Cryptanalysis for Beginners

Ivica Nikolić

Nanyang Technological University, Singapore

17 August 2012

1 Introduction

2 Definition of Cryptanalysis

3 Techniques for Cryptanalysis

4 Crypto Designer vs Crypto Analyst

5 Conclusion

Symmetric Primitives

- The very basic building blocks of various cryptosystems
- Used because of the properties they have
- Types:
  1. **Block ciphers**
  2. Stream ciphers
  3. **Cryptographic hash functions**
  4. MACs

The Importance of Cryptanalysis

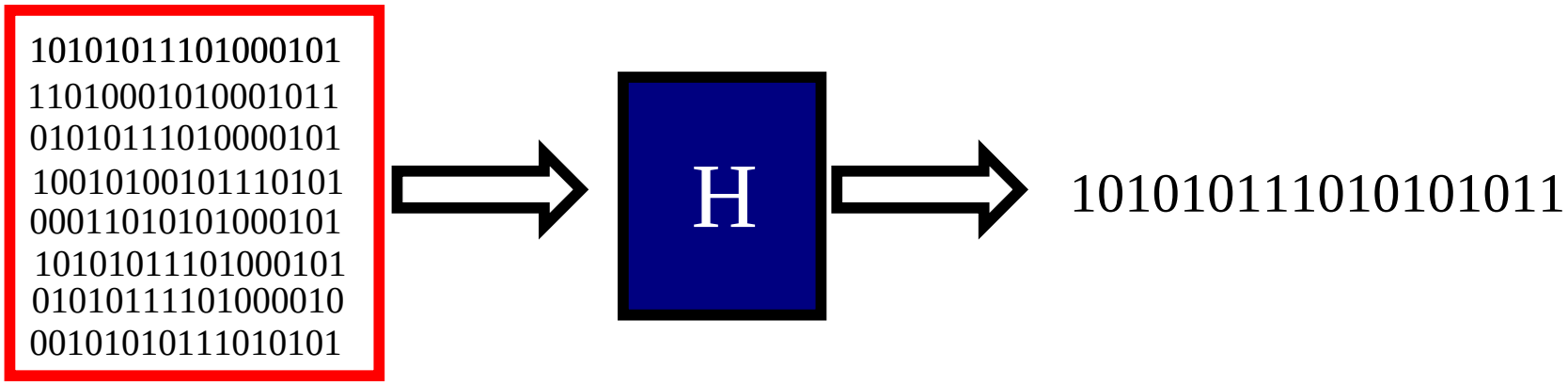
- Security of the whole system is based on the security of the primitives
- No bullet-proof approach for building secure and fast primitives

Primitives have to undergo thorough analysis

To design "secure" primitive one has to show no attacks exist

Hash Functions

- Hash function maps arbitrary length input to fixed length output
  $H : \{0,1\}^* \rightarrow \{0,1\}^n$



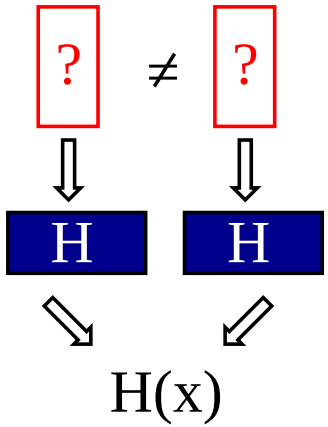
Cryptographic Hash Functions

$$H : \{0,1\}^* \rightarrow \{0,1\}^n$$

Three properties:

1. **Collisions resistance**
2. Preimage resistance
3. Second-preimage resistance

Secure if it has these properties + no "non-randomness"



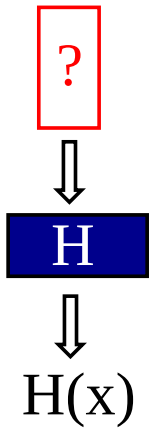
Cryptographic Hash Functions

$$H : \{0,1\}^* \rightarrow \{0,1\}^n$$

Three properties:

