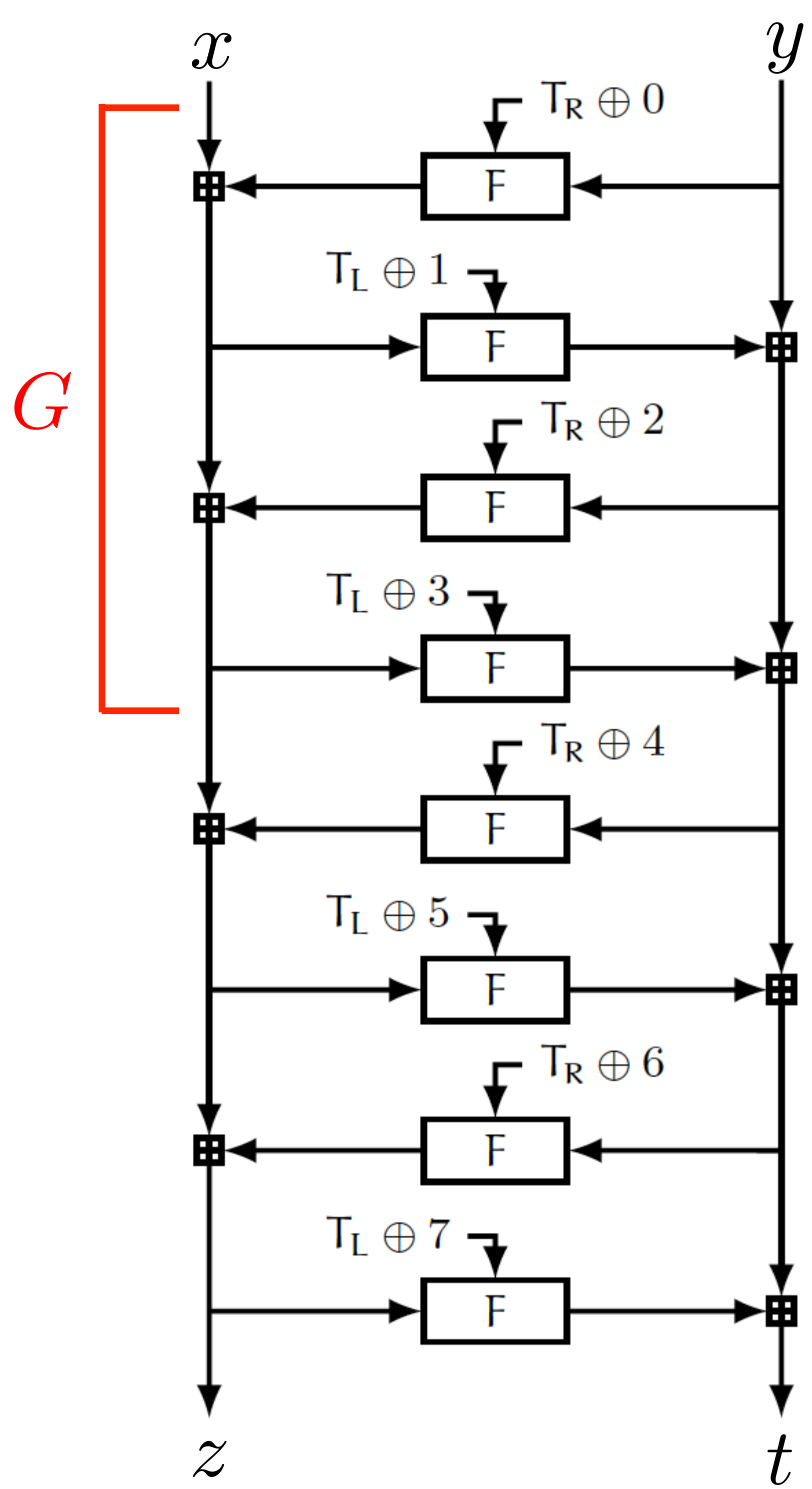


FF3 with tweak
$T = (T_L, T_R)$

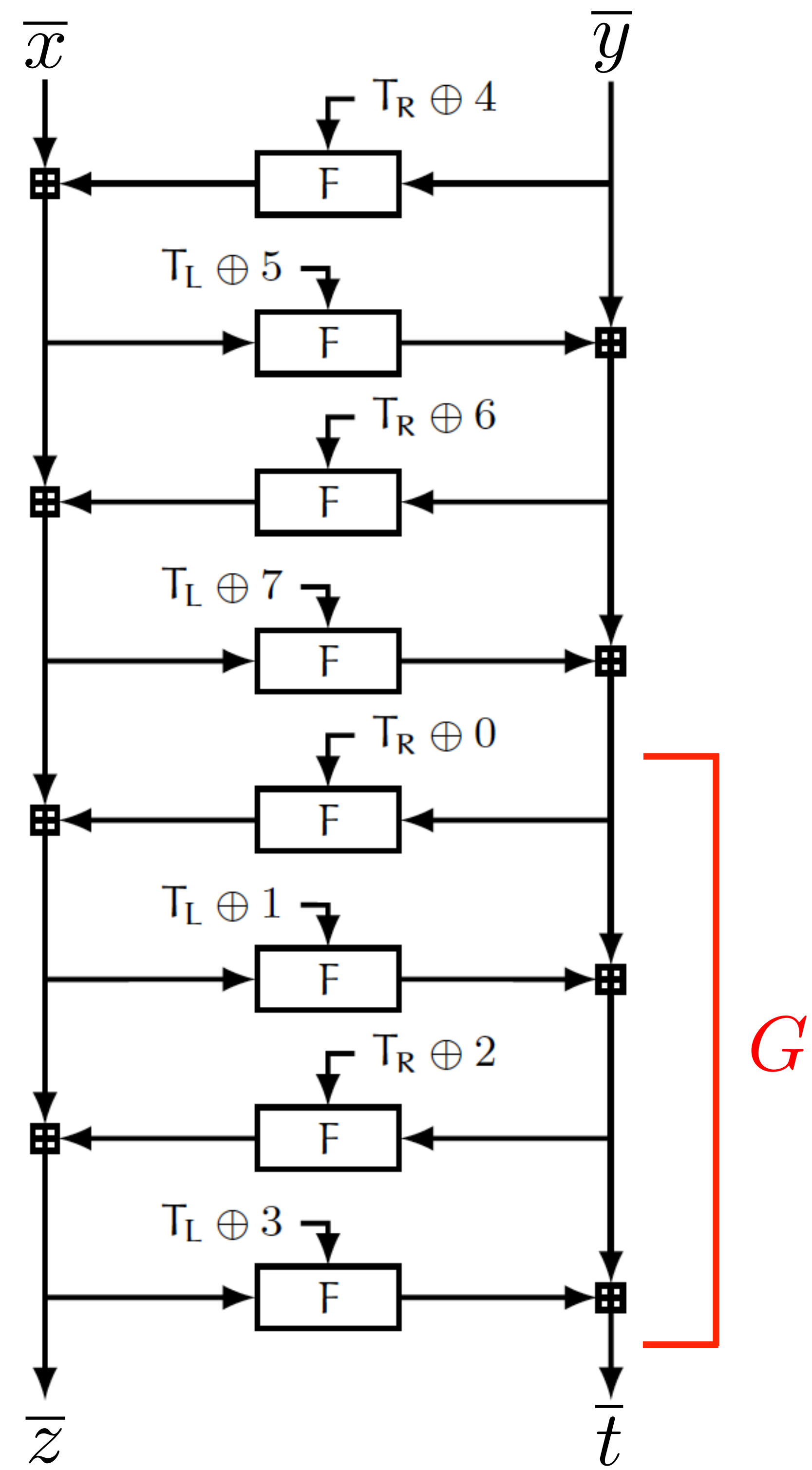


FF3 with tweak
$T' = (T_L, T_R) \oplus (4, 4)$

Slide Attack

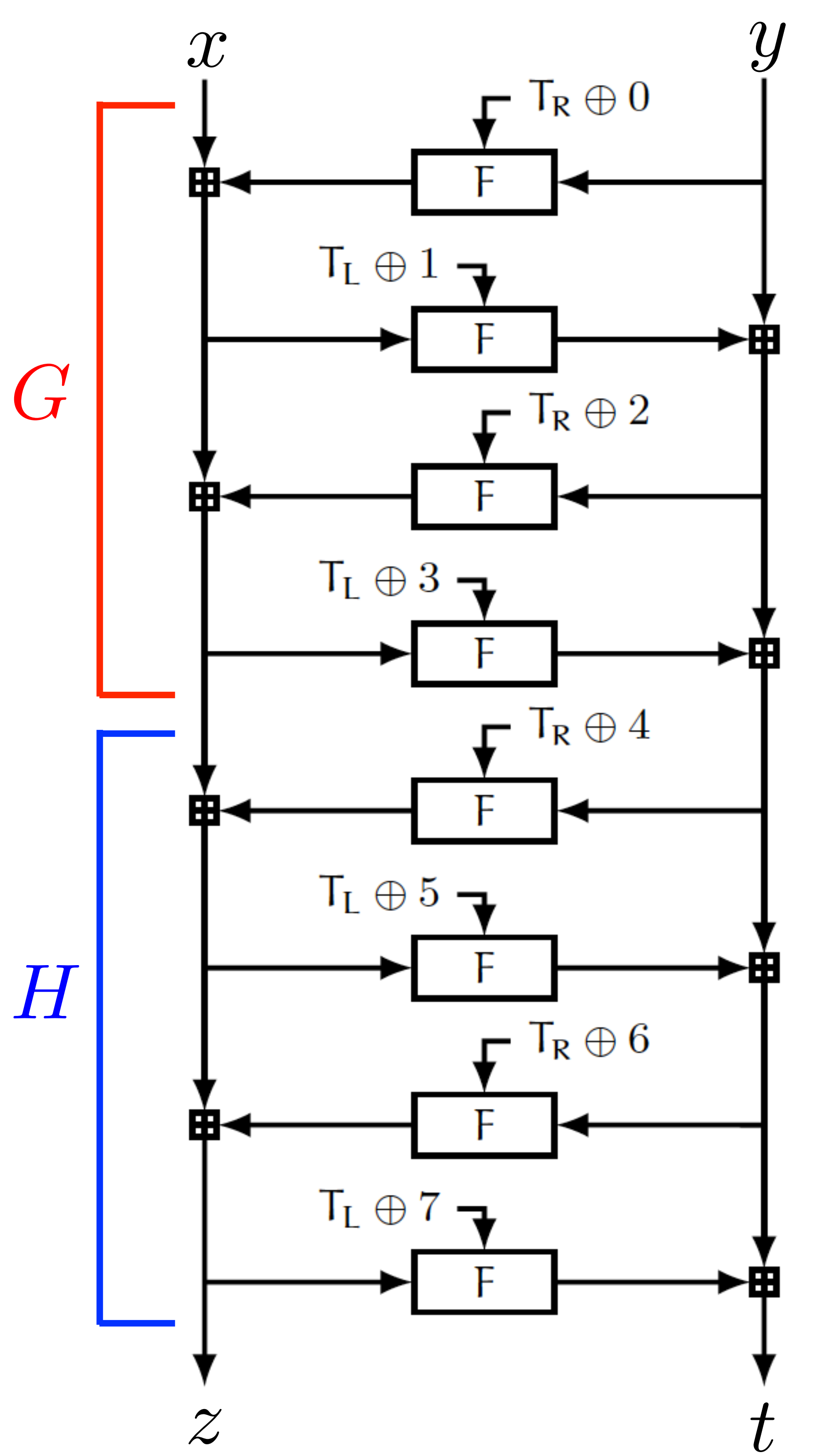


FF3 with tweak
$T = (T_L, T_R)$

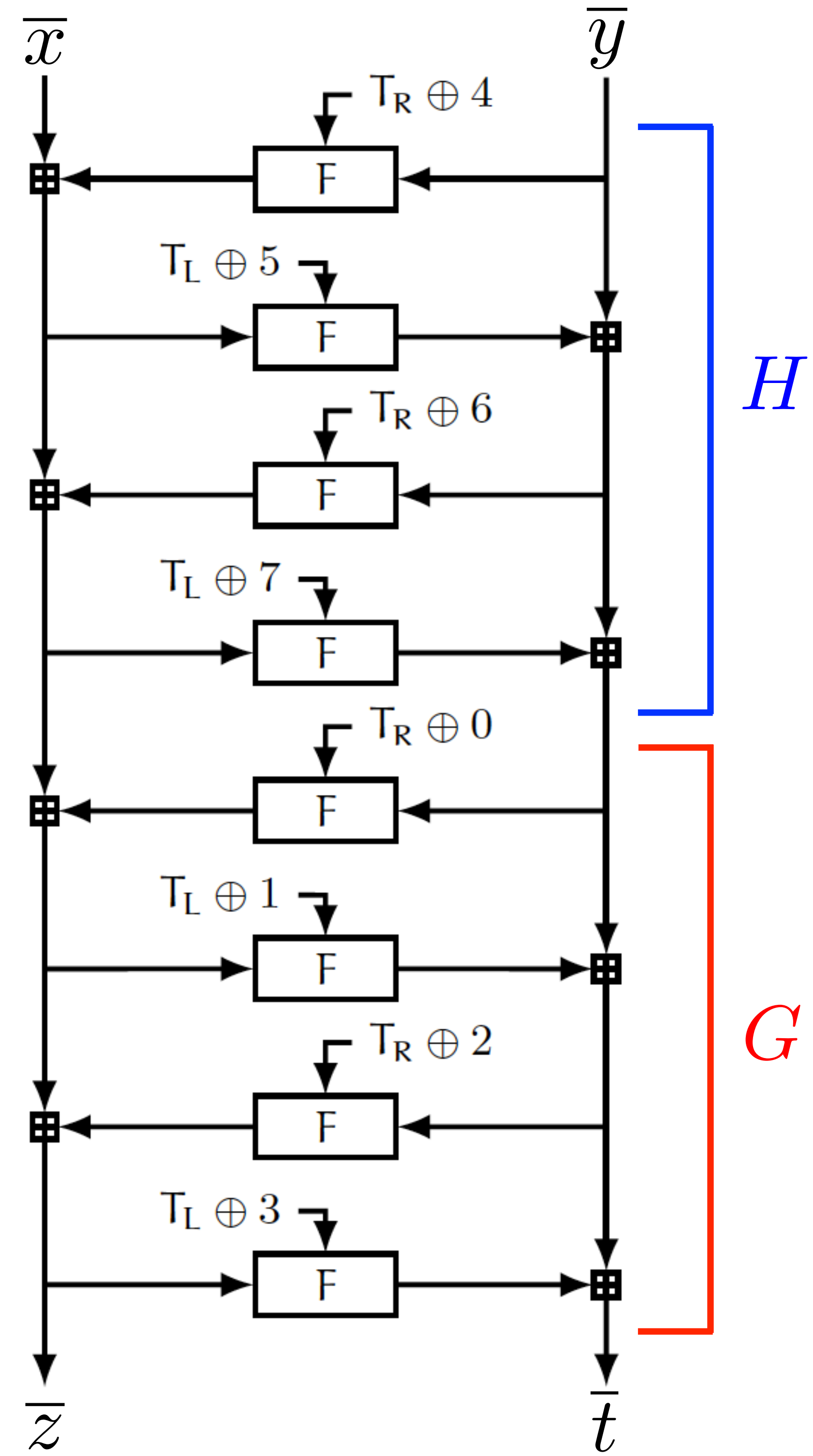


FF3 with tweak
$T' = (T_L, T_R) \oplus (4, 4)$

Slide Attack



FF3 with tweak
$T = (T_L, T_R)$



