Linear Cryptanalysis of FF3-1 and FEA

Tim Beyne

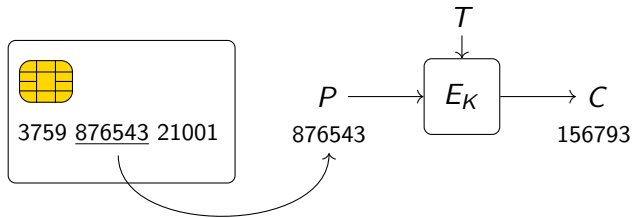
imec-COSIC, ESAT, KULeuven

August 17, 2021

COSIC

Format Preserving Encryption

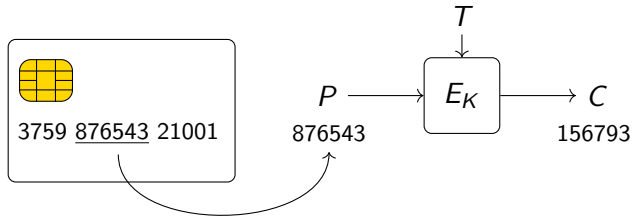
- Encryption on a small domain



- Tweak T

Format Preserving Encryption

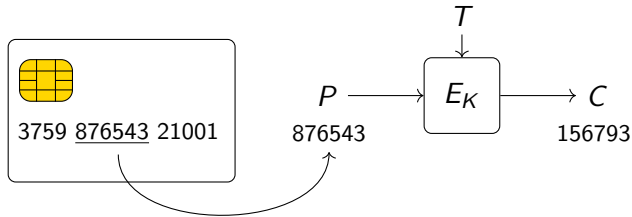
- Encryption on a small domain



- Tweak T
- Standards
  - United States: FF1 and FF3-1 (NIST SP800-38G rev. 1)
  - South Korea: FEA-1 and FEA-2 (TTAK.KO-12.0275)

Format Preserving Encryption

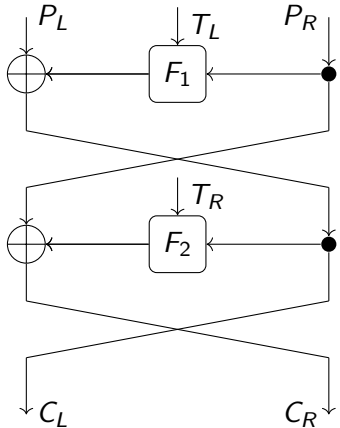
- Encryption on a small domain



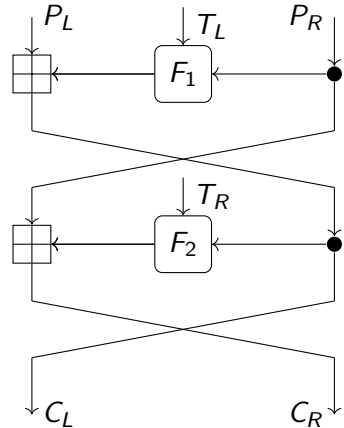
- Tweak T
- Standards
  - United States: FF1 and FF3-1 (NIST SP800-38G rev. 1)
  - South Korea: FEA-1 and FEA-2 (TTAK.KO-12.0275)

Format Preserving Encryption

FEA-1 and FF3-1



(a) FEA-1 (12^* rounds)
$P_L, P_R \in \mathbb{F}_2^m$, $N = 2^m$



(b) FF3-1 (8 rounds)
$P_L, P_R \in \mathbb{Z}/N\mathbb{Z}$

⚠ Alternating round tweaks

Format Preserving Encryption

Previous attacks on FEA and FF3/FF3-1

- Generic attacks on r-round Feistel ciphers (domain size N^2)
  - Distinguisher: $\widetilde{\mathcal{O}}(N^{r-4})$ data [Patarin, 2004]
  - Message-recovery: $\widetilde{\mathcal{O}}(N^{r-3})$ data [Bellare et al., 2016]
- Dedicated attacks on FF3 (flaw in tweak-schedule)
  - Codebook-recovery: $\widetilde{\mathcal{O}}(N^{11/6})$ data [Durak and Vaudenay, 2017]
  - Later improvements: $\widetilde{\mathcal{O}}(N^{6/4})$ data [Amon et al., 2021]
- NIST response (2019):
  - Modified tweak-schedule for FF3 ('FF3-1')
  - $N \geq 1000$