1. Collisions resistance
2. **Preimage resistance**
3. Second-preimage resistance

Secure if it has these properties + no "non-randomness"



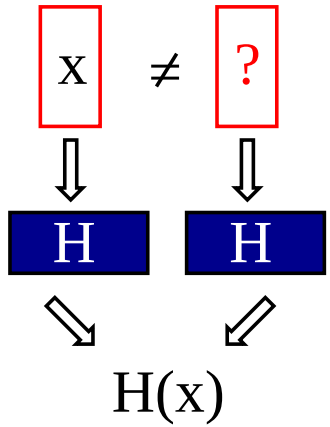
Cryptographic Hash Functions

$$H : \{0,1\}^* \rightarrow \{0,1\}^n$$

Three properties:

1. Collisions resistance
2. Preimage resistance
3. **Second-preimage resistance**

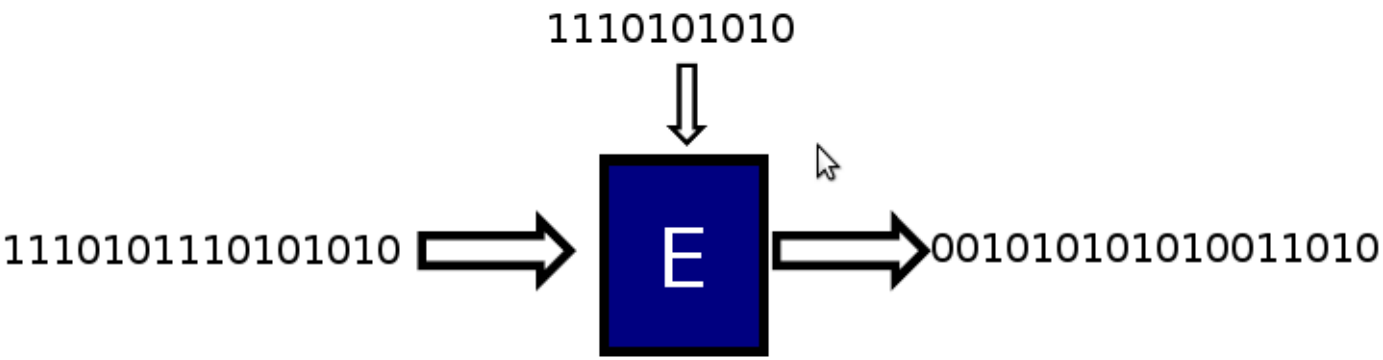
Secure if it has these properties + no "non-randomness"



Block Ciphers

$$E : \{0,1\}^n \times \{0,1\}^k \rightarrow \{0,1\}^n$$

- Cipher maps message (plaintext) into ciphertext using a secret key
- Permutation for a fixed key

