The Curse of Small Domains

New Attacks on Format-Preserving Encryption

Viet Tung Hoang
Florida State University

Stefano Tessaro
UC Santa Barbara

Ni Trieu
Oregon State University

CRYPTO 2018
August 20, 2018

Format-Preserving Encryption (FPE)

[FIPS 74, BS97 BR02,BRPS09,...]

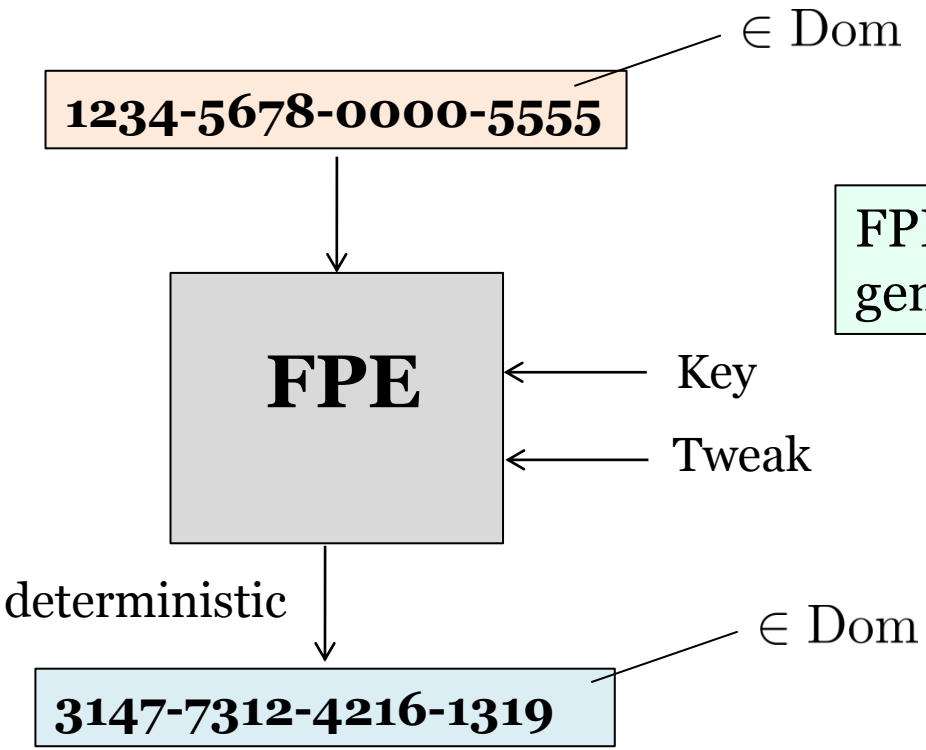
Widely used to encrypt credit-card numbers and fields in legacy databases

-**Property**: Ciphertext has the same "format" as the plaintext → Avoid disrupting the system

Ciphertexts also look like credit-card numbers

Format-Preserving Encryption (FPE)

[FIPS 74, BS97 BR02,BRPS09,...]



FPE = tweakable blockcipher with a general message space Dom

Dom = set of credit-card numbers , set of PINs, set of SSNs, ...

The Need for Tweaks

Scenario: DB enforces columns to store valid CC numbers.

Customer	CC #
John Doe	1234-0001-4321-5678
Jane Doe	9876-0004-3133-7311
…	…
Alice Crypto	9876-0001-1234-1234

FPE-encrypt with key K and tweak "customer"

Customer	CC #
John Doe	4931-3137-3827-5934
Jane Doe	3819-5724-9477-3816
…	…
Alice Crypto	4820-4728-8439-1872

Trans. #	CC #
1	1234-0001-4321-5678
2	1234-0001-4321-5678
3	9876-0001-1234-1234
…	…

FPE-encrypt with key K and tweak "transaction"

Trans. #	CC #
1	8431-5938-5229-6788
2	8431-5938-5229-6788
3	3015-0101-5343-3134
…	…

Technical Challenge: FPE Domain Can Be Small

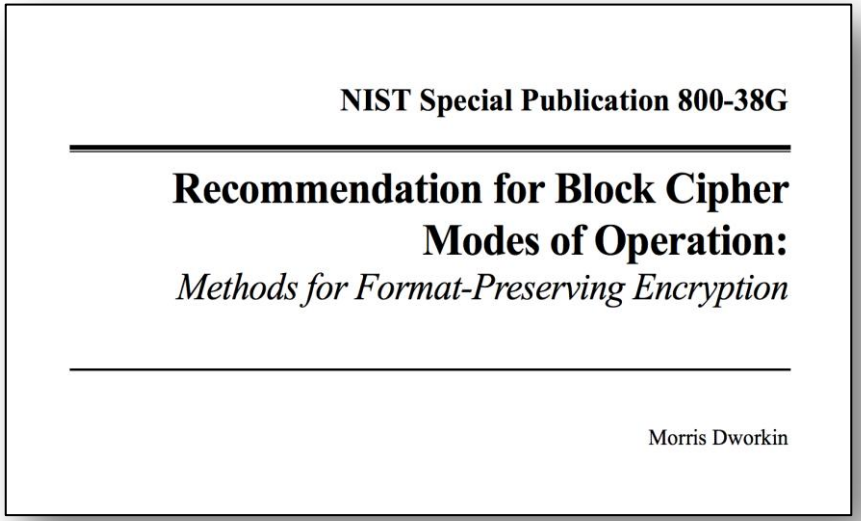
Credit-card numbers: $|\mathrm{Dom}| = 10^{16} \approx 2^{53}$