FF3 with tweak
$T' = (T_L, T_R) \oplus (4, 4)$

Chosen Plaintext Attack on FF3

xy_0^1

Chosen Plaintext Attack on FF3

$$E_K^T = H \circ G$$

$$xy_0^1$$

$H \circ G$

$$xy_1^1$$

$H \circ G$

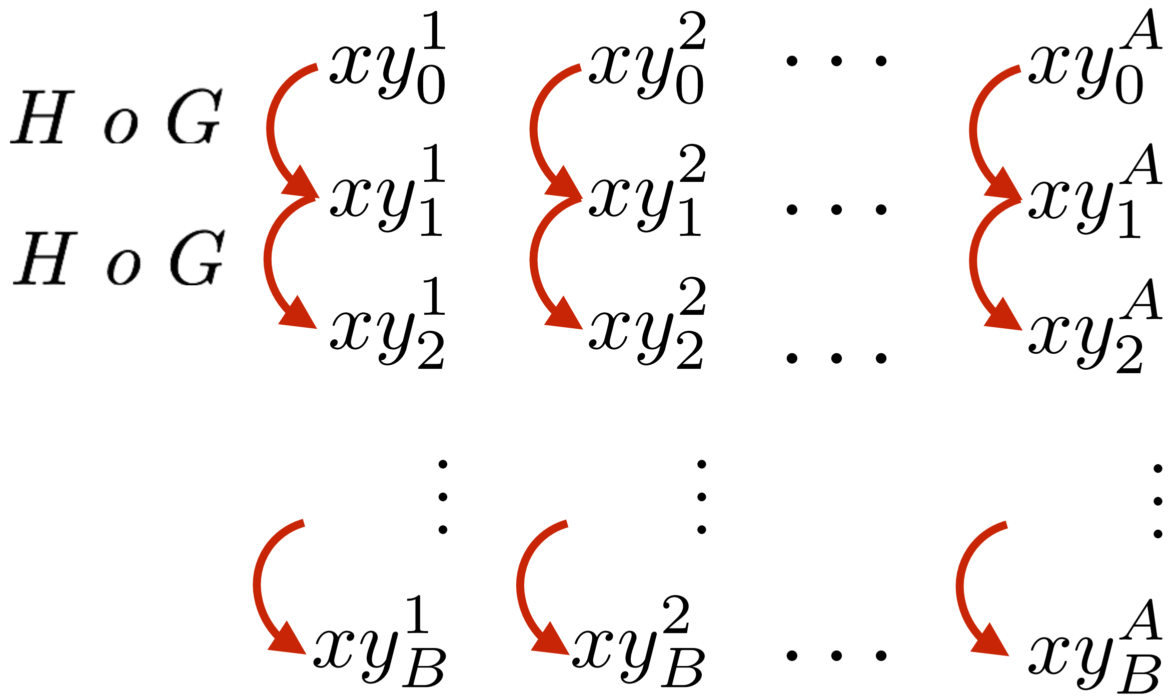
$$xy_2^1$$

$$\vdots$$

$$xy_B^1$$

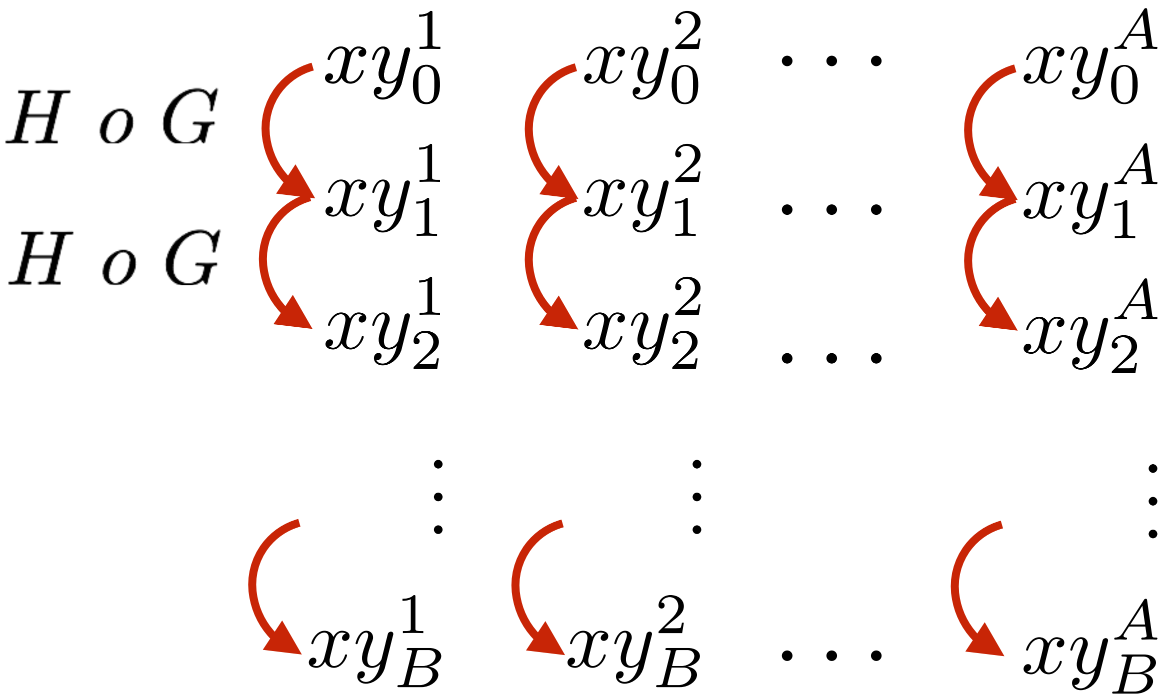
Chosen Plaintext Attack on FF3

$$E_K^T = H \; o \; G$$

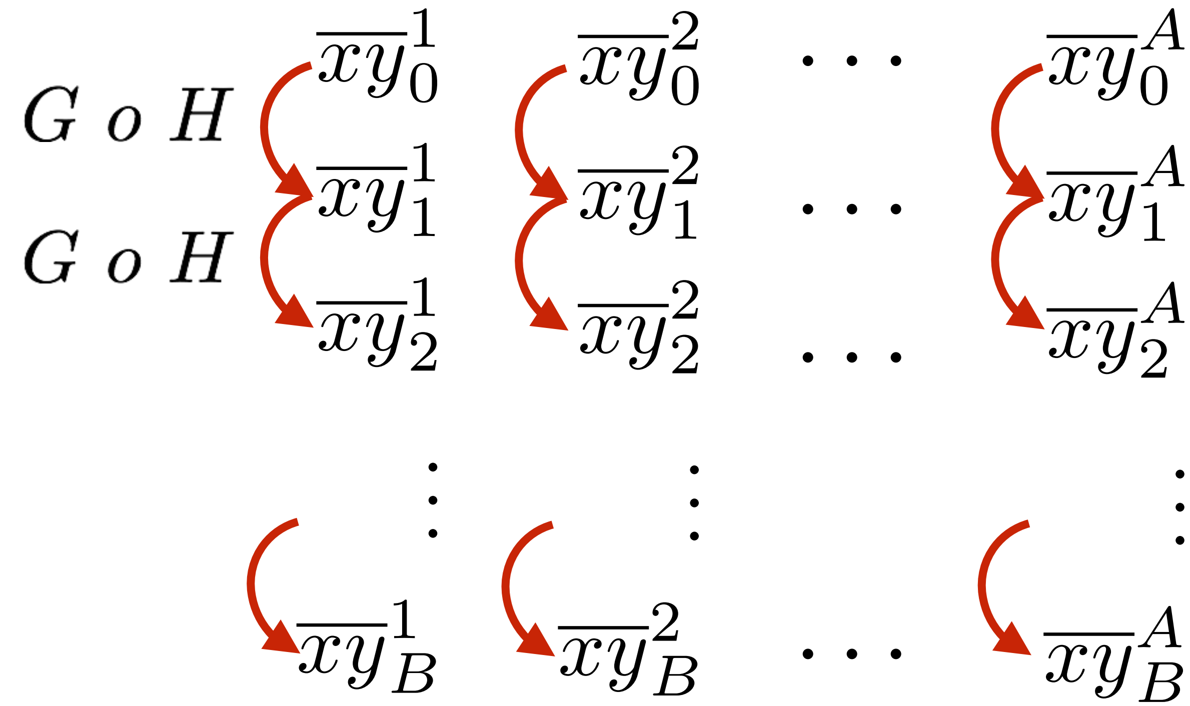


