On The Distribution of Linear Biases: Three Instructive Examples

Mohamed Ahmed Abdelraheem[1], Martin Ågren[2], Peter Beelen[1], and Gregor Leander[1]

[1] Technical University of Denmark

[2] Lund University, Sweden

Outline

Outline

Setting

We are analyzing/constructing/breaking block ciphers...

Fix the (unknown) key and consider the permutation

$F\colon\ \mathbb{F}_2^n \to \mathbb{F}_2^n$.

Linear Approximation

Given

$$F : \mathbb{F}_2^n \to \mathbb{F}_2^n,$$

a linear approximation is an equation like

$$\langle \boldsymbol{\alpha}, \mathbf{x} \rangle = \langle \boldsymbol{\beta}, F(\mathbf{x}) \rangle.$$

(Input mask $\boldsymbol{\alpha}$, output mask $\boldsymbol{\beta}$.)

Linear Approximation

Given

$$F : \mathbb{F}_2^n \to \mathbb{F}_2^n,$$

a linear approximation is an equation like

$$\langle \boldsymbol{\alpha}, \mathbf{x} \rangle = \langle \boldsymbol{\beta}, F(\mathbf{x}) \rangle.$$

(Input mask $\boldsymbol{\alpha}$, output mask $\boldsymbol{\beta}$.)

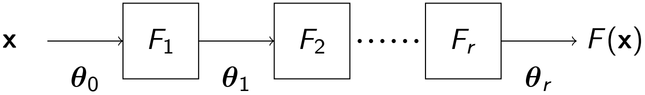
The bias $\epsilon_F(\boldsymbol{\alpha}, \boldsymbol{\beta})$:

$$\mathbf{Pr}\left[\langle \boldsymbol{\alpha}, \mathbf{x} \rangle = \langle \boldsymbol{\beta}, F(\mathbf{x}) \rangle\right] = \frac{1}{2} + \epsilon_F(\boldsymbol{\alpha}, \boldsymbol{\beta})$$

The correlation $c_F(\boldsymbol{\alpha}, \boldsymbol{\beta})$:

$$c_F(\boldsymbol{\alpha}, \boldsymbol{\beta}) = 2\epsilon_F(\boldsymbol{\alpha}, \boldsymbol{\beta})$$

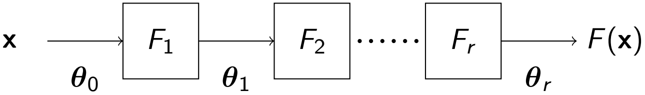
Linear Approximation of a Composite Function



A linear trail θ is a collection of all intermediate masks

$$\boldsymbol{\theta} = (\boldsymbol{\theta}_0 = \boldsymbol{\alpha}, \ldots, \boldsymbol{\theta}_r = \boldsymbol{\beta}).$$

Linear Approximation of a Composite Function



A linear trail θ is a collection of all intermediate masks

$$\boldsymbol{\theta} = (\boldsymbol{\theta}_0 = \boldsymbol{\alpha}, \ldots, \boldsymbol{\theta}_r = \boldsymbol{\beta}).$$

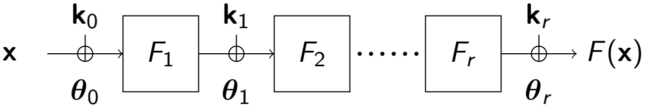
The correlation of a trail is

$$C_{\boldsymbol{\theta}} = \prod_i c_{F_i}(\boldsymbol{\theta}_i, \boldsymbol{\theta}_{i+1}).$$

Theorem

$$c_F(\boldsymbol{\alpha}, \boldsymbol{\beta}) = \sum_{\boldsymbol{\theta}:\ \boldsymbol{\theta}_0 = \boldsymbol{\alpha}, \boldsymbol{\theta}_r = \boldsymbol{\beta}} C_{\boldsymbol{\theta}}.$$