PINs: $|\mathrm{Dom}| = 10^4 \approx 2^{14}$

Even smaller domains: ANSI ASC X9.124 envisions an application for $|\mathrm{Dom}| = 100$

Real-world FPEs

suspended but likely to get reinstated



NIST Special Publication 800-38G

Recommendation for Block Cipher Modes of Operation:
Methods for Format-Preserving Encryption

Morris Dworkin

- Specified two schemes, FF1 and FF3, based on Feistel

Companies offering FPE

HPE Voltage, Veriphone, Ingenico, and others

Other FPE solutions from industry:

DTP from Protegrity:

-Claimed to be more secure than NIST's FPEs

-Largely follows ad-hoc solution of [BS97]

FNR from Cisco:

-Proposed but not used

-Use [NR99] variant of Feistel

Prior FPE Attacks

N: domain size

Paper	Recover	Time	#Msg per tweak	Adaptive	Known msg vs target	Break
[BHT16]	A single target	$\tilde{O}(N^{r/2-1})$	3	No	Same right half	FF1 FF3
[DV17]	Entire codebook	$O(N^{2.5})$	$\Theta(N^{11/12})$	Yes	N/A	FF3

Not applicable to generic Feistel

Easily fixed by restricting the tweak space

unbroken so far

Scheme	FF1	FF3	FNR
Round # r	10	8	9

Prior FPE Attacks

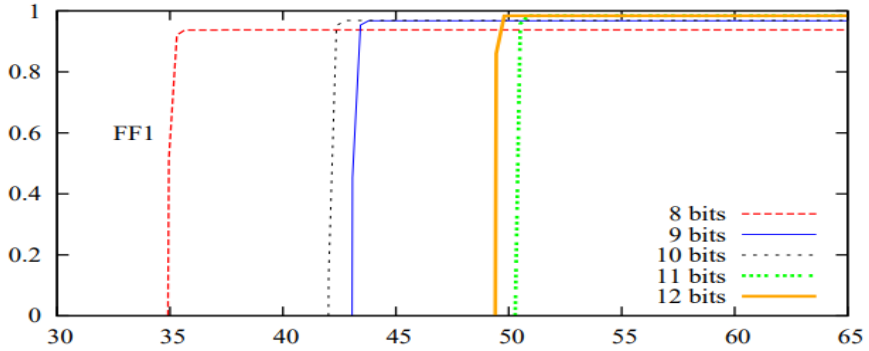
N: domain size

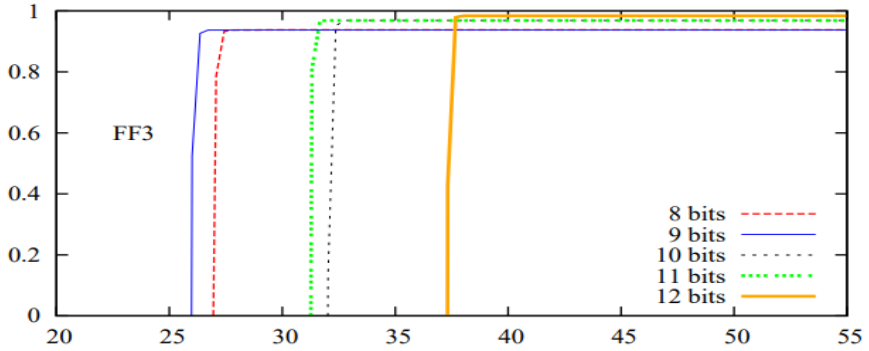
Paper	Recover	Time	#Msg per tweak	Adaptive	Known msg vs target	Break
[BHT16]	A single target	$\tilde{O}(N^{r/2-1})$	3	No	Same right half	FF1 FF3
[DV17]	Entire codebook	$O(N^{2.5})$	$\Theta(N^{11/12})$	Yes	N/A	FF3
Ours	Multiple targets	$\tilde{O}(N^{r/2-1})$	$\tilde{O}(\sqrt{N})$	No	None	FF1 FF3 FNR