Format Preserving Encryption

Previous attacks on FEA and FF3/FF3-1

- Generic attacks on r-round Feistel ciphers (domain size N^2)
  - Distinguisher: $\widetilde{\mathcal{O}}(N^{r-4})$ data [Patarin, 2004]
  - Message-recovery: $\widetilde{\mathcal{O}}(N^{r-3})$ data [Bellare et al., 2016]

- ~~Dedicated attacks on FF3 (flaw in tweak-schedule)~~
  - ~~Codebook-recovery: $\widetilde{\mathcal{O}}(N^{11/6})$ data [Durak and Vaudenay, 2017]~~
  - ~~Later improvements: $\widetilde{\mathcal{O}}(N^{6/4})$ data [Amon et al., 2021]~~

- NIST response (2019):
  - Modified tweak-schedule for FF3 ('FF3-1')
  - $N \geq 1000$

Overview

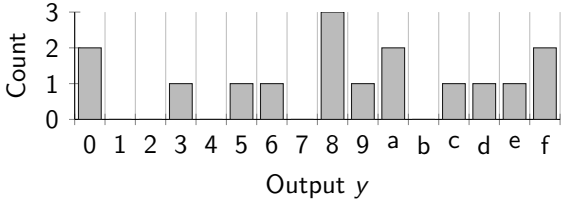
- New attacks in this work:
  - Generic attack on Feistel ciphers with alternating tweaks
  - Distinguishing/message-recovery with data $\approx \sqrt{\text{previous data}}$

- High-level overview
- Linear distinguishers
- Multidimensional linear distinguishers
- Message recovery attacks

High-level overview

Small uniform random functions

- Sample a function $F : \mathbb{F}_2^4 \to \mathbb{F}_2^4$ uniformly at random
- Output distribution of F for uniform random input?
  i.e. for each $y \in \mathbb{F}_2^4$, the number of $x \in \mathbb{F}_2^4$ s.t. $F(x) = y$

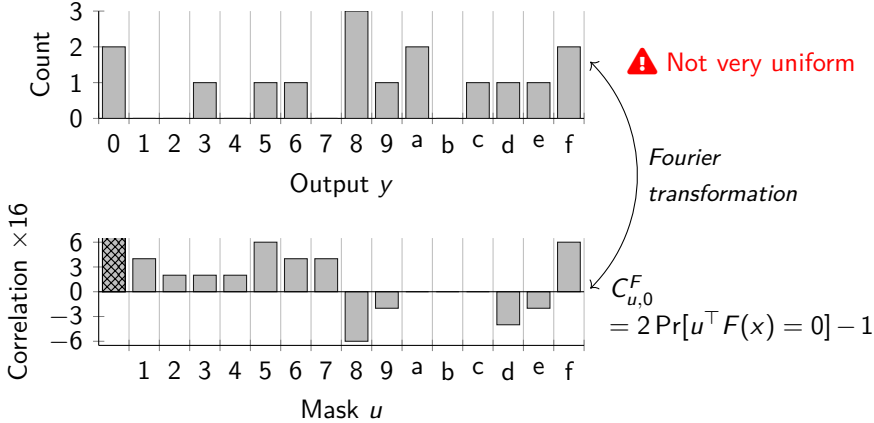


Not very uniform

High-level overview

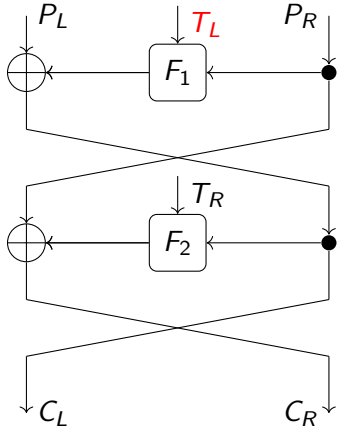
Small uniform random functions

- Sample a function $F : \mathbb{F}_2^4 \to \mathbb{F}_2^4$ uniformly at random
- Output distribution of F for uniform random input?
  i.e. for each $y \in \mathbb{F}_2^4$, the number of $x \in \mathbb{F}_2^4$ s.t. $F(x) = y$