Linear Approximation of a Composite Function



A linear trail θ is a collection of all intermediate masks

$$\boldsymbol{\theta} = (\boldsymbol{\theta}_0 = \boldsymbol{\alpha}, \ldots, \boldsymbol{\theta}_r = \boldsymbol{\beta}).$$

The correlation of a trail is

$$C_{\boldsymbol{\theta}} = (-1)^{\langle \boldsymbol{\theta}, \mathbf{k} \rangle} \prod_i c_{F_i}(\boldsymbol{\theta}_i, \boldsymbol{\theta}_{i+1}).$$

Theorem (Linear Hull)

$$c_F(\boldsymbol{\alpha}, \boldsymbol{\beta}) = \sum_{\boldsymbol{\theta}:\ \boldsymbol{\theta}_0 = \boldsymbol{\alpha}, \boldsymbol{\theta}_r = \boldsymbol{\beta}} (-1)^{\langle \boldsymbol{\theta}, \mathbf{k} \rangle} C_{\boldsymbol{\theta}}.$$

Outline

The Problem

We can: bound the correlation of single linear trails.

We cannot: bound the correlation of a linear approximation.

Because: Many linear trails interact in a key dependent way.

Each key gives a different correlation.
We need to understand the distribution.

Some Approaches

I: Deal with single trails.

Some Approaches

I: Deal with single trails.

II: Model the situation – make assumptions.
(Possible assumption: Different trails are independent.)

Some Approaches

I: Deal with single trails.

II: Model the situation – make assumptions.
(Possible assumption: Different trails are independent.)

III: Perform experiments to validate the model/assumptions.

Some Approaches

I: Deal with single trails.

II: Model the situation – make assumptions.
(Possible assumption: Different trails are independent.)

III: Perform experiments to validate the model/assumptions.

Todo: Develop a sound framework.
Why has it not been done before?

- it's difficult
- we didn't try very hard

Our Contribution

Three interesting examples of what can happen.

- Counterexample to earlier “theorem”.
- Give an idea what you can/cannot hope to prove.
- Serve as inspiration for future work.

Outline

Normal Distribution?

Consider an n-bit block cipher and assume

- independent round keys,
- (exponentially in n) many non-zero trails,
- all with the same absolute correlation.

If we pick a key, what bias do we get?

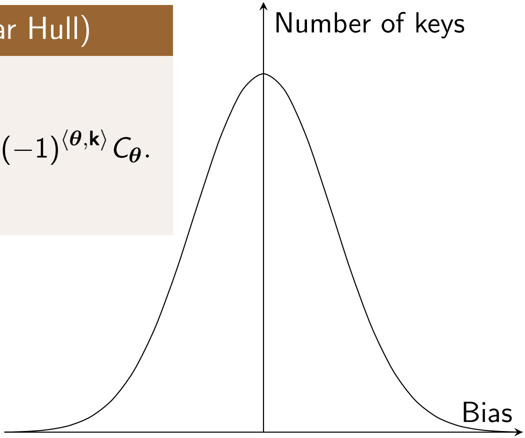
Theorem (Daemen and Rijmen, ePrint 2005/212)

The bias distribution tends to a normal distribution as $n \to \infty$.

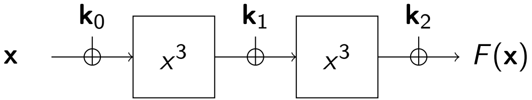
Normal Distribution?

Theorem (Linear Hull)

$$c_F(\boldsymbol{\alpha}, \boldsymbol{\beta}) = \sum_{\boldsymbol{\theta}} (-1)^{\langle \boldsymbol{\theta}, \mathbf{k} \rangle} C_{\boldsymbol{\theta}}.$$

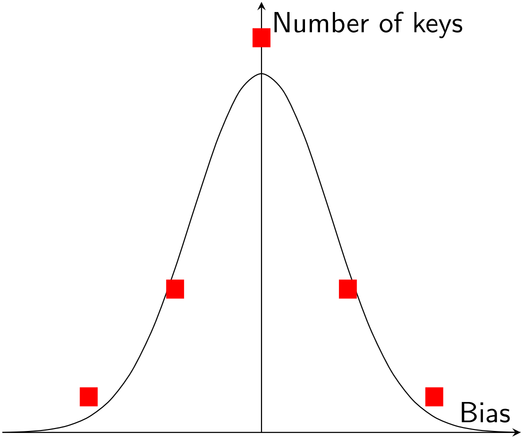


The CUBE Cipher



- independent round keys, ✓
- (exponentially in n) many non-zero trails, ✓
- all with the same absolute correlation, ✓
- toy cipher.