Chosen Plaintext Attack on FF3

$$E_K^T = H \circ G$$

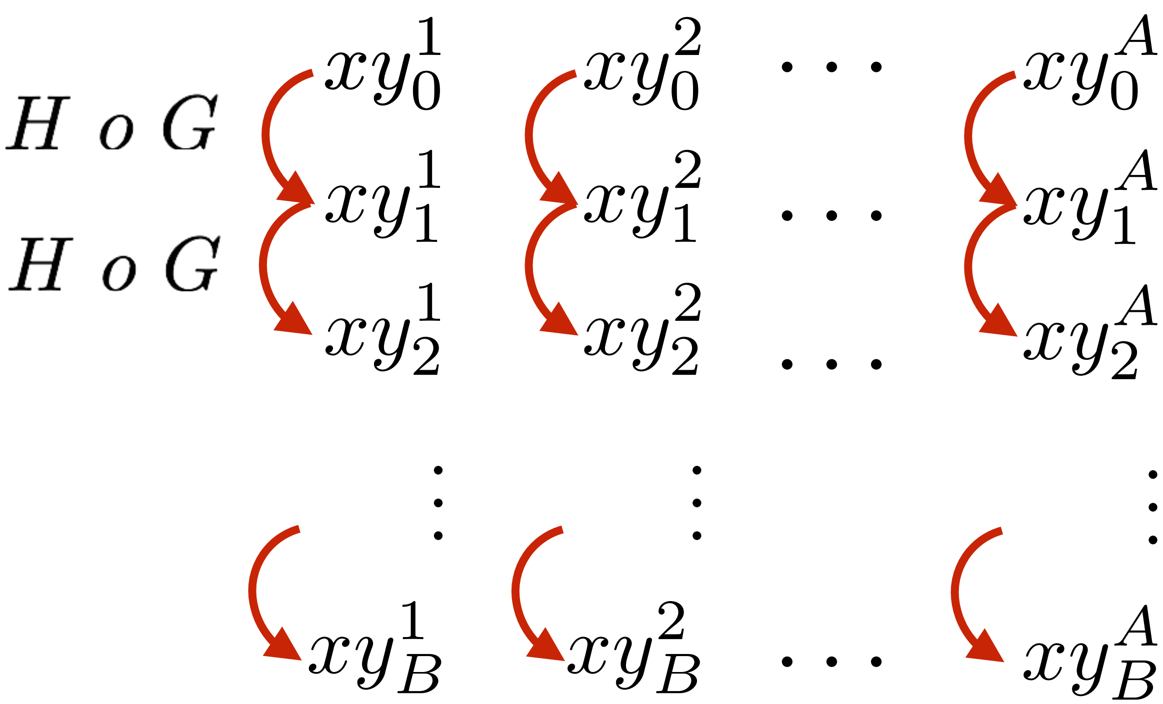


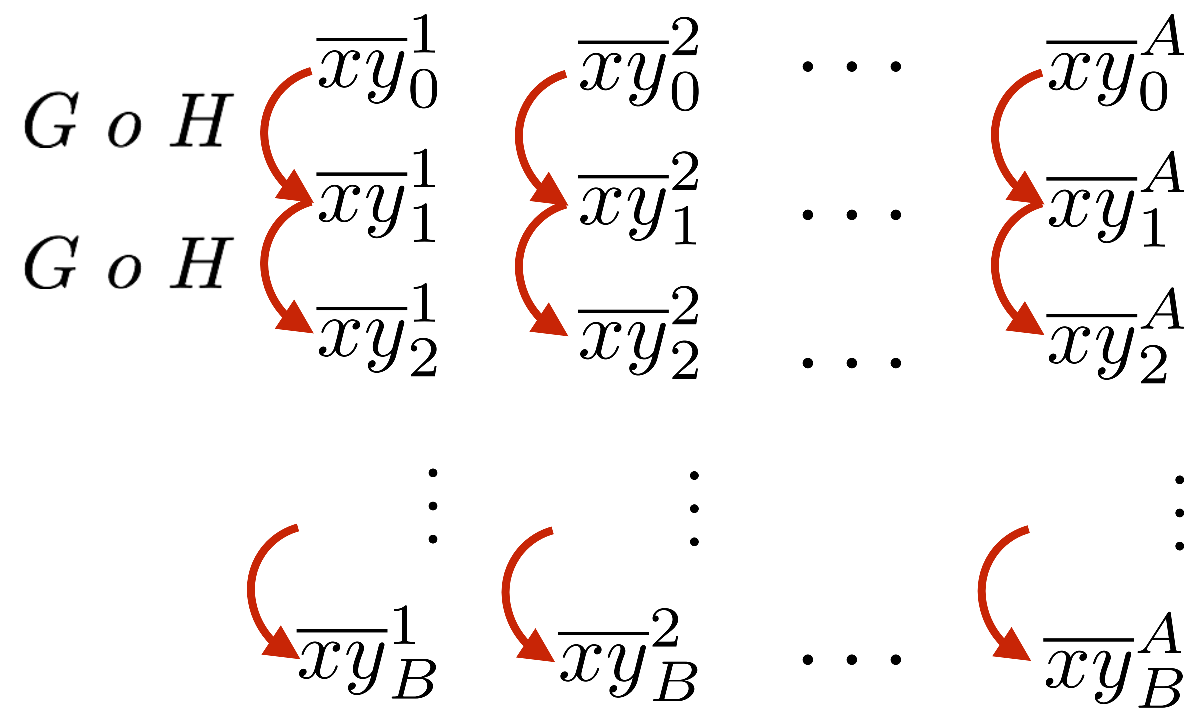
$$E_K^{T \oplus (4,4)} = G \circ H$$



Chosen Plaintext Attack on FF3

$$E_K^T = H \ o \ G \qquad\qquad E_K^{T \oplus (4,4)} = G \ o \ H$$





$$xy_j^i \qquad \overline{xy}_0^{i'}$$

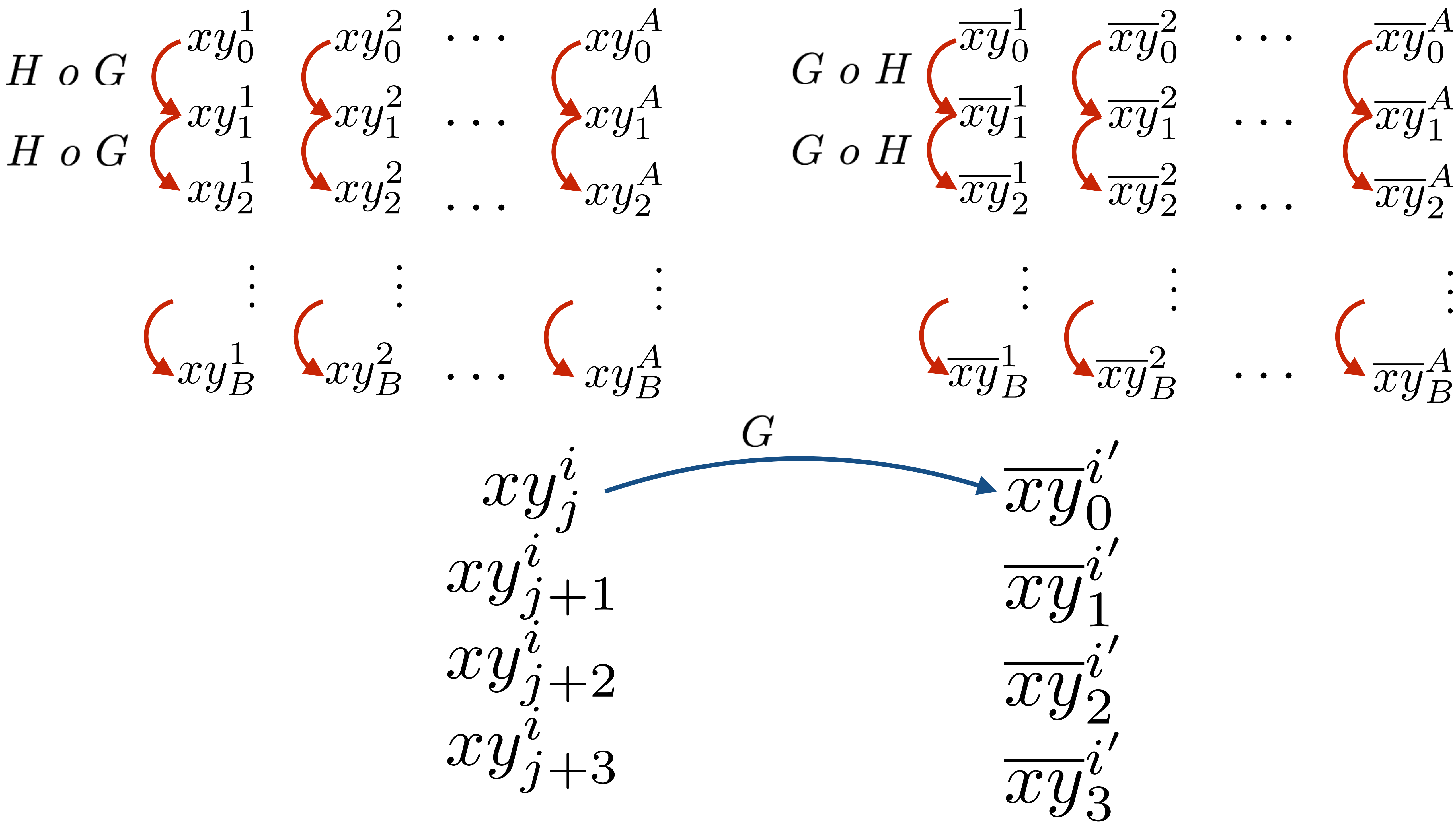
$$xy_{j+1}^i \qquad \overline{xy}_1^{i'}$$