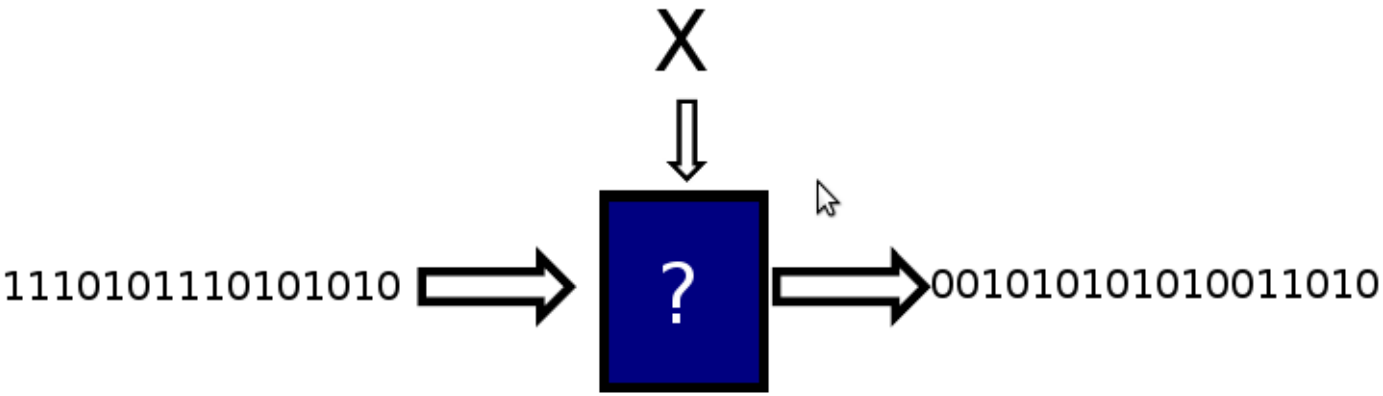


Block Ciphers

$$E : \{0,1\}^n \times \{0,1\}^k \rightarrow \{0,1\}^n$$

Frameworks for attacks (the key is secret and fixed)

- **Distinguisher - what can you say about the cipher**
- Key recovery - what can you say about the key

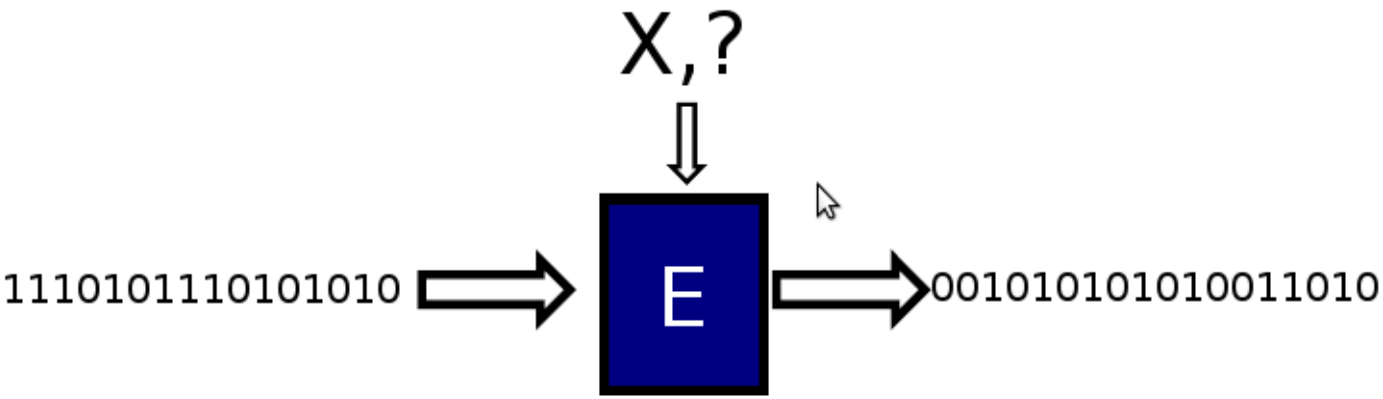


Block Ciphers

$$E : \{0,1\}^n \times \{0,1\}^k \rightarrow \{0,1\}^n$$

Frameworks for attacks (the key is secret and fixed)

- Distinguisher - what can you say about the cipher
- **Key recovery - what can you say about the key**



1 Introduction

2 Definition of Cryptanalysis

3 Techniques for Cryptanalysis

4 Crypto Designer vs Crypto Analyst

5 Conclusion

What is Cryptanalysis

The job of the cryptanalyst is to inspect the security of crypto primitive.
It boils down to:

- **Launching an attack** - showing a weakness in the primitive. The cipher/hash is marked as insecure and should not be used
- **Showing the primitive is resistant** to certain class of attacks

What is Cryptanalysis

- It is very hard to show that cipher/hash is resistant against all **known** attacks (mostly depends on the transforms used)
- It is impossible (so far) to claim the cipher/hash will stay resistant against **future** attacks

Definition of Attack

Trivial attacks are applicable to any cipher/hash, e.g:

- Brute-force of the whole key space will reveal the secret key - similar for preimages in hash
- Hashing sufficient number of messages will eventually lead to collisions

Attack is valid if it is not trivial

Definition of Attack

To claim an attack is non-trivial the cryptanalyst has to:

- Find complexity for ideal primitive
- Show that for the attacked primitive the complexity is less