Scheme	FF1	FF3	FNR
Round # r	10	8	9

Cost of Our Attack on FF1/FF3

Success rate

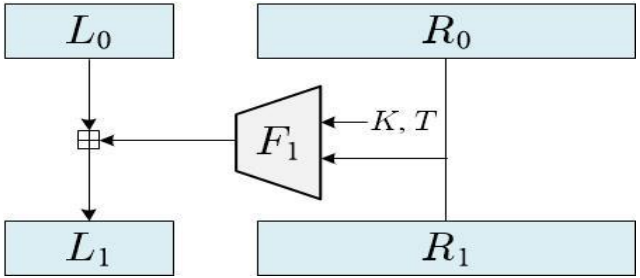




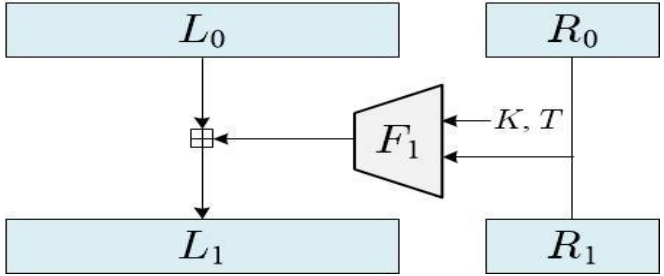
Log of ciphertext # per target

Expanding versus Contracting

FF1: start with contracting round functions



FF3: start with expanding round functions



FF3's design choice is inferior

Domain	Our cost (for FF1)	Our cost (for FF3)	[BHT16]'s cost (for FF1)	[BHT16]'s cost (for FF3)
$\{0,1\}^9$	2^{44}	2^{26}	2^{44}	2^{38}
$\{0,\ldots,9\}^3$	2^{56}	2^{21}	2^{56}	2^{49}

Our Results

Scheme	Attack type	Practical for
FF1/FF3/FNR	Known-plaintext attack	Small domains
DTP	Ciphertext-only attack	**Any** domain

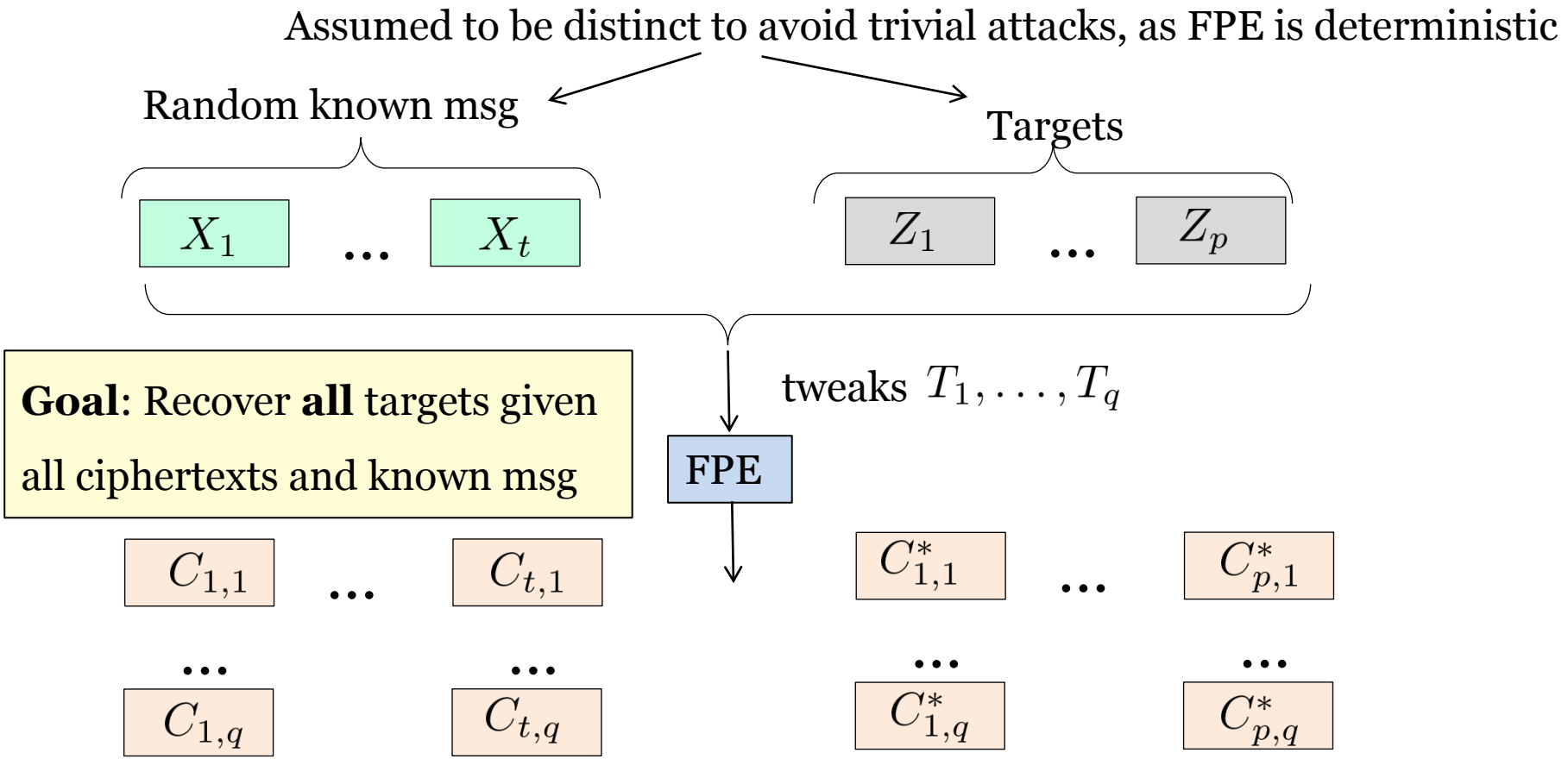
#ciphertexts needed to recover target with 90% success against DTP

