Block Ciphers and Linear Cryptanalysis

19. August 2015

FluxFingers
Ruhr University Bochum

Friedrich Wiemer
Outline

1 Block Ciphers
   ■ Overview
   ■ Design Strategy
   ■ Lightweight Crypto

2 Linear Cryptanalysis
   ■ Overview
   ■ Linear Cryptanalysis
   ■ Connection to Key Schedule
Examples of Block Ciphers

- DES (Feistel Network)
- AES (Substitution Permutation Network)
- PRESENT (Lightweight Block Cipher)
DES

Feistel Networks

- proposed 1975
- developed: IBM — and NSA 😊
- 56 Bit Key
- 64 Bit Blocksize
- 16 Rounds
- 8 S-boxes: 6 → 4 Bit
DES

- proposed 1975
- developed: IBM — and NSA
- 56 Bit Key
- 64 Bit Blocksize
- 16 Rounds
- 8 S-boxes: 6 → 4 Bit
AES

Substitution Permutation Networks

- proposed 1998
- developed: Daemen and Rijmen
- 128, 192, 256 Bit Key
- 128 Bit Blocksize
- 10, 12, 14 Rounds
- 1 S-box: 8 → 8 Bits
AES

- proposed 1998
- developed: Daemen and Rijmen
- 128, 192, 256 Bit Key
- 128 Bit Blocksize
- 10, 12, 14 Rounds
- 1 S-box: 8 → 8 Bits
Design Strategy

The Mathematicians Approach

- based on security proofs
- reduce breaking the cipher to mathematical hard problems
The Mathematicians Approach

- based on security proofs
- reduce breaking the cipher to mathematical hard problems
- slow 😊

The Engineers Approach

- build efficient scheme such that it is resistant against known attacks
- fast
- small
- few math
Design Strategy

The Mathematicians Approach

- based on security proofs
- reduce breaking the cipher to mathematical hard problems
- slow 😞
- fat 😞
Design Strategy

The Mathematicians Approach

- based on security proofs
- reduce breaking the cipher to mathematical hard problems
- slow 😊
- fat 😊
- too much math 😞
Design Strategy

The Mathematicians Approach

- based on security proofs
- reduce breaking the cipher to mathematical hard problems
- slow 😞
- fat 😞
- too much math 😞

The Engineers Approach

- build efficient scheme
- such that it is resistant against known attacks
Design Strategy

The Mathematicians Approach
- based on security proofs
- reduce breaking the cipher to mathematical hard problems
- slow 😞
- fat 😞
- too much math 😞

The Engineers Approach
- build efficient scheme
- such that it is resistant against known attacks
- fast 😊
Design Strategy

The Mathematicians Approach
- based on security proofs
- reduce breaking the cipher to mathematical hard problems
- slow 🙄
- fat 😞
- too much math 😞

The Engineers Approach
- build efficient scheme
- such that it is resistant against known attacks
- fast 😊
- small 😊
Design Strategy

The Mathematicians Approach
- based on security proofs
- reduce breaking the cipher to mathematical hard problems
- slow 😊
- fat 😊
- too much math 😞

The Engineers Approach
- build efficient scheme
- such that it is resistant against known attacks
- fast 😊
- small 😊
- few math 😞
Ubiquitous Computing

- very constrained devices needed for Internet of Things
- need crypto schemes with very low requirements
Ubiquitous Computing

- very constrained devices needed for Internet of Things
- need crypto schemes with very low requirements

How efficient *(small, fast, low power, low latency)* can we be, without sacrificing security?
**PRESENT**

- proposed 2007
- developed: Orange Labs, RUB, DTU
- 1 S-box: $4 \rightarrow 4$ Bits

| 80, 128 Bit Key |
| 64 Bit Blocksize |
| 31 Rounds |
present

- proposed 2007
- developed: Orange Labs, RUB, DTU
- 1 S-box: 4 → 4 Bits
- 80, 128 Bit Key
- 64 Bit Blocksize
- 31 Rounds

Let $F_{k_i} : \mathbb{F}_2^{64} \rightarrow \mathbb{F}_2^{64}$ be PRESENT’s round function:
PRESENT