High-level overview

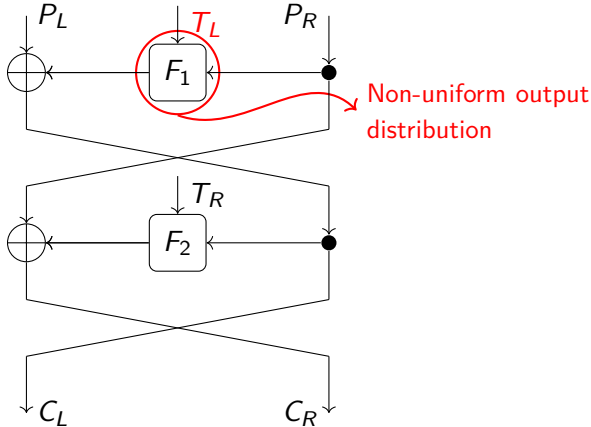
Alternating tweaks



- Fix T_L, but let (P_L, P_R, T_R) be uniform random on $(\mathbb{F}_2^m)^3$

High-level overview

Alternating tweaks



- Fix T_L, but let (P_L, P_R, T_R) be uniform random on $(\mathbb{F}_2^m)^3$

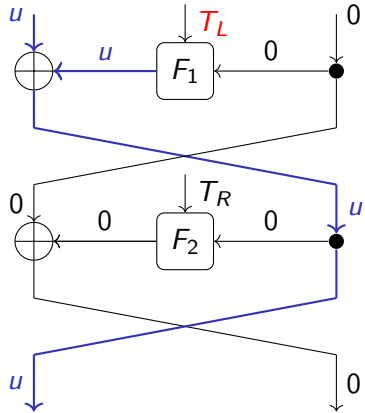
$\Longrightarrow$ $P_L + C_L$ non-uniform

Overview

- High-level overview
- Linear distinguishers
- Multidimensional linear distinguishers
- Message recovery attacks

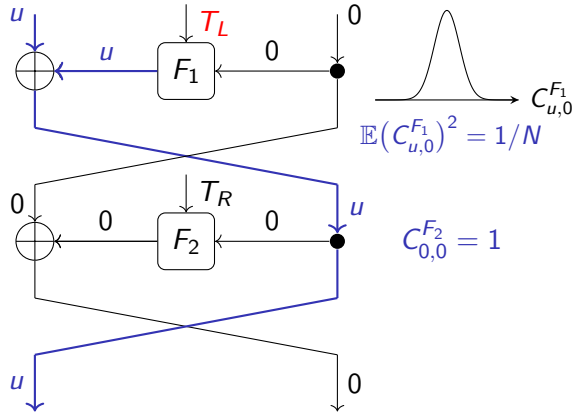
Linear distinguishers

FEA-1: Two-Round Iterative Trail



Linear distinguishers

FEA-1: Two-Round Iterative Trail



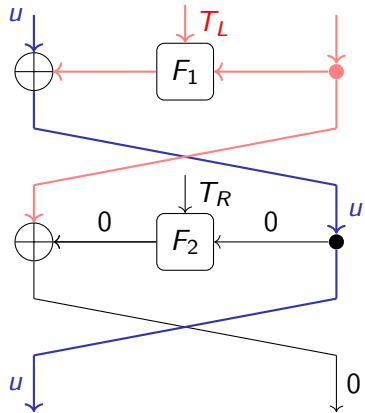
- Expected squared correlation of (dominant) r-round trail:

$$\mathbb{E}\left(C^{F_r}_{0,0} C^{F_{r-1}}_{u,0} \cdots C^{F_2}_{0,0} C^{F_1}_{u,0}\right)^2 = 1/N^{r/2}$$