$$xy_{j+2}^i \qquad \overline{xy}_2^{i'}$$

$$xy_{j+3}^i \qquad \overline{xy}_3^{i'}$$

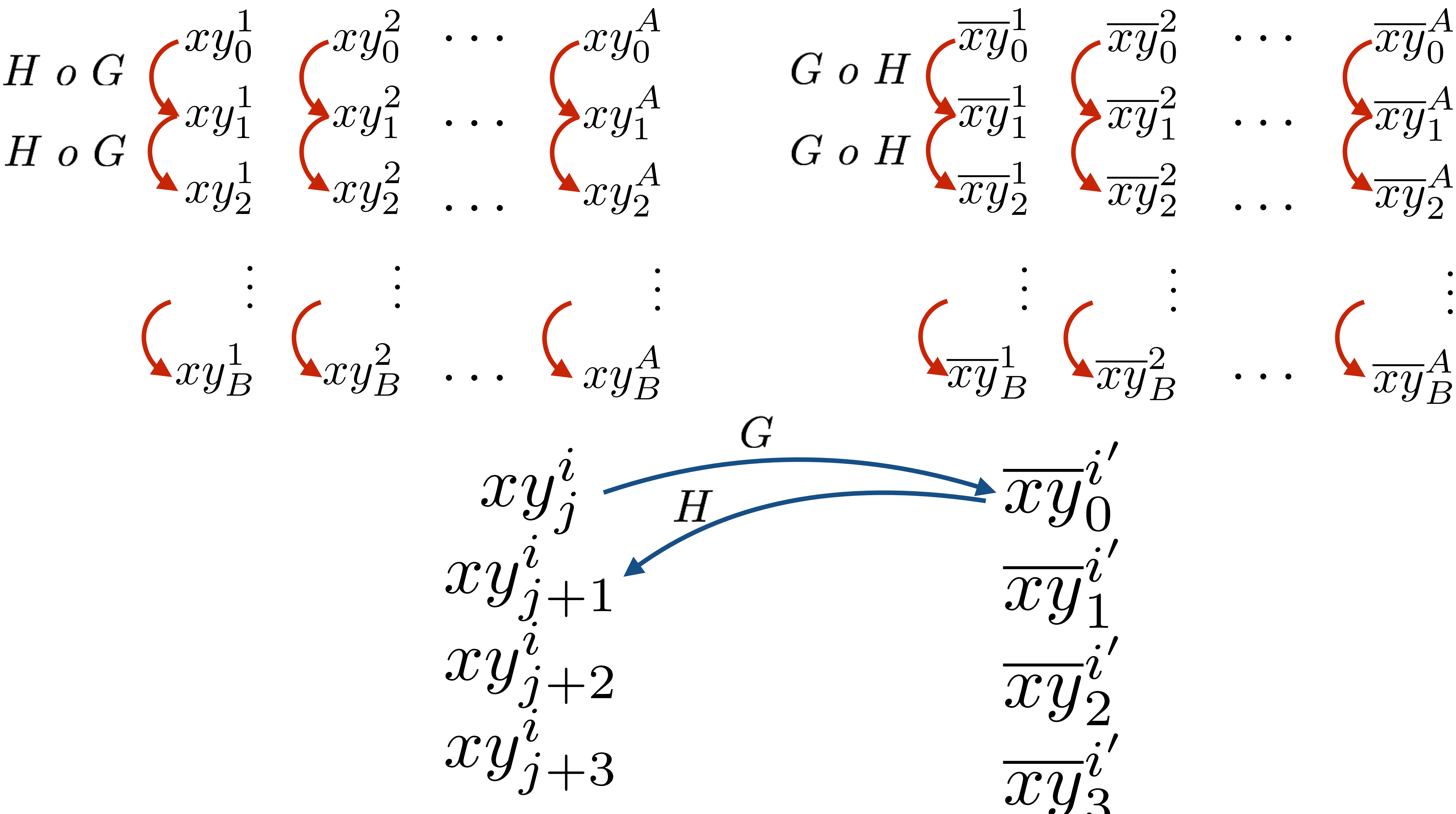
Chosen Plaintext Attack on FF3

$$E_K^T = H \ o \ G \qquad\qquad E_K^{T \oplus (4,4)} = G \ o \ H$$



Chosen Plaintext Attack on FF3

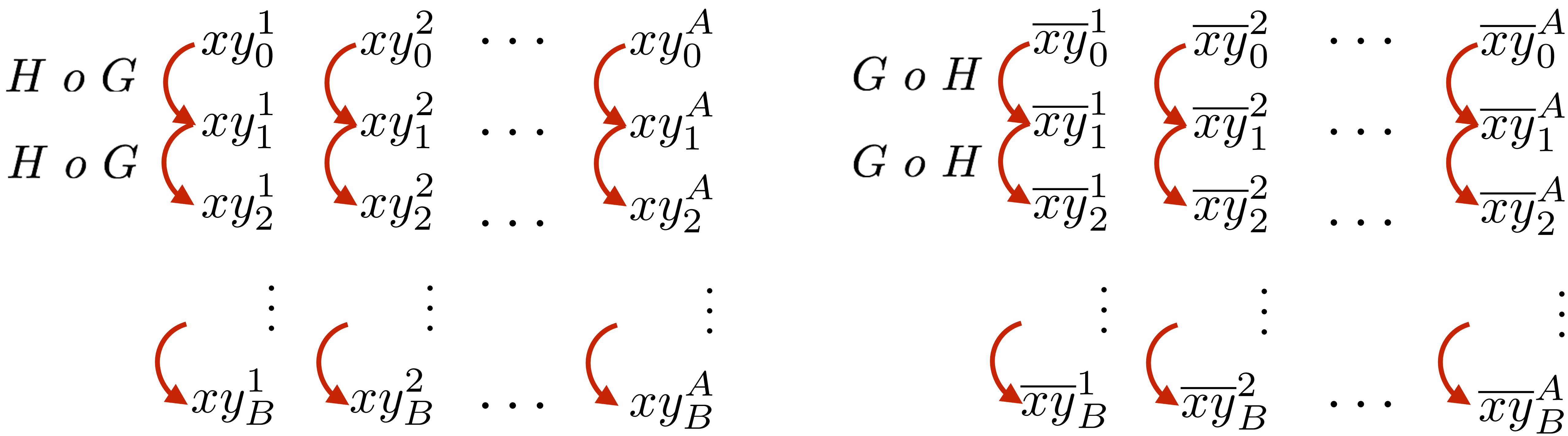
$$E_K^T = H \circ G \qquad\qquad E_K^{T \oplus (4,4)} = G \circ H$$

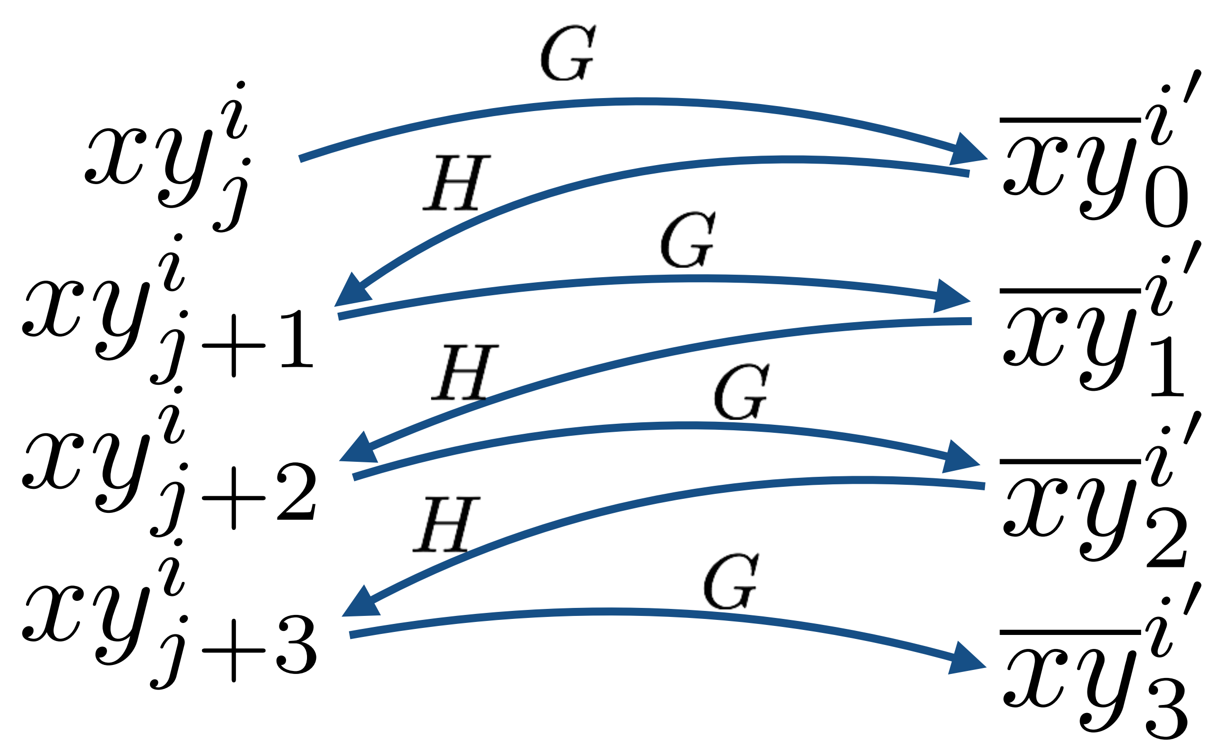


If $G(xy_j^i) = \overline{xy}_0^{i'}$, then $H(\overline{xy}_0^{i'}) = xy_{j+1}^i$.

Chosen Plaintext Attack on FF3

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

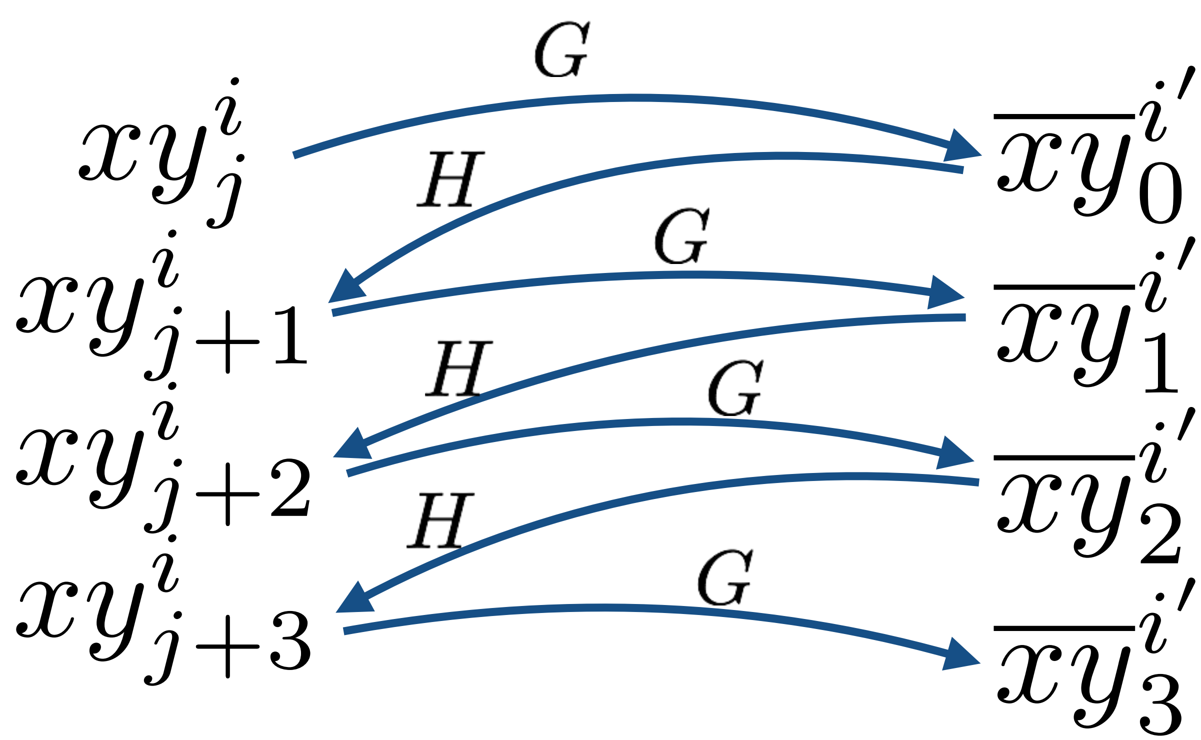




If $G(xy_j^i) = \overline{xy}_0^{i'}$, then $H(\overline{xy}_0^{i'}) = xy_{j+1}^i$.

Chosen Plaintext Attack on FF3

Pr (two segments of length B defined with xy_j^i and $\overline{xy}_0^{i'}$ overlap on at least M points) $\approx \frac{2(B-M)}{N^2}$.



If $G(xy_j^i) = \overline{xy}_0^{i'}$, then $H(\overline{xy}_0^{i'}) = xy_{j+1}^i$.

Experimental Results

Results with $L = 3$, $M \approx N^{\frac{3}{2}} (N)^{\frac{1}{2L}}$, $B = 2M$, and $A = \dfrac{N}{\sqrt{2M}}$

N	M	A	B	#trials	Pr[succ]
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%

N: the domain size to a round function.
M: the query complexity of 4-round attack with a parameter **L**.
A: the number of arbitrary plaintext to apply chain encryption.
B: the length of the chain encryption.