The complexity depends on the input sizes, e.g. for n-bit hash, a trivial collision requires $2^{n/2}$ hash calls

1 Introduction

2 Definition of Cryptanalysis

3 Techniques for Cryptanalysis

4 Crypto Designer vs Crypto Analyst

5 Conclusion

History

Modern cryptanalysis started in the 90's with the attacks on the block cipher standard DES:

- Differential attack - Biham-Shamir
- Linear attack - Matsui

Other Techniques

New techniques emerged as a form of differential attacks or completely independent:

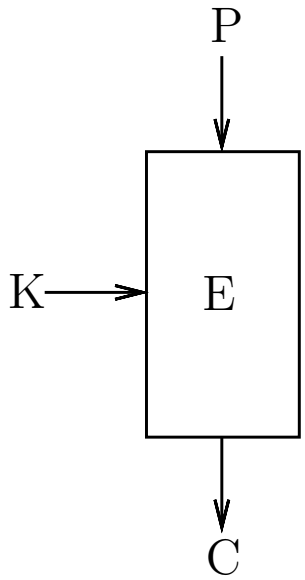
- Impossible, higher-order, boomerang/rectangle, rebound, super S-boxes attacks
- Meet-in-the-middle, splice-and-cut attacks
- Integral attacks
- Slide attack
- Mod-n cryptanalysis
- Rotational cryptanalysis
- **Many other**

NANYANG TECHNOLOGICAL UNIVERSITY

Differential Attack for Block Ciphers

Block cipher $E_K(P)$

- Input: Plaintext P and key K
- Output: Ciphertext C



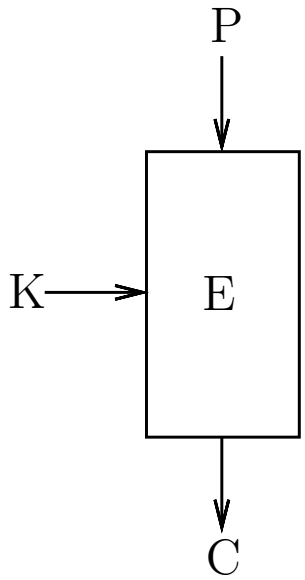
Differential Attack for Block Ciphers

Attacker does not know the key.
He can fix:

- P and obtain C
- C and obtain P

and try to find:

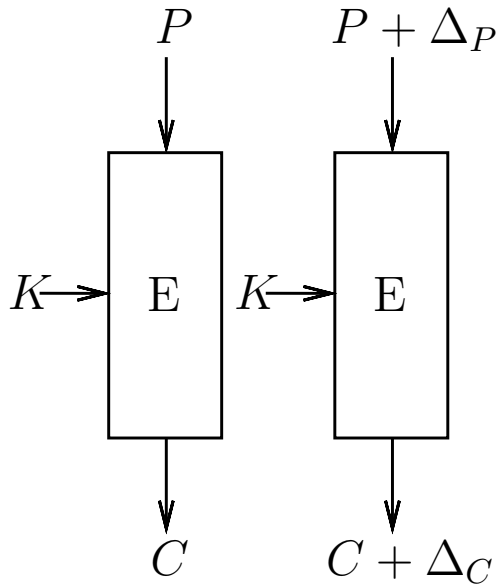
- Distinguisher
- Key recovery



Differential Attack for Block Ciphers

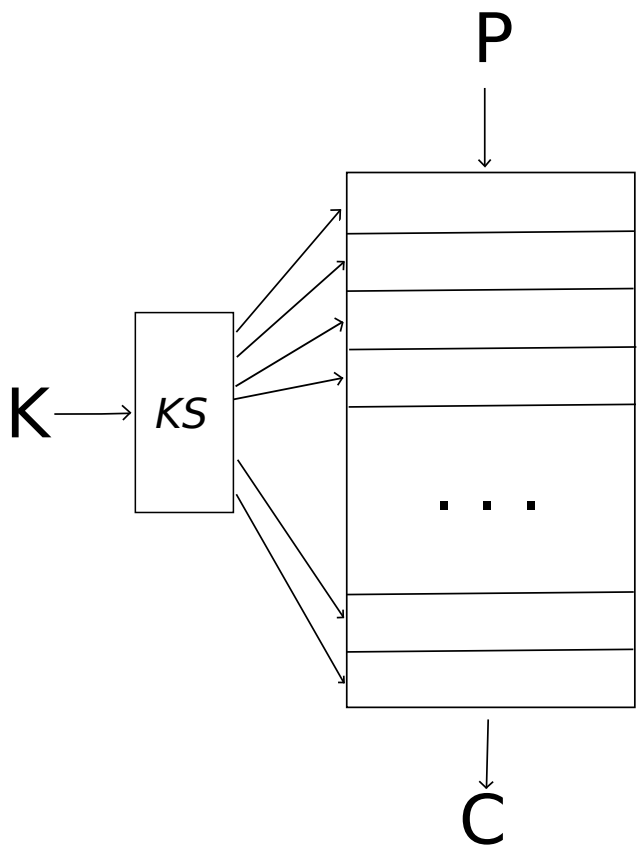
Differential analysis – the most popular form of attack. Find *specific* differences Δ_P, Δ_C s.t.:

$$\text{plaintexts } (P, P \oplus \Delta_P)$$
$$\downarrow$$
$$\text{ciphertexts } (C, C \oplus \Delta_C)$$



Differential Attack for Block Ciphers

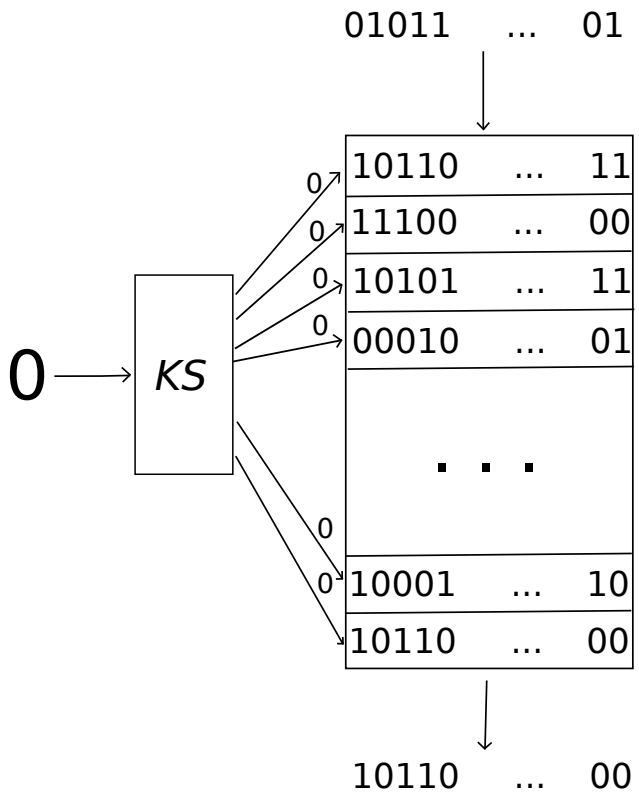
- Internally, a cipher has some number of rounds
- A key schedule from the master key produces round keys (subkeys)



Differential Attack for Block Ciphers

Differential characteristic – round-by-round propagation of some initial difference