Encoding	PIN	SSN	CCN
Decimal	460,000	525,000	575,000
Alphanumeric	46,000	51,000	53,000

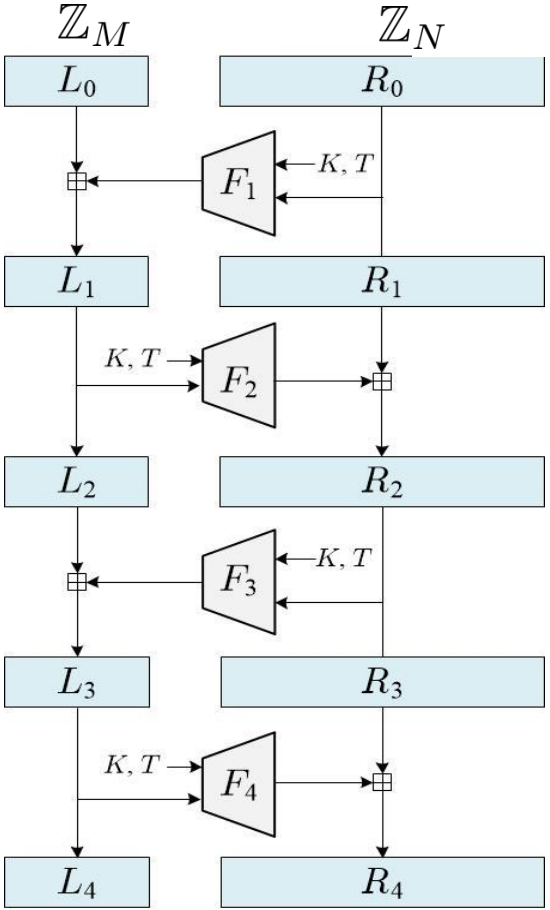
Protegrity uses alphanumeric encoding to enlarge domains

→ Make DTP actually **10 times weaker**

Attack Scenario: Known-Plaintext Attack



Feistel-based FPE



M and N can be very small

For FF1/FF3: $MN \geq 100$

We consider (abstract) domain $\mathbb{Z}_M \times \mathbb{Z}_N$

$(\mathbb{Z}_M, \boxplus)$ and $(\mathbb{Z}_N, \boxplus)$ are abelian groups

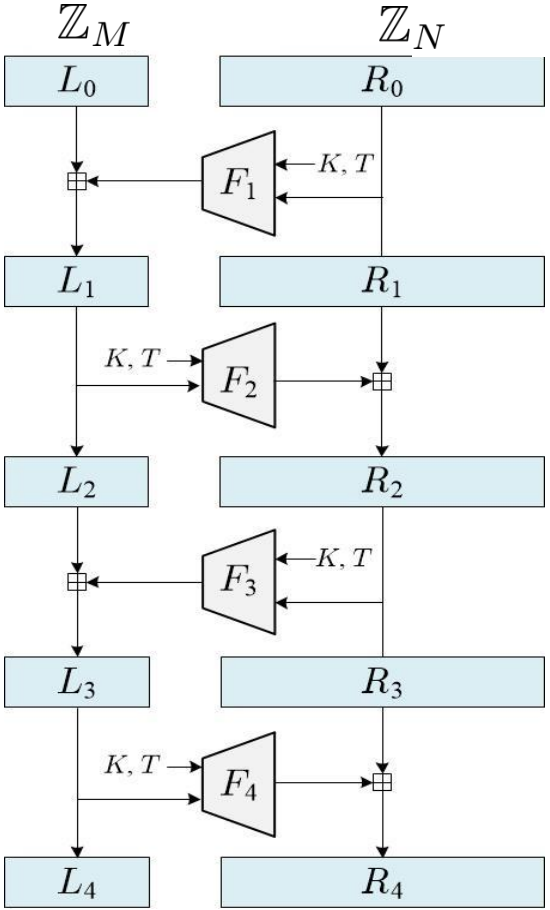
$\boxminus$ is inverse of $\boxplus$

Round functions are modeled as truly random

r-round Feistel ($r = 10$ for FF1, $r = 8$ for FF3)