Conclusions

- Feistel Networks over small domains are not well understood yet.
  - We need more research for generic attacks on Feistel networks.

Conclusions

- Feistel Networks over small domains are not well understood yet.
  - We need more research for generic attacks on Feistel networks.
- FF3 suffers from very bad domain separation.
  - Fix to prevent from this attack: concatenate the tweak and round index.

Thank You!

Security of Feistel Networks

r : round numbers
q : number of queried plaintext
N^2 : domain size of Feistel network

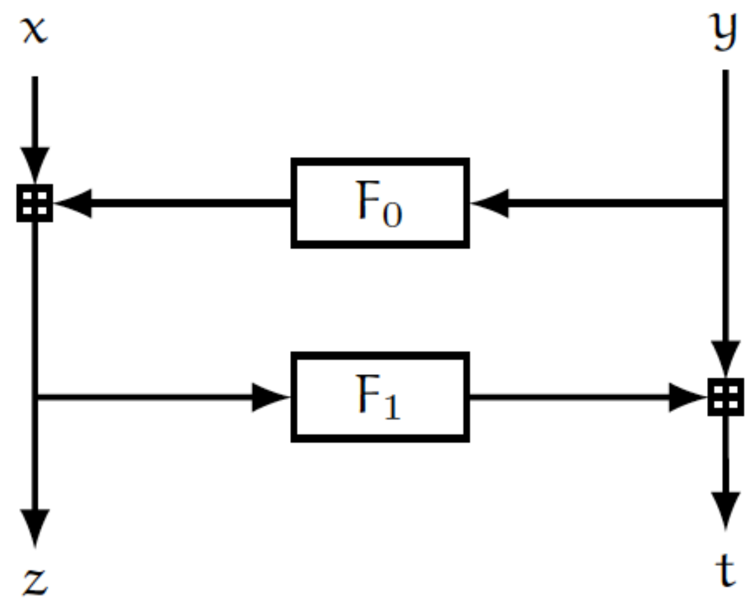
Security Proofs: [Patarin'10] proved that

- No distinguisher exists with $q \ll N$ known plaintext when $r \geq 4$.
- No distinguisher exists with $q \ll N$ chosen plaintext when $r \geq 5$.
- No distinguisher exists with $q \ll N$ chosen plaintext/ciphertext $r \geq 6$.
- If no distinguisher is possible, no other attack is possible either.

Information theory: The adversary needs $q = \frac{r}{2}N$ known plaintext to recover all the round functions.

Trivial attack: When the adversary knows the encryption of $q = N^2$ plaintext, it obtains the entire codebook for any r.

Warm Up: 2-round Feistel Networks



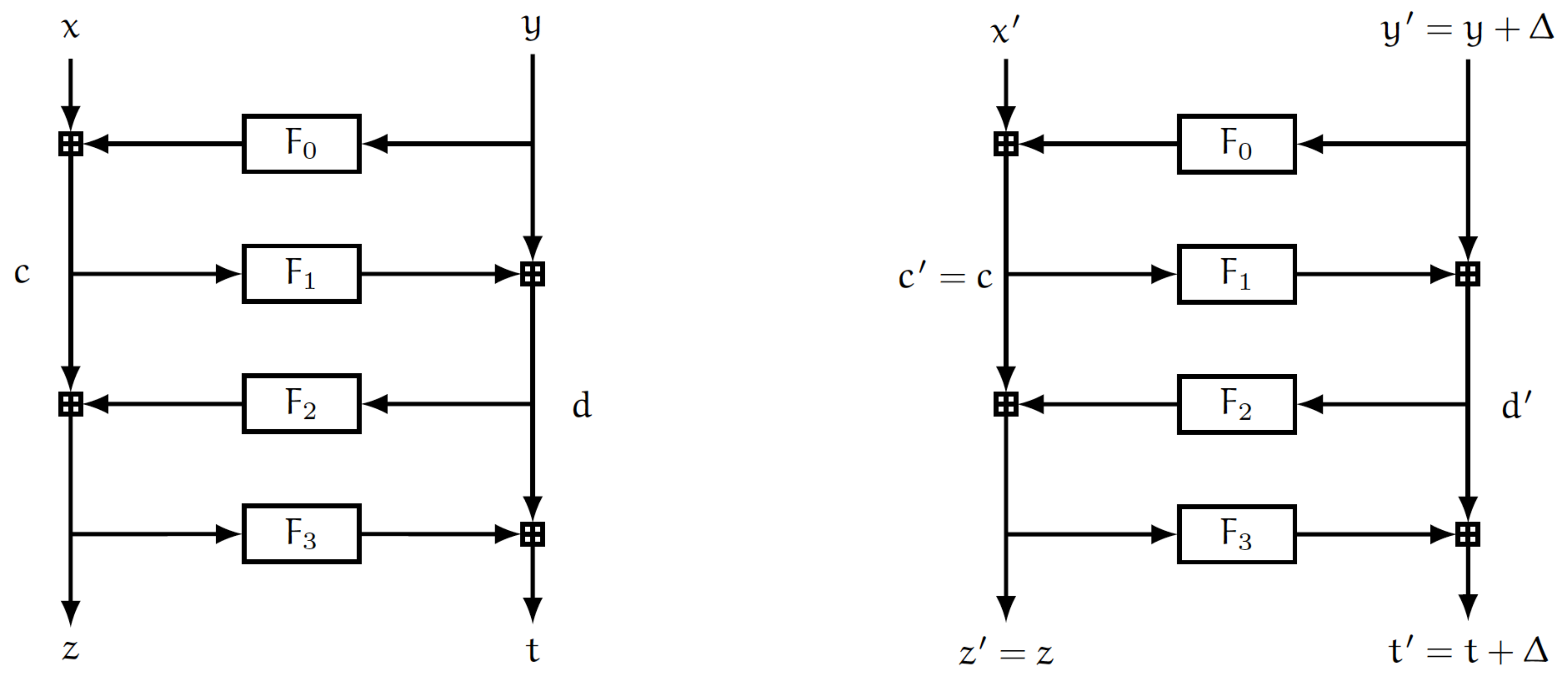
F_0, F_1 are round functions.

$x||y \in \mathbb{Z}_N \times \mathbb{Z}_N$, so is $z||t$.

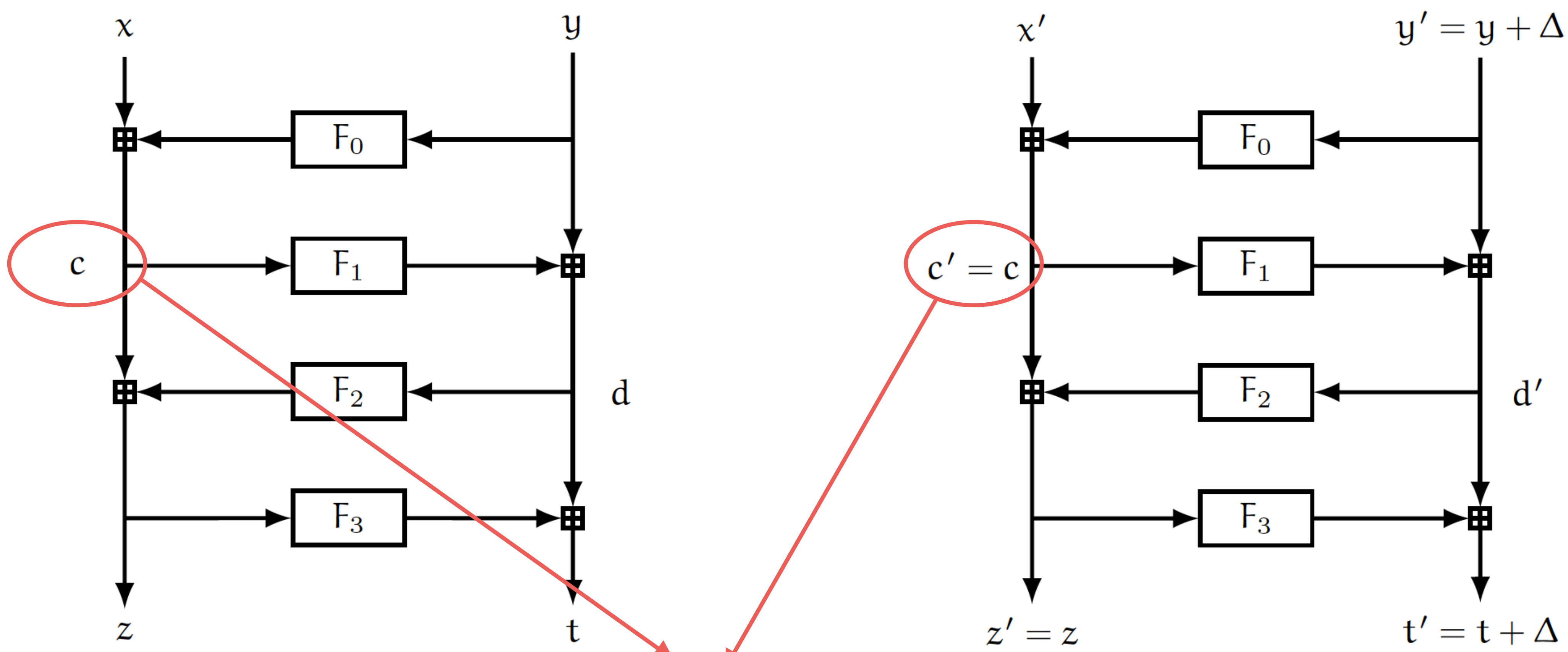
$z = x + \mathbf{F_0}(y)$
$t = y + \mathbf{F_1}(z)$

- N^2 known-plaintext attack is trivial.
- Can we figure out a round-function-recovery with less than N^2 known-plaintext?
- Each known plaintext/ciphertext gives a point in round functions.
  - Since we know x and z, it is easy to derive $F_0(y)=z-x$.
  - We simply compute $F_1(z)=t-y$.
- N (when $N \ll N^2$) known plaintext recovers the all the round functions with good probability.

The Principle of 4-round Attack on Feistel Networks

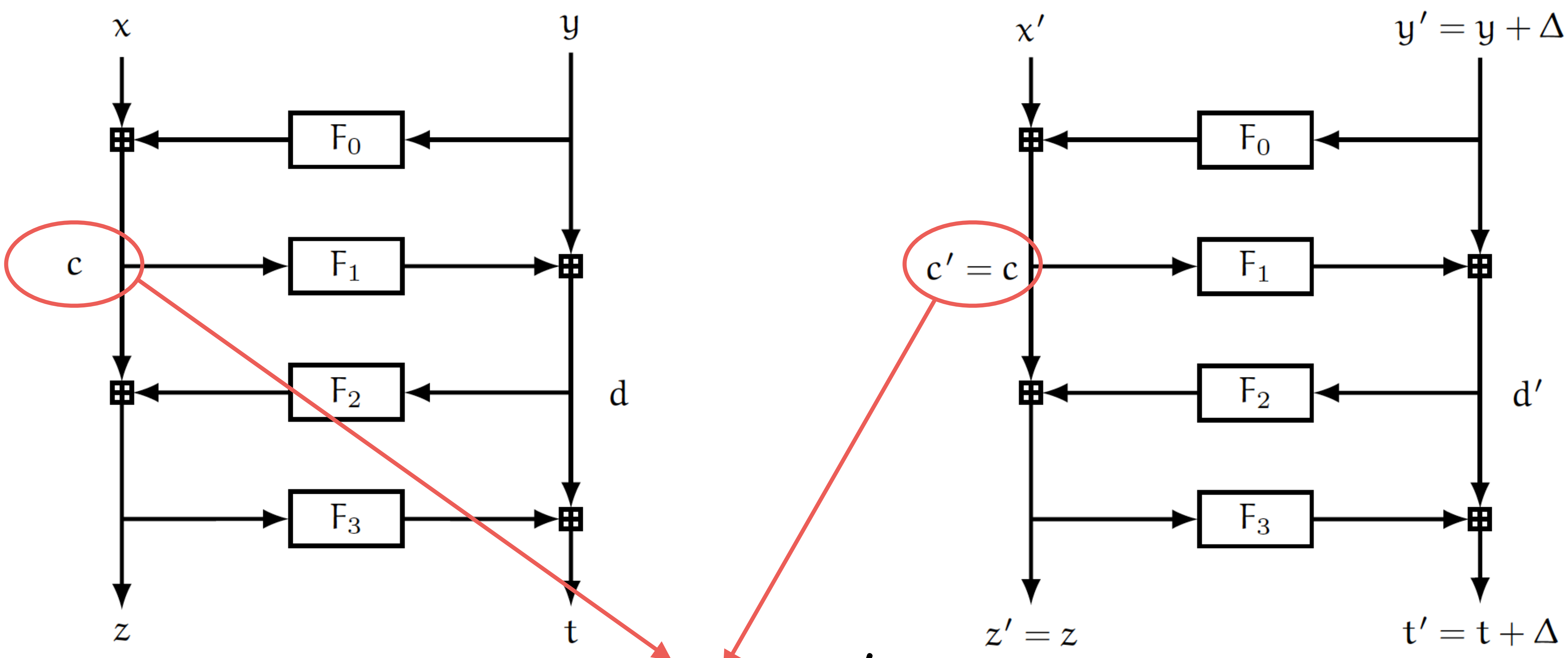


The Principle of 4-round Attack on Feistel Networks



Find collision on $c = c'$ to characterize F_0.