Normal Distribution?



CUBE cipher vs. the normal distribution.

Only 5 values — for any n!

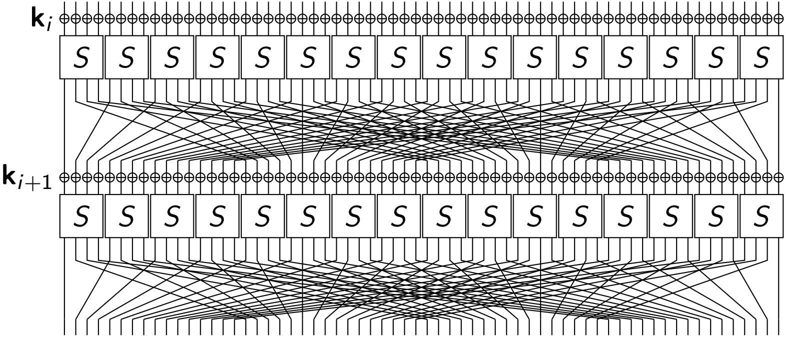
The Role of Key-Scheduling

Common analysis:
Assume independent round keys
and hope that the key-scheduling
does not influence the distribution.

Two counter-examples:

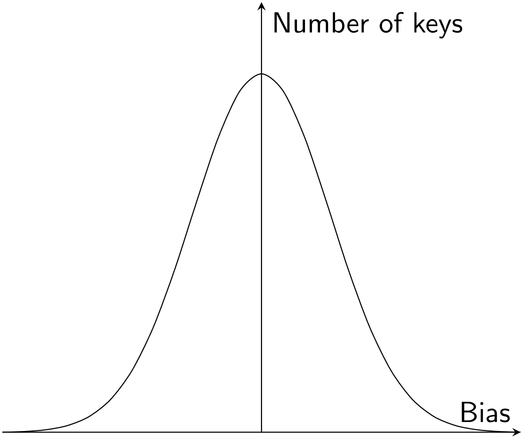
- PRESENT with identical round-keys
- PRINTcipher

PRESENT



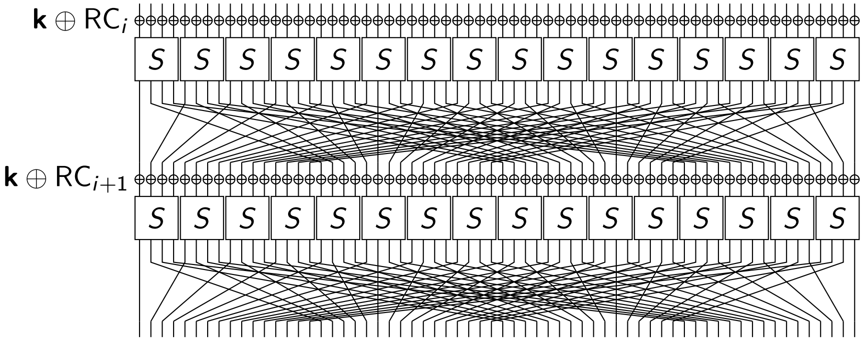
- many linear trails with one active Sbox per round
- distribution is close to normal

PRESENT



Distribution for 17 rounds of PRESENT.