Attack Idea: Bias

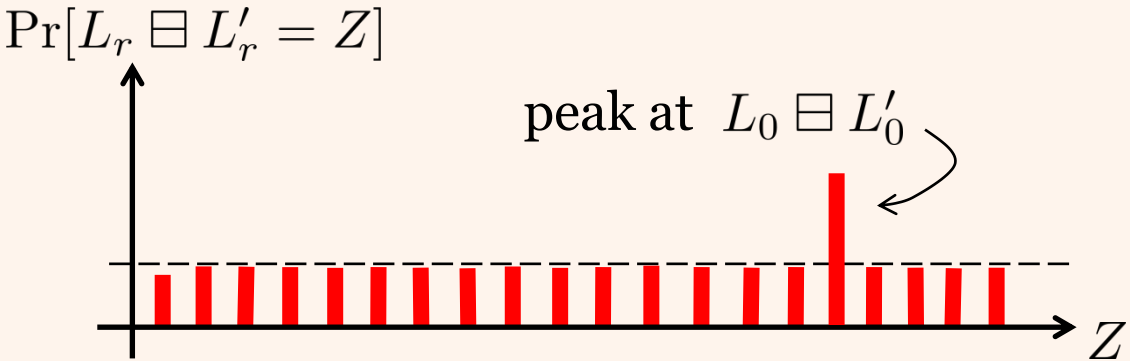
[Patarin 91, BHT16]



Question: Take two inputs (L_0, R_0) and (L'_0, R_0) such that $L_0 \neq L'_0$

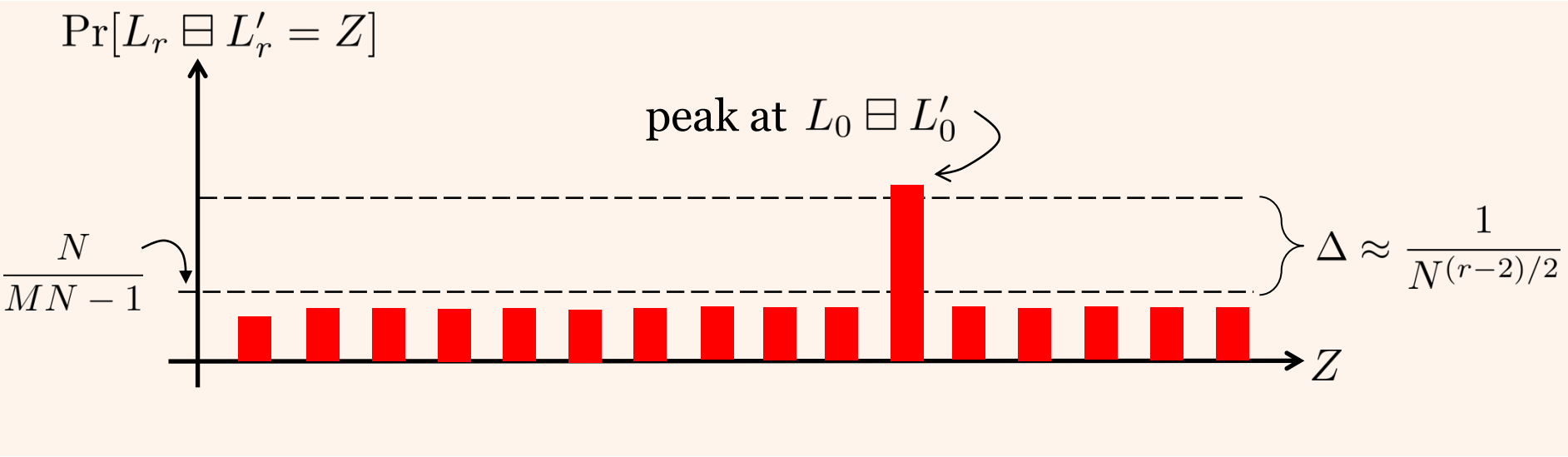
Same right half

What's the distribution of $L_r \boxminus L'_r$?