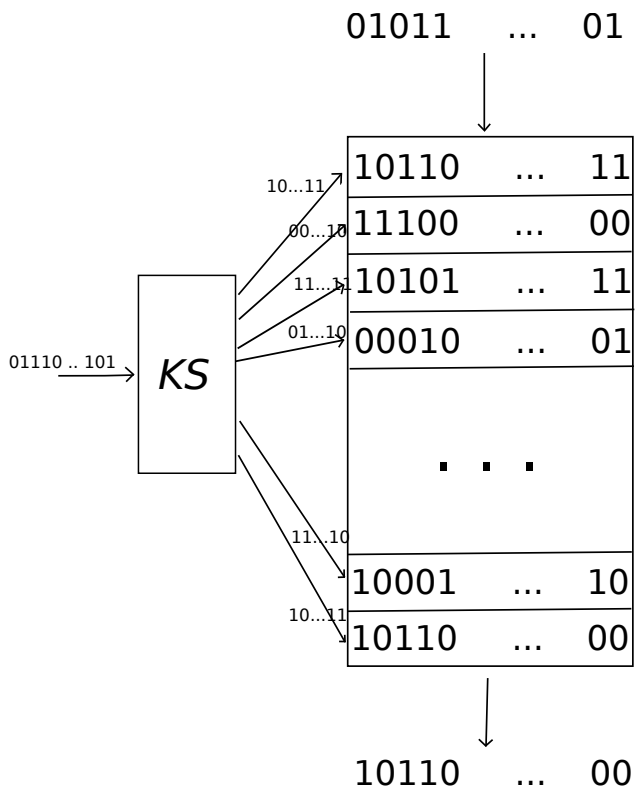
- Fixed-key differential characteristic - no difference in the key



Differential Attack for Block Ciphers

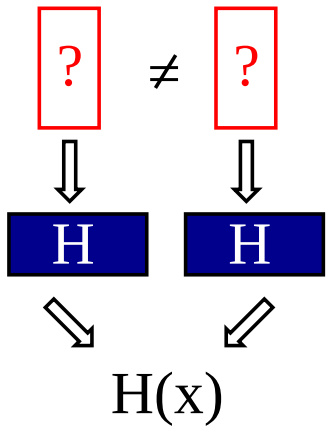
Differential characteristic – round-by-round propagation of some initial difference

- *Related-key differential characteristic* - difference in the key as well



Differential Attack for Hash Functions

- Differentials for hash functions leading to a zero output difference can produce collisions
- When the output difference is small, it leads to so-called near-collisions
- When the output difference is any, it leads to differential distinguishers



Difficulties of Launching Differential Attack

Differential attacks require large amount of effort due to enormous number of possible differential paths
A successful attack is usually a mixture of:

- Trial and error
- Experience

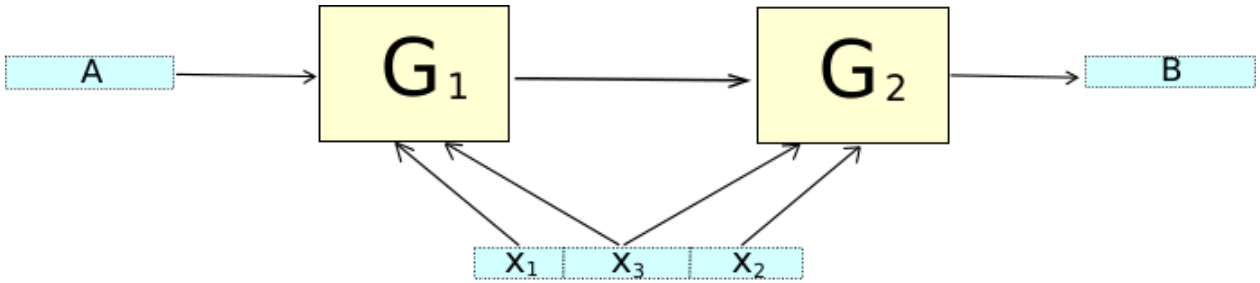
Linear Attack

Every primitive internally uses non-linear transformations (otherwise it would be a linear function and hence can easily be distinguished)

The idea of linear cryptanalysis is to approximate the non-linear transformations with linear equivalents in order to build equations involving only plaintext, ciphertext and key bits

Meet-in-the-middle Attack

- The attack is used for key recovery attacks in block ciphers and preimage attacks for hash functions
- It it applicable when the expanded message can be partitioned into two sets of independent inputs and part of the primitive can be inverted