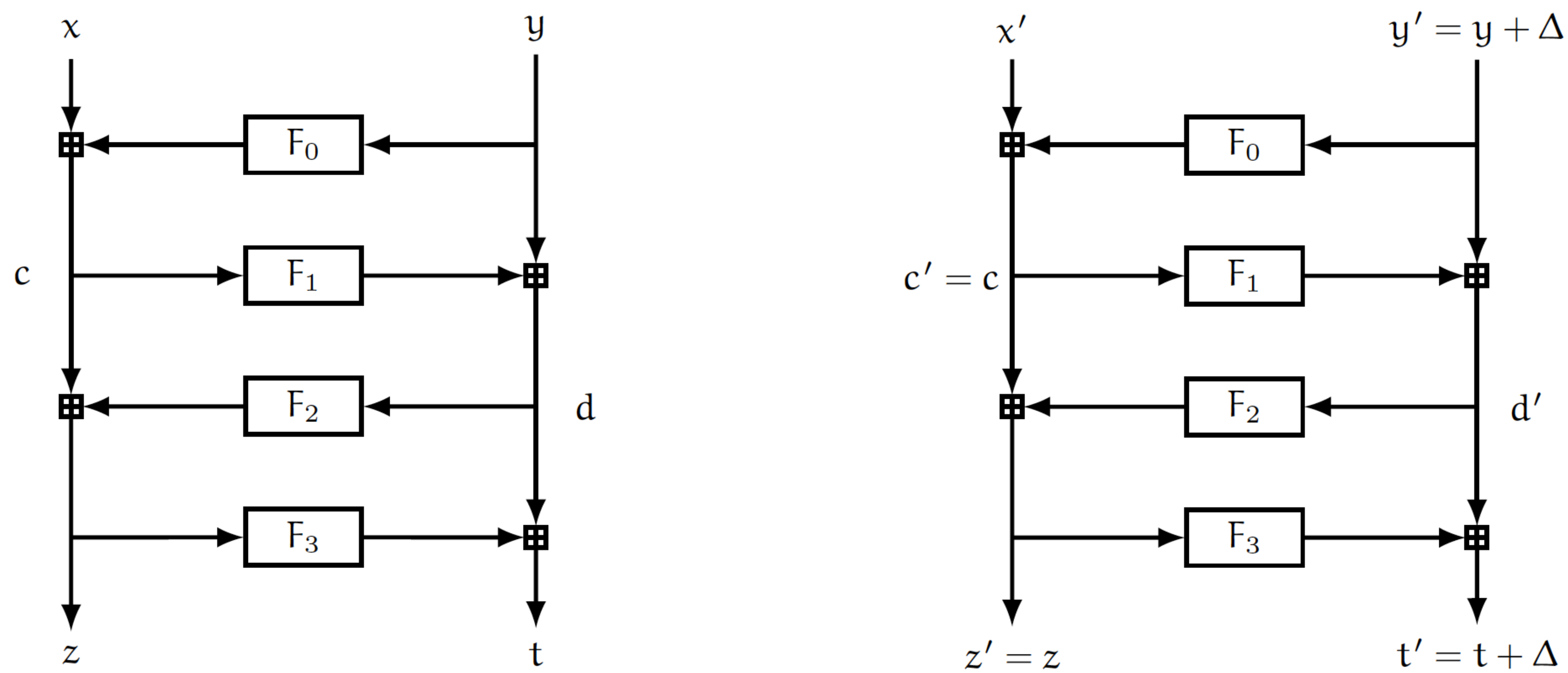
The Principle of 4-round Attack on Feistel Networks



Find collision on $c = c'$ to characterize F_0.

Property: If $c = c'$, then $x - x'$=$F_0(y')$ - $F_0(y)$

The Principle of 4-round Attack on Feistel Networks

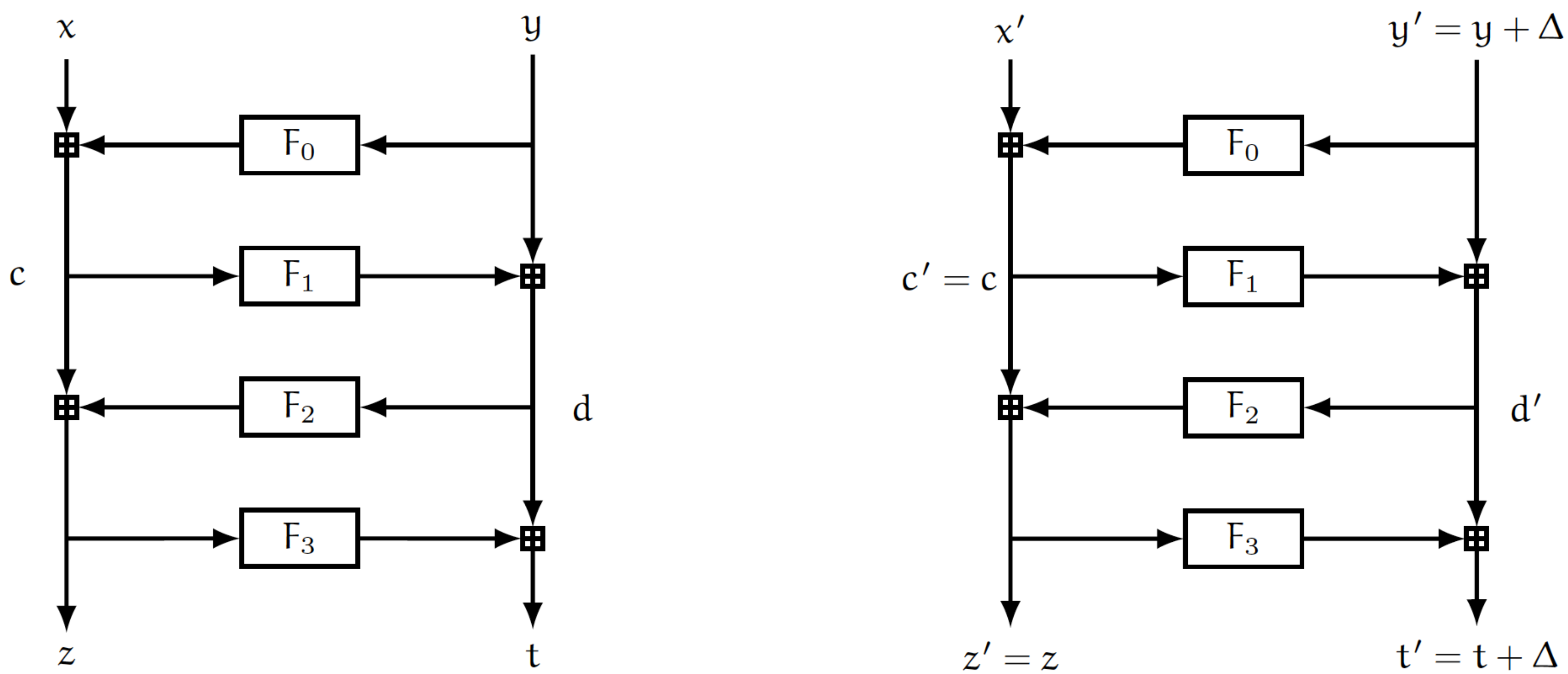


Problem: Adversary cannot check if $c = c'$.

Property: If $c = c'$, then $x - x'$=$F_0(y')$ - $F_0(y)$

The Principle of 4-round Attack on Feistel Networks

$$V = \{(xyzt, x'y'z't') | z' = z, t' - y' = t - y, xy \neq x'y'\}$$



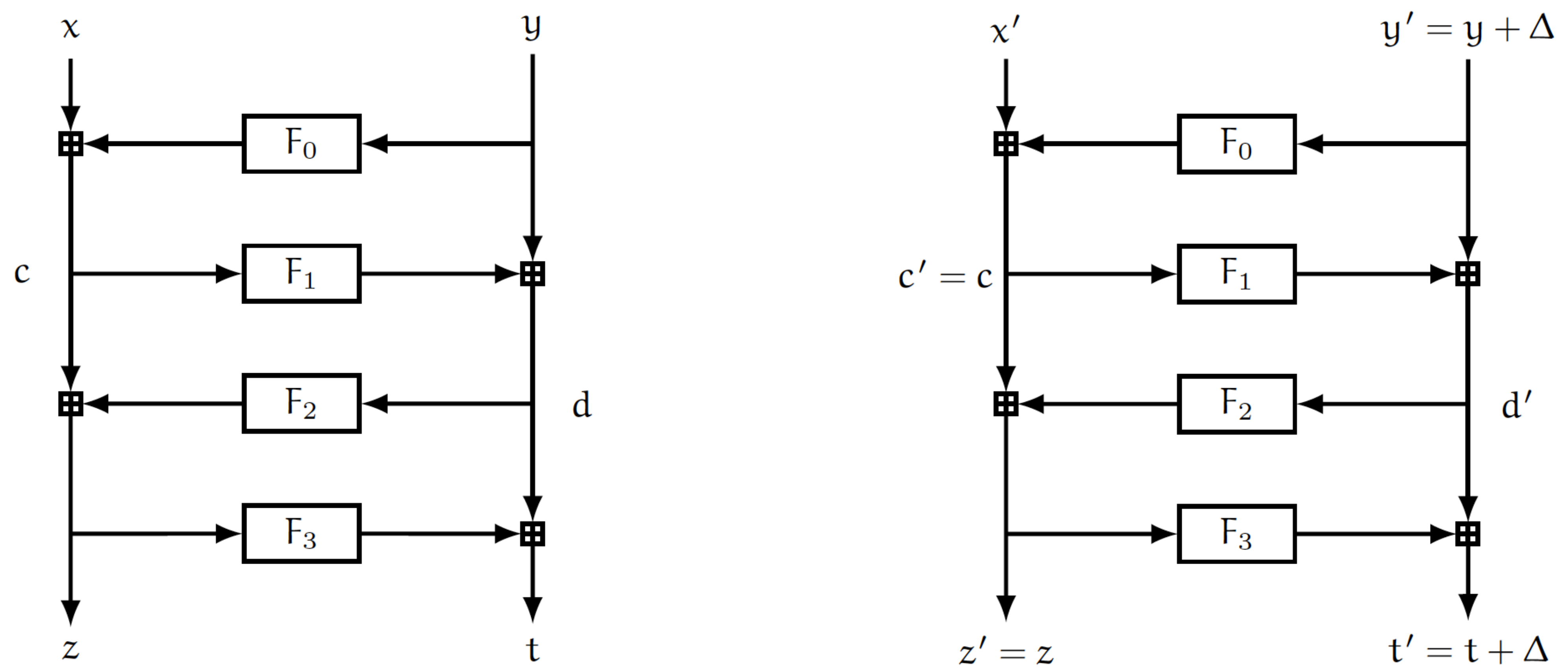
Problem: Adversary cannot check if $c = c'$.