Using Bias

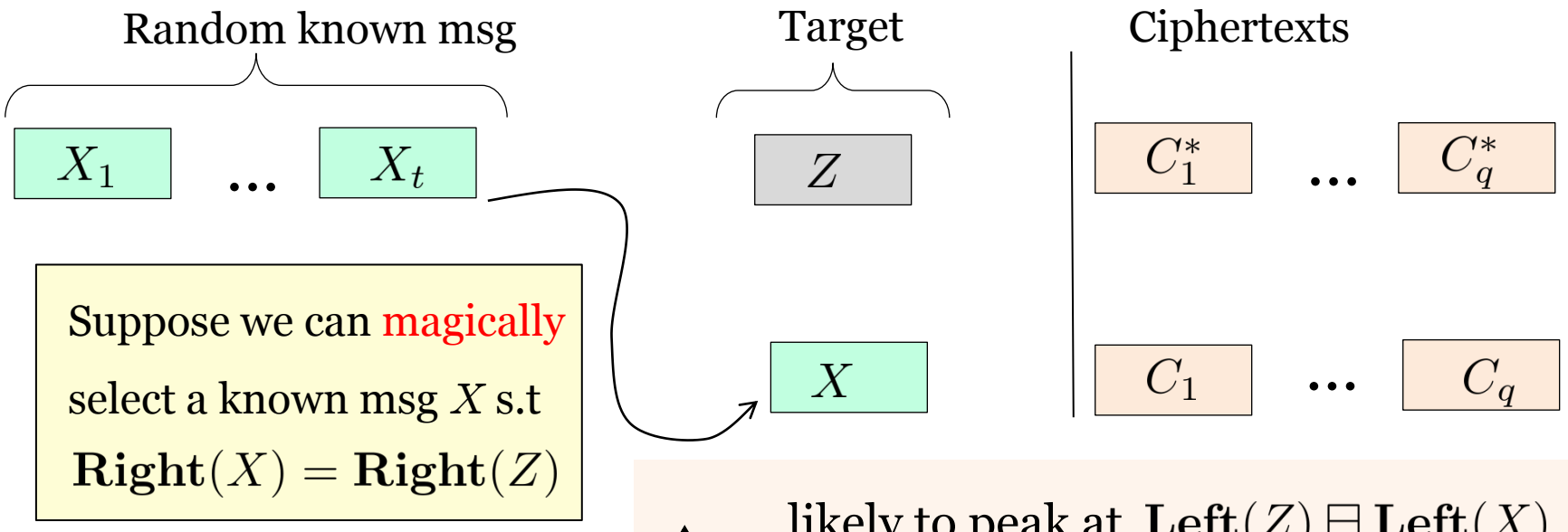
[BHT16]



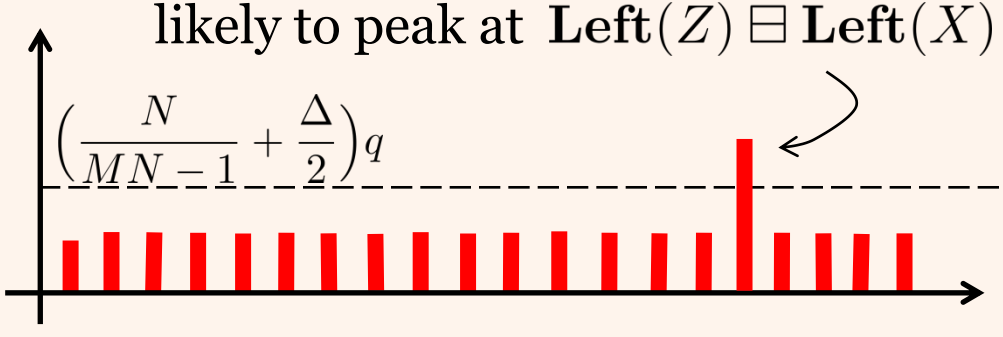
The bias is too small to exploit directly, but can be **amplified** if we have **enough** plaintext/ciphertext pairs!

A Wishful Dream

Basically [BHT16] attack



- Can trivially recover $\mathbf{Right}(Z)$
- Plot the frequency histogram of $\mathbf{Left}(C_i^*) \boxminus \mathbf{Left}(C_i)$



Narrowing Known Messages

Random known msg

X_1 ... X_t ⟶ Y_1 ... Y_N

Some Y_i must have the same right half as the target

Select s.t. $\{\mathbf{Right}(Y_1), \ldots, \mathbf{Right}(Y_N)\} = \mathbb{Z}_N$

Question: How big is t so that selection is possible w.h.p?

Coupon-Collector problem:
-There are N types of coupons
-We buy t coupons and wish to have all N types w.h.p.

Classic setting: coupons have truly random types → $t \approx 2N\ln(N)$

Our setting: known msg are distinct, so coupons are biased towards new types

→ $t \approx \min\{2\sqrt{MN\ln(N)}, 2N\ln(N)\}$

Pinpointing The Correct Known Message

Y_1 ⋯ Y_N Z

$\{\mathbf{Right}(Y_1), \ldots, \mathbf{Right}(Y_N)\} = \mathbb{Z}_N$

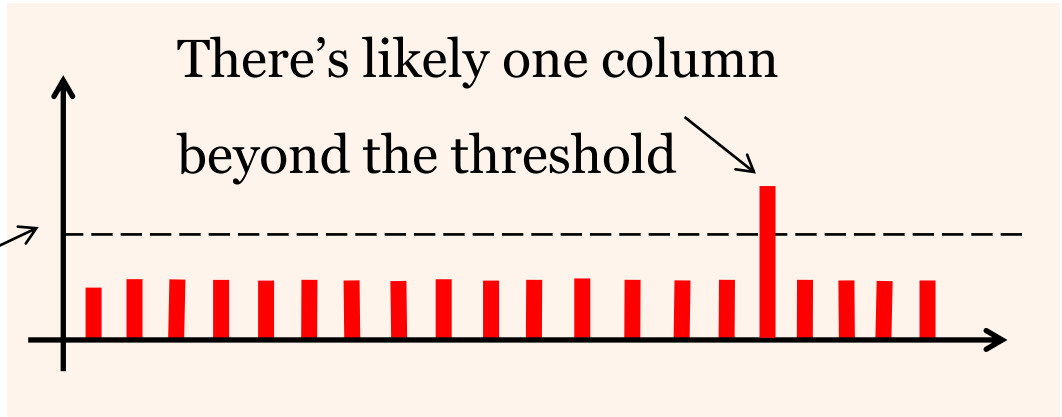
$C_{1,1}$ ⋯ $C_{N,1}$ C_1^* ⋯ C_q^*

⋮ ⋮

$C_{1,q}$ $C_{N,q}$

If $\mathbf{Right}(Y_k) = \mathbf{Right}(Z)$

For each Y_k, plot the frequency histogram of $\mathbf{Left}(C_i^*) \boxminus \mathbf{Left}(C_{k,i})$