Linear distinguishers

FEA-1: Improved Trail

- Fix (right half of) the plaintext

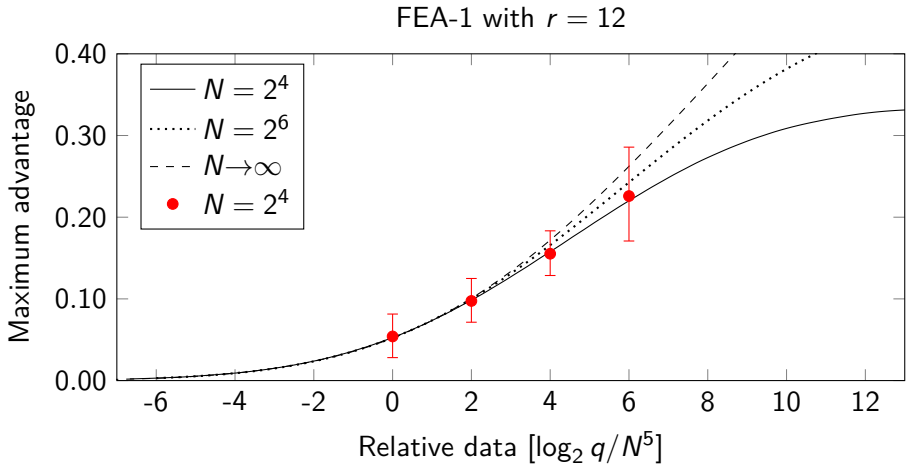


$\rightarrow$ Excected squared correlation $1/N^{r/2-1}$

- Data complexity $q = \Theta(1/c^2)$; *heuristically:* $1/c^2 \approx N^{r/2-1}$

Linear distinguishers

Concrete data complexity



- Similar figures for FEA-2 and FF3-1 in the paper

Overview

- High-level overview
- Linear distinguishers
  using approximately $N^{r/2-1}$ data
- Multidimensional linear distinguishers
- Message recovery attacks

Multidimensional linear distinguishers

Combining multiple linear approximations

- Iterative trail works for any mask u
  set of all masks is a vector space

- Instead of estimating $|c(u)|$, estimate

$$\sum_{u \neq 0} c^2(u)$$

- Data-complexity (approximate)

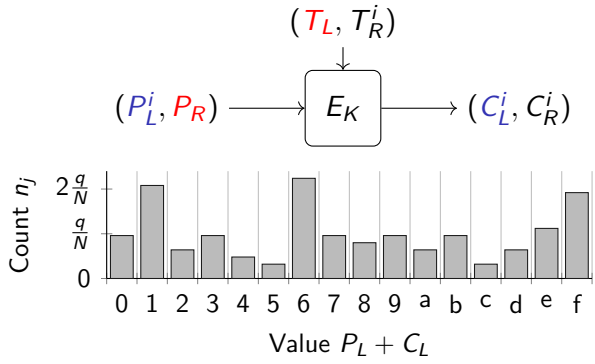
$$\sqrt{N} \Big/ \mathbb{E} \sum_{u \neq 0} c^2(u) \sim \sqrt{N} \times 1/N^{r/2-2} = N^{r/2-1.5}$$

→ Exact (fixed-key) correlations $c(u)$ unknown

Multidimensional linear distinguishers

χ^2-distinguisher

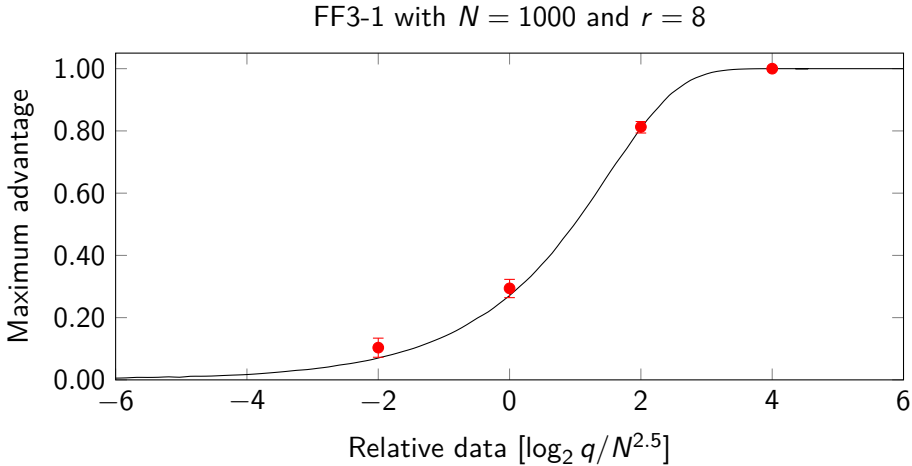
- Equivalent description of multidimensional linear distinguisher