Property: If $c = c'$, then $x - x'$=$F_0(y')$ - $F_0(y)$

The Principle of 4-round Attack on Feistel Networks

$$V = \{(xyzt, x'y'z't') | z' = z, t' - y' = t - y, xy \neq x'y'\}$$

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



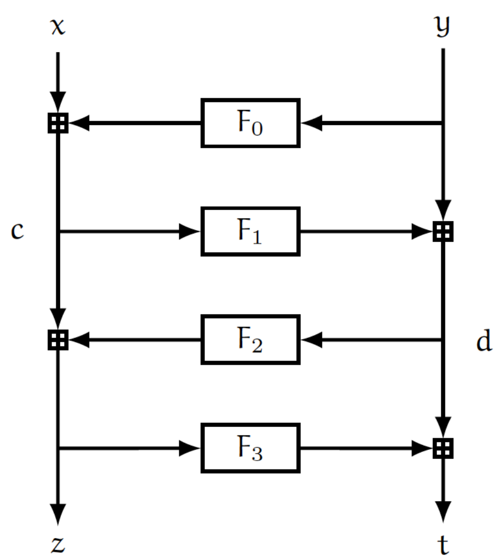
Problem: Adversary cannot check if $c = c'$.

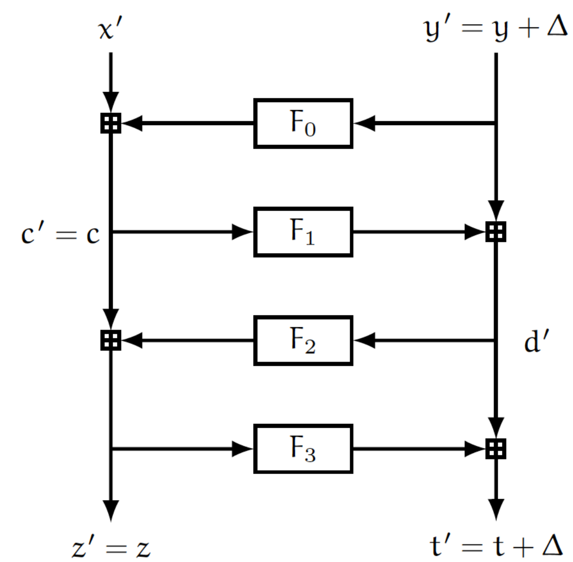
Property: If $c = c'$, then $x - x'$=$F_0(y')$ - $F_0(y)$

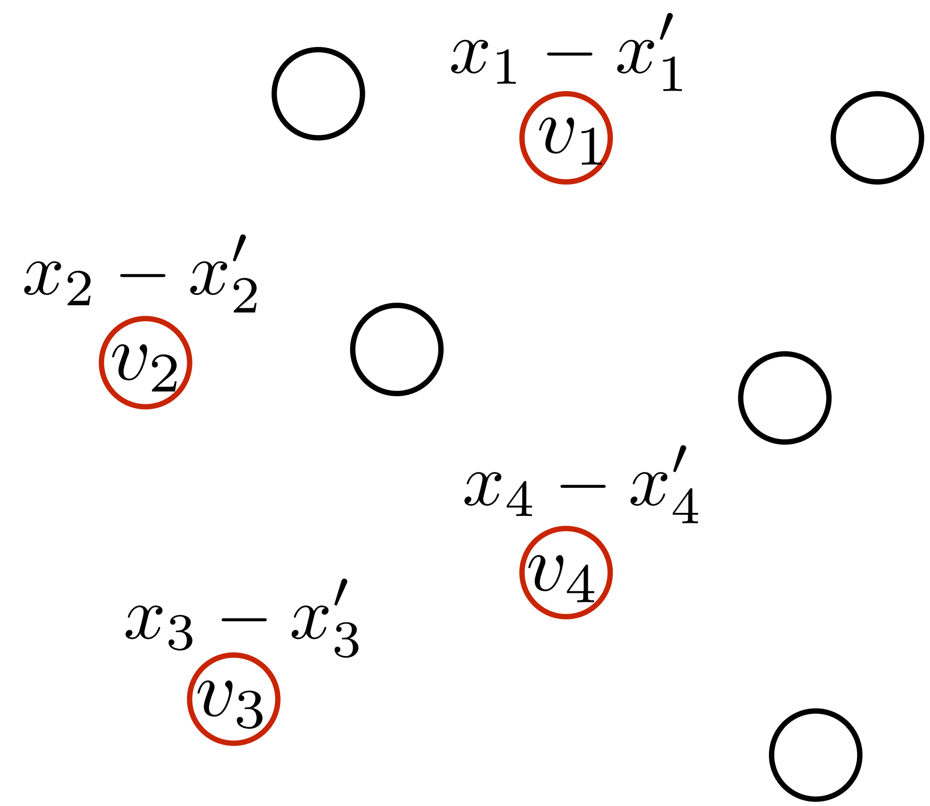
The Principle of 4-round Attack on Feistel Networks

$$V = \{(xyzt, x'y'z't') | z' = z, t' - y' = t - y, xy \neq x'y'\}$$

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







Problem: Adversary cannot check if $c = c'$.

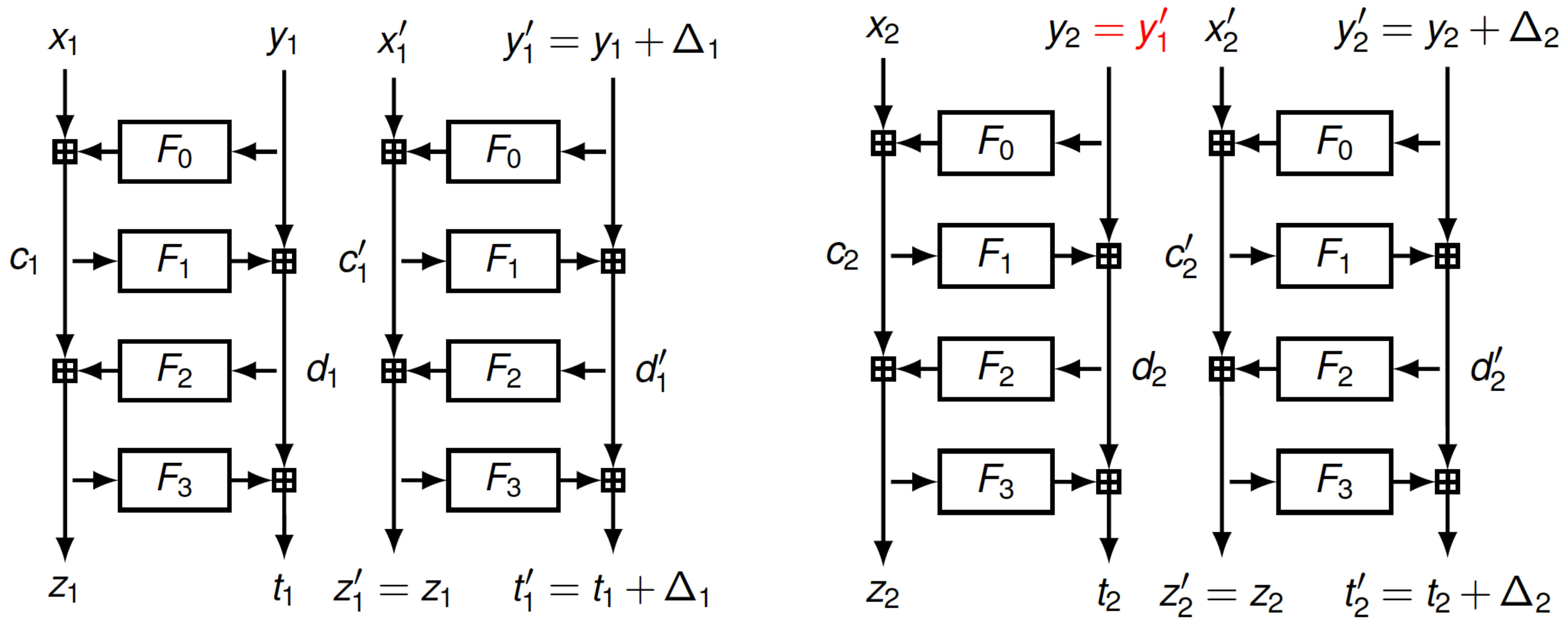
Property: If $c = c'$, then $x - x'$=F0(y') - F0(y)

Define label$(xyzt, x'y'z't') = x - x'$

How to Identify Good Vertices?

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

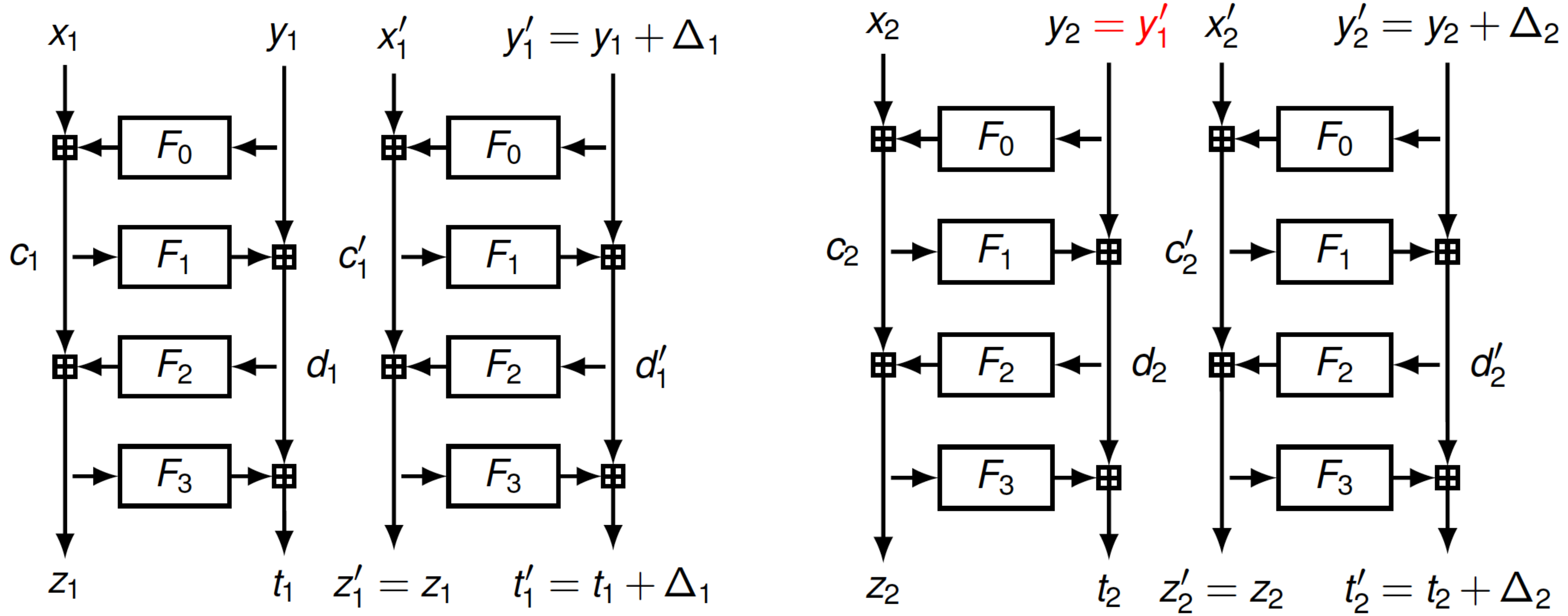
$$E = \{x_1 y_1 z_1 t_1 x'_1 y'_1 z'_1 t'_1, x_2 y_2 z_2 t_2 x'_2 y'_2 z'_2 t'_2 | y'_1 = y_2\}$$



How to Identify Good Vertices?