$\left(\frac{N}{MN-1} + \frac{\Delta}{2}\right)q$

Pinpointing The Correct Known Message

Y_1 ⋯ Y_N Z

$\{\mathbf{Right}(Y_1), \ldots, \mathbf{Right}(Y_N)\} = \mathbb{Z}_N$

$C_{1,1}$ ⋯ $C_{N,1}$ C_1^* ⋯ C_q^*

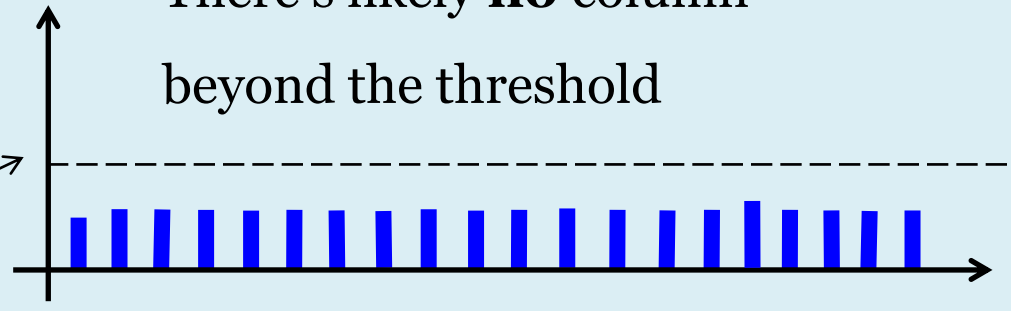
⋮ ⋮

$C_{1,q}$ $C_{N,q}$

If $\mathbf{Right}(Y_k) \neq \mathbf{Right}(Z)$

For each Y_k, plot the frequency histogram of $\mathbf{Left}(C_i^*) \boxminus \mathbf{Left}(C_{k,i})$

There's likely **no** column beyond the threshold

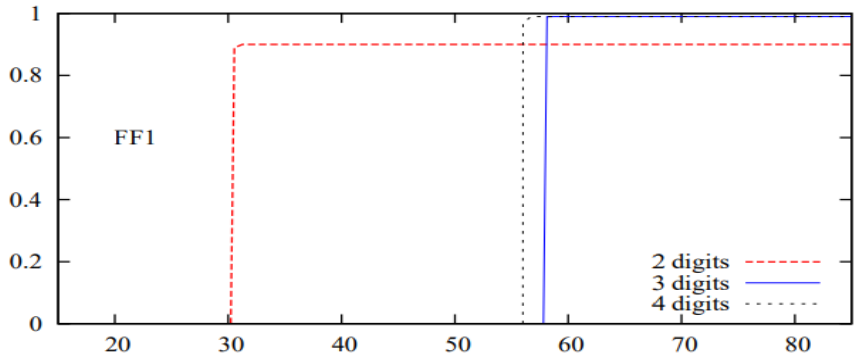


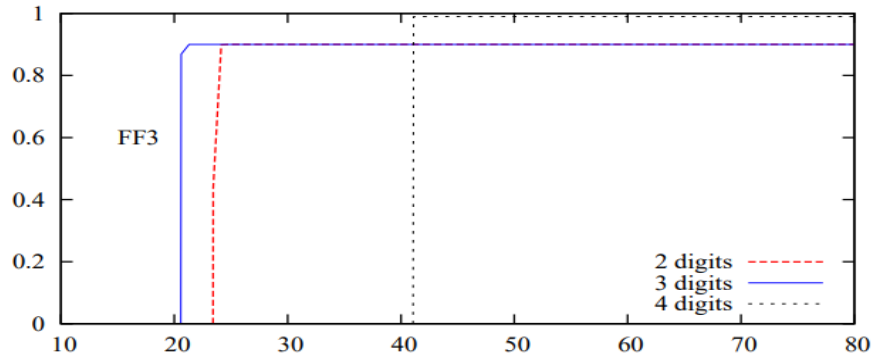
$$\left(\frac{N}{MN-1} + \frac{\Delta}{2}\right)q$$

How Many Tweaks Needed?