- proposed 2007
- developed: Orange Labs, RUB, DTU
- 1 S-box: 4 → 4 Bits
- 80, 128 Bit Key
- 64 Bit Blocksize
- 31 Rounds

Let $F_{k_i} : \mathbb{F}_2^{64} \rightarrow \mathbb{F}_2^{64}$ be PRESENT’s round function:

PRESENT Round

Friedrich Wiemer | Block Ciphers and Linear Cryptanalysis | 19. August 2015
Overview Attacks

## Attacks on Block Ciphers

- Differential Cryptanalysis
- *Linear Cryptanalysis*
- Integral,
- Interpolation,
- Statistical Saturation,
- Invariant Subspace,
- Algebraic,
- Related Key,
- ...
Introduction to Linear Cryptanalysis

- invented by Matsui 1993–1994
- broke DES
- together with Differential Cryptanalysis most used attack on block ciphers

Image: http://www.isce2009.ryukoku.ac.jp/eng/keynote_address.html
Can we linear approximate a function $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$?
**Basic Idea: Linear Approximations**

Dot-Product, Masks and Linear Bias

Can we linear approximate a function $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$?

**Dot-Product**

$$\langle \alpha, x \rangle = \bigoplus_{i=0}^{n-1} \alpha_i x_i$$
Can we linear approximate a function $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$?

## Dot-Product

\[
\langle \alpha, x \rangle = \bigoplus_{i=0}^{n-1} \alpha_i x_i
\]

## Mask

Let $\alpha, \beta, x \in \mathbb{F}_2^n$ and

\[
\langle \alpha, x \rangle = \langle \beta, F(x) \rangle \quad (1)
\]

- We say $\alpha$ is an *input mask* and $\beta$ is an *output mask*.
- Eq. 1 does not hold for every input/output masks.
Can we linear approximate a function $F : \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$?

**Dot-Product**

$$\langle \alpha, x \rangle = \bigoplus_{i=0}^{n-1} \alpha_i x_i$$

**Mask**

Let $\alpha, \beta, x \in \mathbb{F}_2^n$ and

$$\langle \alpha, x \rangle = \langle \beta, F(x) \rangle \quad (1)$$

- We say $\alpha$ is an *input mask* and $\beta$ is an *output mask*.
- Eq. 1 does not hold for every input/output masks.
- It is biased, i.e., $\Pr[\langle \alpha, x \rangle = \langle \beta, F(x) \rangle] = \frac{1}{2} - \varepsilon(\alpha, \beta)$. 
Example
Masks for 2-Round reduced PRESENT

Mask (21, 21) over 2 rounds
Attack

Approach

- Find good approximation for all but last round
- that is: a good \textit{mask} over $r - 1$ rounds
**Approach**

- Find good approximation for all but last round
  - that is: a good *mask* over $r - 1$ rounds
- With many plaintext/ciphertext pairs, we can observe the masks statistical behaviour
  - that is: we can compute its *bias*
Attack

Approach

- Find good approximation for all but last round
  that is: a good mask over \( r - 1 \) rounds

- With many plaintext/ciphertext pairs, we can observe the masks statistical behaviour
  that is: we can compute its bias

- Hypothesis of Wrong Key Randomization
- Guess last round key and compute experimental bias
Example
Linear Cryptanalysis of 3-Round reduced PRESENT

Attacking 3-Round reduced PRESENT
■ Attack complexity of linear cryptanalysis is proportional to $\frac{1}{\varepsilon^2}$.
■ In experiments, we observe a key dependency of the linear bias.
Attack complexity of linear cryptanalysis is proportional to $\frac{1}{\varepsilon^2}$.
In experiments, we observe a key dependency of the linear bias.

The distribution of linear biases follows a normal distribution.
Its width is defined by the variance.
Attack complexity of linear cryptanalysis is proportional to $\frac{1}{\varepsilon^2}$.
In experiments, we observe a key dependency of the linear bias.

The distribution of linear biases follows a normal distribution.
Its width is defined by the variance.

What happens with different key-schedules?
Distributions
Independent Round Keys

Linear Correlation

Friedrich Wiemer | Block Ciphers and Linear Cryptanalysis | 19. August 2015
Questions?
Thank you for your attention!