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

$$E = \{x_1 y_1 z_1 t_1 x'_1 y'_1 z'_1 t'_1, x_2 y_2 z_2 t_2 x'_2 y'_2 z'_2 t'_2 | y'_1 = y_2\}$$



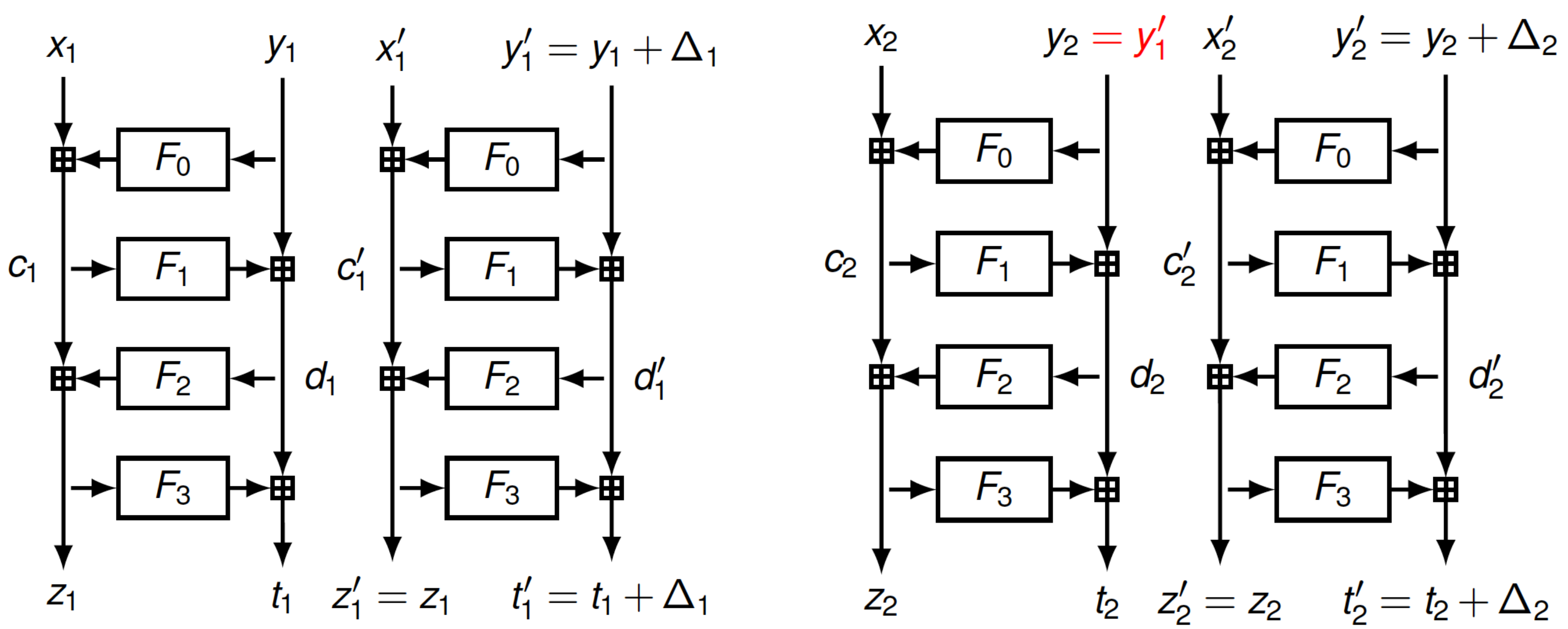
Property: If $v_1 v_2 \ldots v_L$ is a cycle with all v_i in V_{good}, then

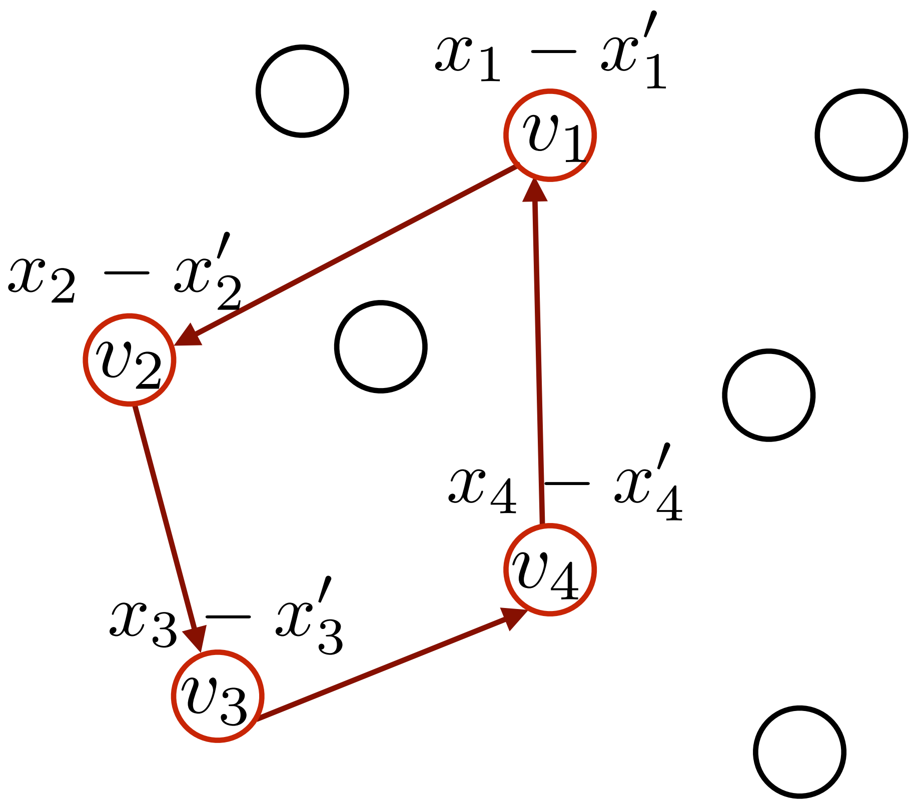
$$\sum_{i=1}^{L} label(v_i) = 0$$

How to Identify Good Vertices?

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

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





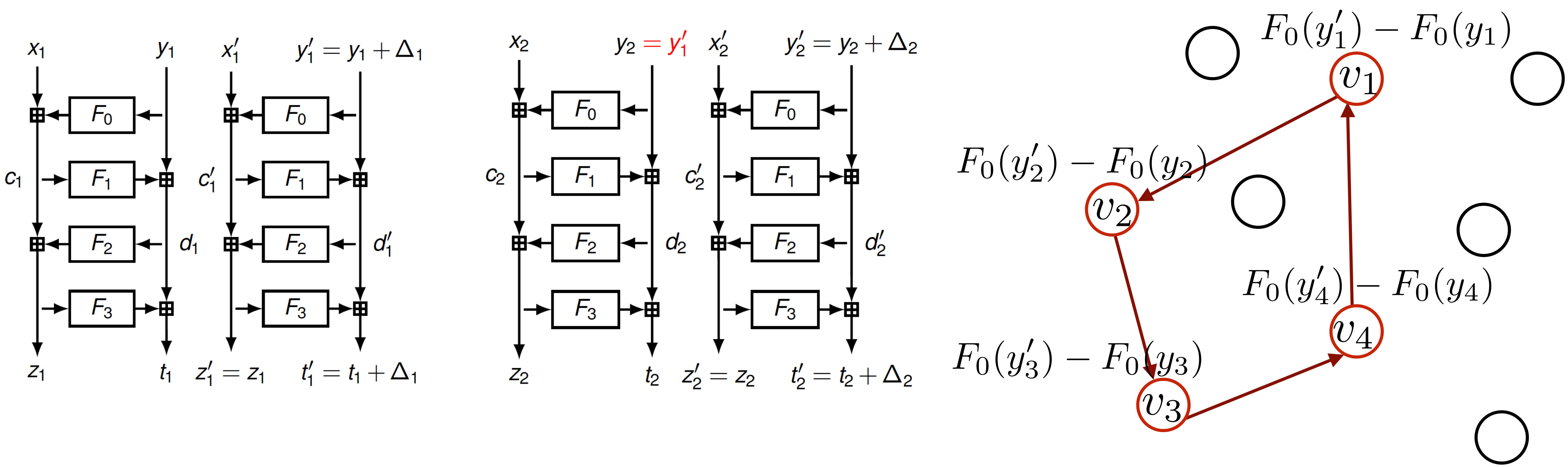
Property: If $v_1 v_2 \ldots v_L$ is a cycle with all v_i in V_{good}, then

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

How to Identify Good Vertices?

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

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

How to Identify Good Vertices?

Lemma 1: For random $v = xyztx'y'z't'$ and F_0, F_1, F_2, F_3,

$$\Pr[v \in V_{good} | v \in V] = \frac{1 - \frac{1}{N}}{2 - \frac{1}{N}} \approx \frac{1}{2}$$

Lemma 2:

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

trivial cycle: v_1 and v_2 are permutation of each other

Conjecture:

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

acceptable cycle: with 2L non-repeating plaintexts.

Chosen Plaintext Attack on FF3

- Let C^i be the cycle spanned by xy_0^i, with T.
- Let $\overline{C}^{i'}$ be the cycle spanned by $\overline{xy}_0^{i'}$ with $T \oplus (4,4)$.

- Pr (xy_0^i and $\overline{xy}_0^{i'}$ in the same cycle (of any length)) $\approx \frac{1}{2}$.

- E (length(C^i) | xy_0^i and $\overline{xy}_0^{i'}$ in the same cycle) $\approx \frac{2N^2}{3}$.

- Pr (two segments of length B defined with xy_0^i and $\overline{xy}_0^{i'}$ overlap on at least M points) $\approx \frac{2(B-M)}{N^2}$.

- Pr (no such i and i' exist) $\approx e^{\frac{-2MA^2}{N^2}}$ when $B = 2M$.

- We derive $B = 2M$ and $A = \frac{N}{\sqrt{2M}}$.

Chosen Plaintext Attack on FF3

input: T

Chosen Plaintext Attack on FF3

input: T

$$T' = T \oplus (4, 4)$$

Chosen Plaintext Attack on FF3

input: T

$T' = T \oplus (4,4)$

for $i = 1\ to\ A$ do

pick xy_0^i and set $xy_j^i = FF3.E_K^T(xy_{j-1}^i)$ for $j = 1, \ldots, B$

pick $\overline{xy}_0^i$ and set $\overline{xy}_j^i = FF3.E_K^{T'}(\overline{xy}_{j-1}^i)$ for $j = 1, \ldots, B$

end for

Chosen Plaintext Attack on FF3

input: T

$T' = T \oplus (4,4)$

for $i = 1\ to\ A$ do

pick xy_0^i and set $xy_j^i = FF3.E_K^T(xy_{j-1}^i)$ for $j = 1, \ldots, B$

pick $\overline{xy}_0^i$ and set $\overline{xy}_j^i = FF3.E_K^{T'}(\overline{xy}_{j-1}^i)$ for $j = 1, \ldots, B$

end for

for $i, i' = 1, \ldots A$ do

for $j = 0\ to\ B - M - 1$ do

assume $G(xy_j^i) = \overline{xy}_0^{i'}$

run 4-round attack on G with $G(xy_{j+k}^i) = \overline{xy}_k^{i'}$ for k=0,…,B-j

if successful, do the same with H and conclude.

end for

for $j = 0\ to\ B - M - 1$ do

assume $G(xy_0^i) = \overline{xy}_{j'}^{i'}$

…same…

end for

end for