Theorem: Suppose that we use $t = \lceil \min\{2\sqrt{MN\ln(N)}, 2N\ln(N)\} \rceil$ random distinct known msg under q tweaks, and want to recover p targets. Then the recovery rate is at least $1 - \frac{1}{N} - p\left(\frac{Mq}{12N^{r-2}}\right) - MNp\left(\frac{Mq}{9N^{r-2}}\right)$

Recovery rate





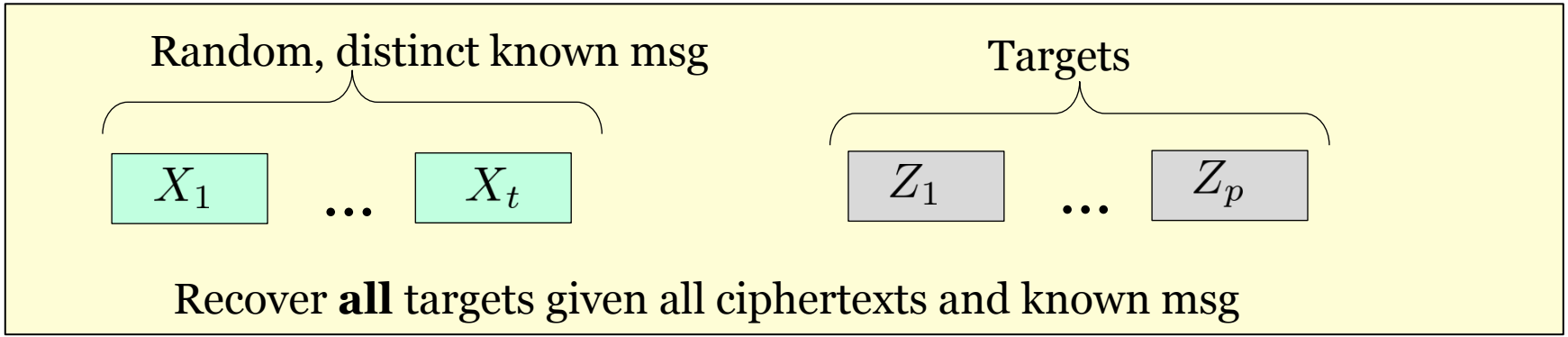
Log (base 2) of q

Experiments On FF3

Empirical results are even better than theoretical analysis

Domain	**# known msg,** t	**# of tweaks,** q	**Recovery rate**	**Time (min)**
$\{0,1\}^7$	33	2^{20}	100%	0.9
		2^{19}	66%	0.46
$\{0,\ldots,9\}^2$	31	2^{23}	100%	5.92
		2^{22}	86%	3.06
$\{0,\ldots,9\}^3$	96	2^{20}	100%	8.72
		2^{19}	66%	5.3

Generalization



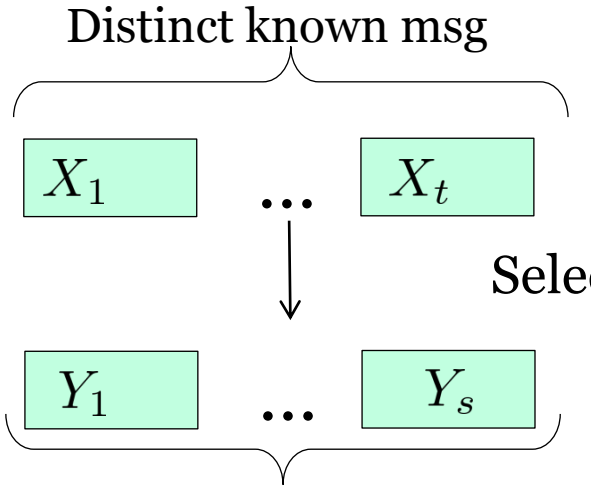
Want:

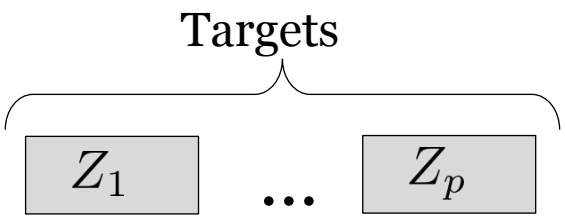
-Handle **arbitrary** distribution of known msg

-Relax the requirements by recovering just **some** (not all) targets

Generalized Attack

Can recover every Z_i satisfying $\mathbf{Right}(Z_i) \in \{\mathbf{Right}(X_1), \ldots, \mathbf{Right}(X_t)\}$





Select s.t. $\{\mathbf{Right}(Y_1), \ldots, \mathbf{Right}(Y_s)\}$

$= \{\mathbf{Right}(X_1), \ldots, \mathbf{Right}(X_t)\}$

To try to recover target Z_i :

-For every Y_k, use frequency histogram to check if $\mathbf{Right}(Y_k) = \mathbf{Right}(Z_i)$

-If such Y_k is found, recover Z_i

Conclusion

-Our attacks are practical for
- FF1/FF3/FNR on tiny domains
- DTP on **any** domains

Recommendation:

-Don't use DTP

Protegrity is already moving to FF1

-Use double encryption for FF1/FF3 on tiny domains, as suggested by ANSI