- Euclidean distance from uniform distribution equals $\sqrt{\frac{1}{N}\sum_{u\neq 0} c^2(u)}$
- Pearson's χ^2-statistic: $\chi^2 = \frac{N}{q}\sum_{j=1}^{N}(n_j - \frac{q}{N})^2$
- Hypothesis test: $\chi^2 \geq t$?

Multidimensional linear distinguishers

Concrete data-complexity



- Similar figures for FEA-1 and FEA-2 in the paper.

Overview

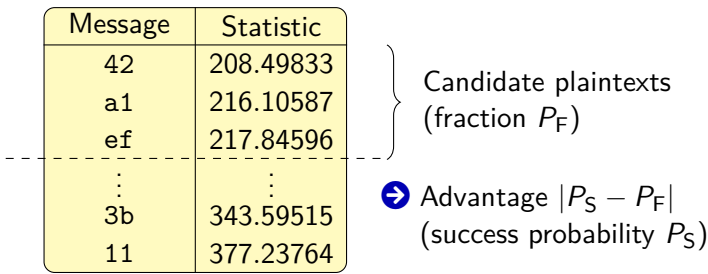
- High-level overview
- Linear distinguishers
  using approximately $N^{r/2-1}$ data
- Multidimensional linear distinguishers
  using approximately $N^{r/2-1.5}$ data
- Message recovery attacks

Message recovery attacks

Overview

- Recover a secret message
  given ciphertext under several tweaks with same T_L

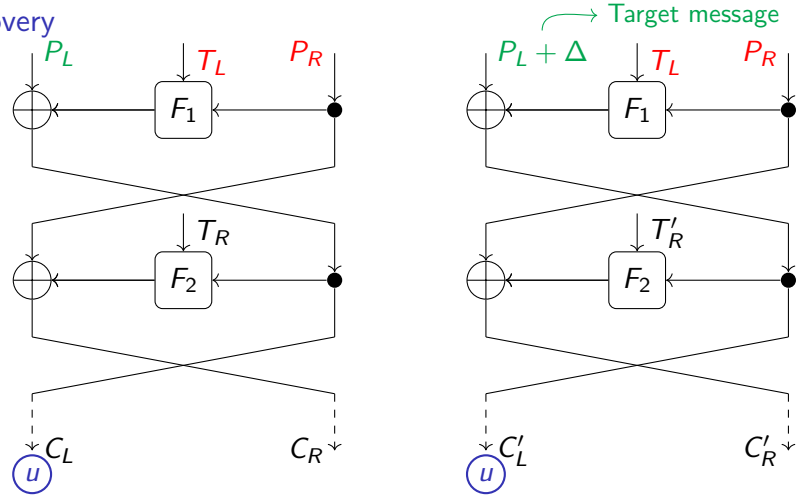
- Results in a ranking of candidate plaintexts