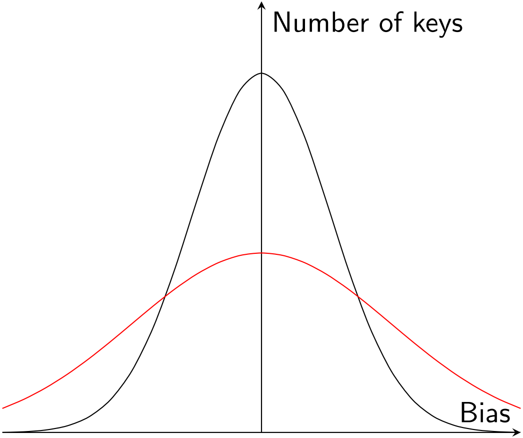
PRESENT with Identical Round-Keys



Modification:

- identical round-keys
- round constants

PRESENT With Identical Round-Keys

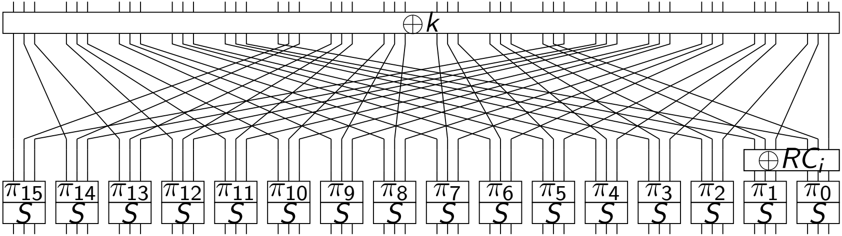


Identical vs. original round-keys.

PRESENT-Conclusions

- PRESENT-const is not secure.
- SPONGENT does not have the PRESENT Sbox.
- More rounds help.

PRINTcipher, Invariant Subspaces, and Eigenvectors

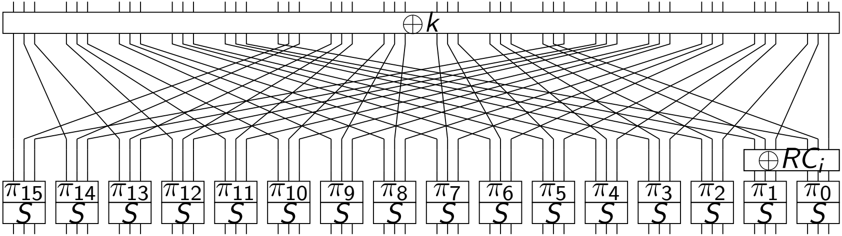


Last year at CRYPTO: invariant subspaces:

Let $U \subseteq \mathbb{F}_2^n$ be a subspace and $d \in \mathbb{F}_2^n$. Assume a weak key.

$$F_k(U + d) = U + d.$$

PRINTcipher, Invariant Subspaces, and Eigenvectors



Last year at CRYPTO: invariant subspaces:

Let $U \subseteq \mathbb{F}_2^n$ be a subspace and $d \in \mathbb{F}_2^n$. Assume a weak key.

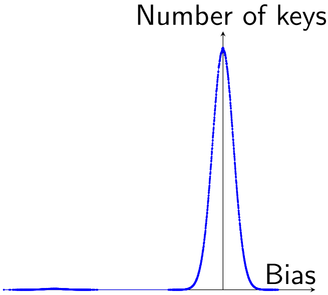
$$F_k(U + d) = U + d.$$

$$\Downarrow$$

$$F(U + d) = U + d.$$

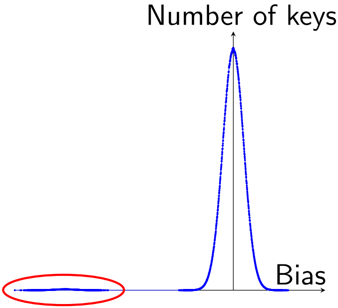
Linear Biases in PRINTcipher

"PRINTcipher-24:"