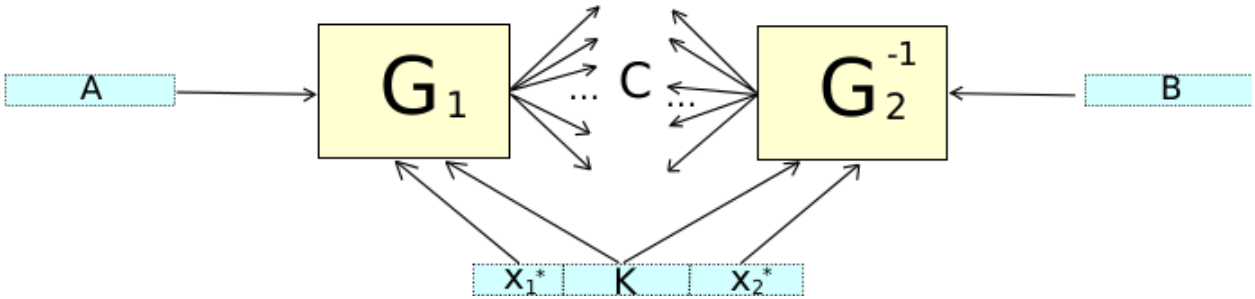
Meet-in-the-middle Attack

- Fix the input, output
- Create many intermediate values from the input
- Create many intermediate values from the output
- Check for matches

Difficulties of Launching MITM Attack

The difficulties are tightly related to its requirements:

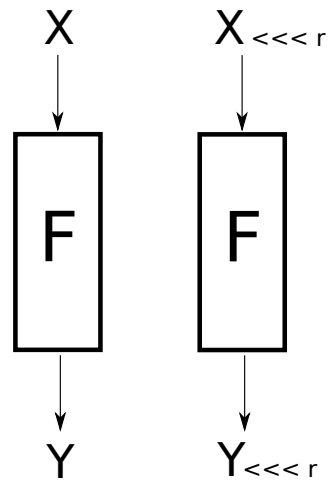
- Partitioning the input space is usually highly nontrivial
- Inverting the second part of the primitive is not always possible
- Usually, it is required to reduce the matching space



Rotational Attack

Check if $F(x) \lll_r = F(x \lll_r)$

- Applicable to certain class of primitives (ARX)
- Easy to check if the primitive is resistants
- Difficulties of launching the attack for higher number of rounds when some transforms in the primitive are non-rotational



1 Introduction

2 Definition of Cryptanalysis

3 Techniques for Cryptanalysis

4 Crypto Designer vs Crypto Analyst

5 Conclusion

Modern Proposals

Modern crypto primitive (block cipher, hash function) has to be:

1. **Efficient**
2. **Secure**

The Designer

Designers are concerned about attracting attention to the primitive.
Hence the cipher/hash has to be:

- Somehow original / completely new
- Efficient

The Analyst

Cryptanalysts are concerned only about security. Hence the cipher has to be:

- More conservative and therefore slower
- As less original as possible

Problems for the Designer

No win situation for the designer?

- If completely new design then some trivial weakness might exist
- If based on old design, then if the old design is broken, probably the proposal will be broken too
- If too many rounds then slow
- If only a few rounds then insecure

Candy for the Analyst

The analyst want to answer the yes/no question if the cipher/hash is secure. Hence, he wants to see:

- Easily breakable design :)
- Design that has some provable properties against most of the attacks
- **Clean design**

Proposal Teams

The proposal team can be:

- Designer solo = 90's proposal, insecure, hard to analyze
- Cryptanalyst solo = slow, conservative, sometimes hard to analyze
- Designer + experienced cryptanalyst = serious proposal, somewhat innovative, "secure"

How to Achieve Security and Efficiency

To achieve security:

- The old transforms should already been analyzed in the past
- The new transforms can be used only if they add to the security

To achieve efficiency:

- No redundant operations
- Carefully chosen number of rounds

1 Introduction

2 Definition of Cryptanalysis

3 Techniques for Cryptanalysis

4 Crypto Designer vs Crypto Analyst

5 Conclusion

Conclusion

- Many analysis techniques exist, differential and linear are the most powerful
- Most of the crypto primitives have been broken, including the 2 block cipher standards and 1 hash function standard => cryptanalysts have done their job
- It is harder to design both an efficient and a secure primitive than to break one