- Left-half and right-half message-recovery attacks

Message recovery attacks

Left-half recovery

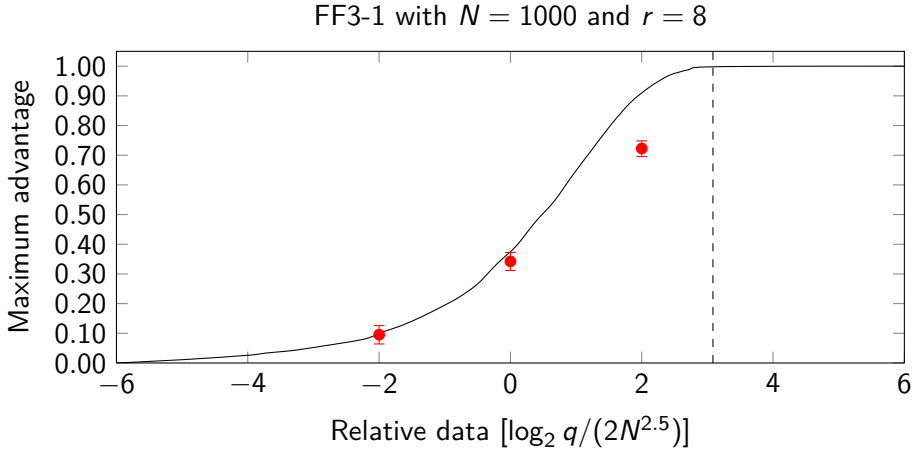


- Distribution of $C'_L \approx$ distribution of C_L translated by Δ
- Motivation: dominant trail gives $c_2(u) \approx (-1)^{u^\top \Delta} c_1(u)$
- Δ can be recovered due to non-uniformity of ciphertexts

Message recovery attacks

Left-half recovery

- Need approximately $N^{r/2-1.5}$ data
- Limitation for FF3-1: $N < 2^{12}$ due to tweak length (unless P_L is variable)

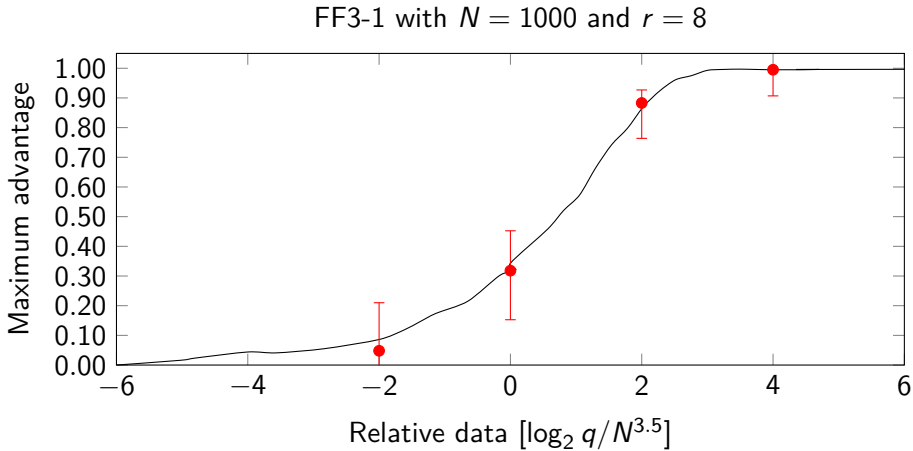


Message recovery attacks
Right-half recovery

- Similar to left-half recovery
  - Recover $F_1(P'_R) - F_1(P_R)$ with P_R known and P'_R the target
  - If $F_1(P'_R) = F_1(P_R)$, then probably $P'_R = P_R$
- Requires $N/2$ times more data (when testing all possible P_R)
- Less limitations on N than left-half recovery because P_L is variable

Message recovery attacks

Right-half recovery



Conclusions

- New attacks on FF3-1 and FEA-1
  - Distinguishers: $N^{r/2-1.5}$ data
  - Left-half message-recovery: $N^{r/2-1.5}$ data
  - Right-half message-recovery: $N^{r/2-0.5}$ data

  (attacks on FEA-2 and key-recovery for FEA-1: see paper)

Conclusions

- New attacks on FF3-1 and FEA-1
  - Distinguishers: $N^{r/2-1.5}$ data
  - Left-half message-recovery: $N^{r/2-1.5}$ data
  - Right-half message-recovery: $N^{r/2-0.5}$ data

  (attacks on FEA-2 and key-recovery for FEA-1: see paper)

- Practical relevance
  - Data with half-fixed tweak is typical (e.g. counter as tweak)
  - High false-positive rate is often acceptable (e.g. checksums, ...)

- Be careful and avoid these standards until they are fixed
  - Don't rely on indistinguishability of ciphertext
  - Avoid the smallest domain sizes

- Alternatives to Feistel-based FPE

`https://homes.esat.kuleuven.be/~tbeyne/fpe`

tim.beyne@esat.kuleuven.be