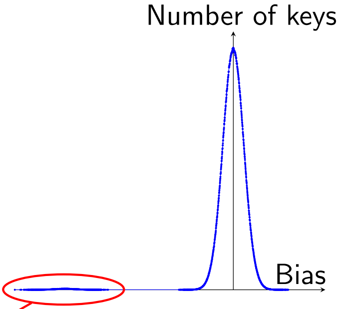
Linear Biases in PRINTcipher

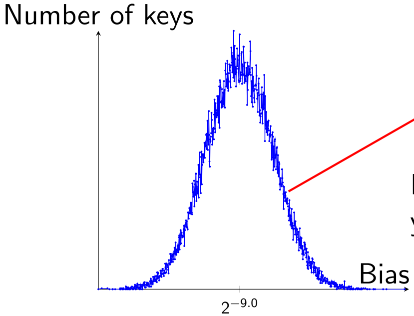
"PRINTcipher-24:"



Linear Biases in PRINTCIPHER

"PRINTCIPHER-24:"





Precisely those keys that yield an invariant subspace!

Correlation Matrices; an Eigenvector

Correlation matrix $C = (c_F(\alpha, \beta))_{\alpha,\beta}$.

Theorem

Invariant subspace $\Rightarrow$ A sub-matrix (A) of the correlation matrix has an eigenvector with a special $\pm$-structure and eigenvalue 1.

The matrix has a nonzero limit. We have trail-clustering!

The Matrix Power Limit

The eigenvector is

$$\text{const} \cdot \begin{pmatrix} +1 & +1 & -1 & -1 & +1 & +1 & -1 & \dots \end{pmatrix}.$$

The Matrix Power Limit

The eigenvector is

$$\text{const} \cdot \begin{pmatrix} +1 & +1 & -1 & -1 & +1 & +1 & -1 & \dots \end{pmatrix},$$

so

$$A^r \to \text{const}^2 \cdot \begin{pmatrix} +1 & +1 & -1 & -1 & +1 & +1 & -1 & \dots \\ +1 & +1 & -1 & -1 & +1 & +1 & -1 & \dots \\ -1 & -1 & +1 & +1 & -1 & -1 & +1 & \dots \\ -1 & -1 & +1 & +1 & -1 & -1 & +1 & \dots \\ +1 & +1 & -1 & -1 & +1 & +1 & -1 & \dots \\ +1 & +1 & -1 & -1 & +1 & +1 & -1 & \dots \\ -1 & -1 & +1 & +1 & -1 & -1 & +1 & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}.$$

The Matrix Power Limit

The eigenvector is

$$\text{const} \cdot \begin{pmatrix} +1 & +1 & -1 & -1 & +1 & +1 & -1 & \dots \end{pmatrix},$$

so

$$A^r \to \frac{1}{2^{16}-1} \cdot \begin{pmatrix} +1 & +1 & -1 & -1 & +1 & +1 & -1 & \dots \\ +1 & +1 & -1 & -1 & +1 & +1 & -1 & \dots \\ -1 & -1 & +1 & +1 & -1 & -1 & +1 & \dots \\ -1 & -1 & +1 & +1 & -1 & -1 & +1 & \dots \\ +1 & +1 & -1 & -1 & +1 & +1 & -1 & \dots \\ +1 & +1 & -1 & -1 & +1 & +1 & -1 & \dots \\ -1 & -1 & +1 & +1 & -1 & -1 & +1 & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}.$$

Indeed, experimentally,
$c_F(\alpha, \beta) \approx \pm 2^{-16}$ (PRINTcipher-48).

Is There any Hope?

Theorem

Invariant subspace $\Rightarrow$ A sub-matrix of the correlation matrix has an eigenvector with a special $\pm$-structure and eigenvalue 1.

Is There any Hope?

Actually,

Theorem

Invariant subspace $\Leftrightarrow$ *A sub-matrix of the correlation matrix has an eigenvector with a special* $\pm$*-structure and eigenvalue* 1.

Outline

Conclusion

- Assessing security against linear cryptanalysis is tricky.
- An old "theorem" is not entirely correct
  — new attempts have to somehow deal with CUBE.

Conclusion

- Assessing security against linear cryptanalysis is tricky.
- An old "theorem" is not entirely correct
  — new attempts have to somehow deal with Cube.
- With identical round-keys, bad things can happen in various ways (PRESENT-const, PRINTcipher).
- With key-schedules, how can we *know* these things don't happen (even for just a few keys)?