Design and Security Evaluation of Lightweight Block Ciphers

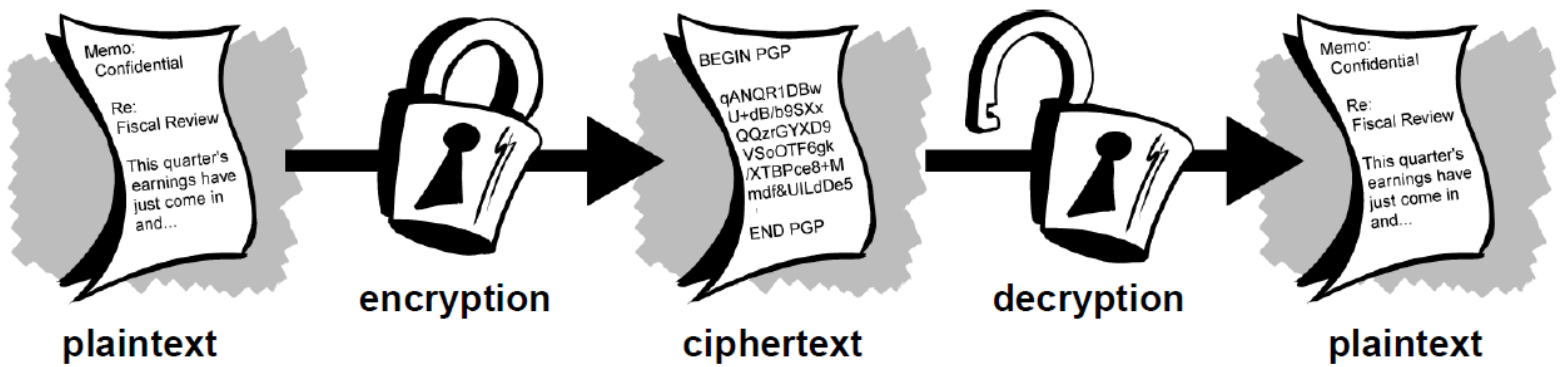
Hadi Soleimany
Shahid Beheshti University

September 2015 (*ISCISC* 2015)

Outline

Cryptography

- Cryptography is secure communication in the presence of an adversary [R. Rivest].



Lightweight Cryptography

- Constrained devices:
  - Cheaper
  - Smaller
  - More powerful

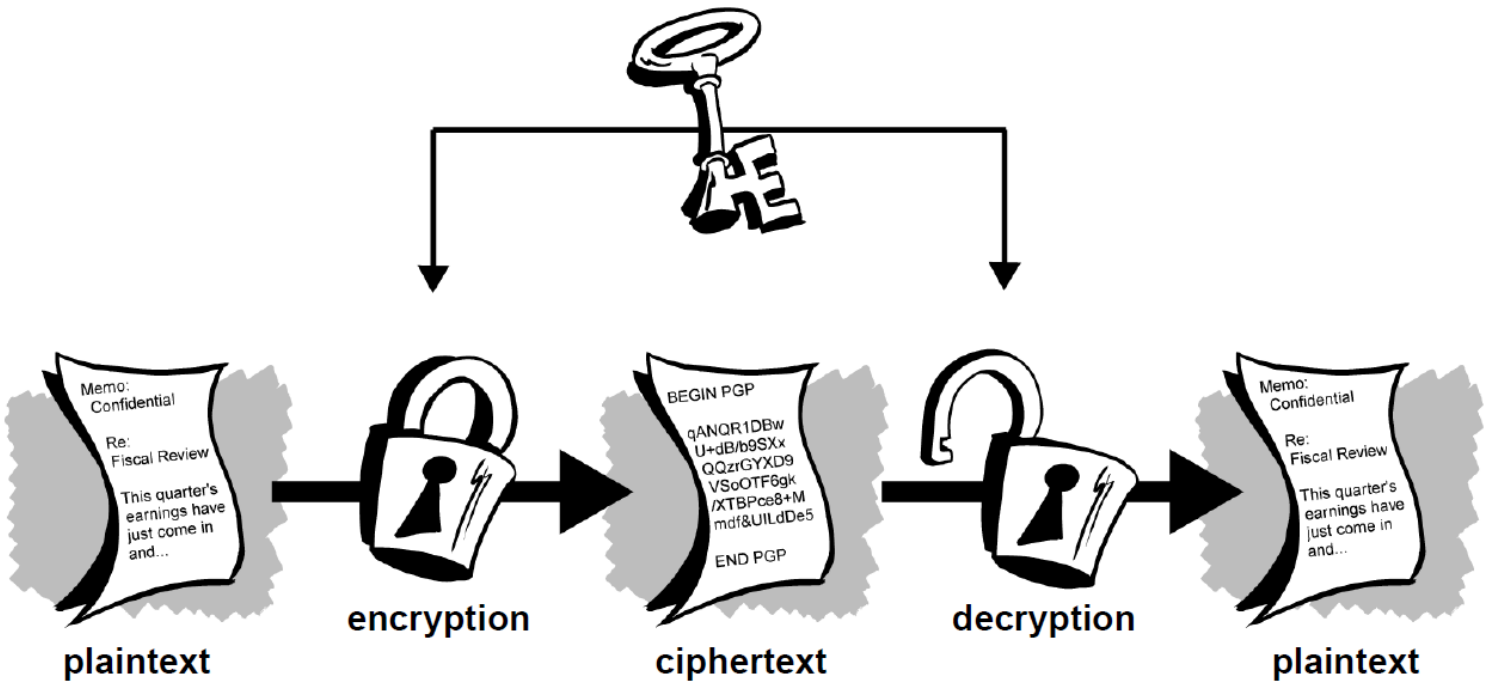
Lightweight Cryptography

- Constrained devices:
  - Cheaper
  - Smaller
  - More powerful
- Limitation of resources:
  - Computing power
  - Battery supply
  - Memory

Lightweight Cryptography

- Constrained devices:
  - Cheaper
  - Smaller
  - More powerful
- Limitation of resources:
  - Computing power
  - Battery supply
  - Memory
- Lightweight cryptography:
  - Moderate security
  - Performance (small footprint, etc.)

Symmetric Cryptography

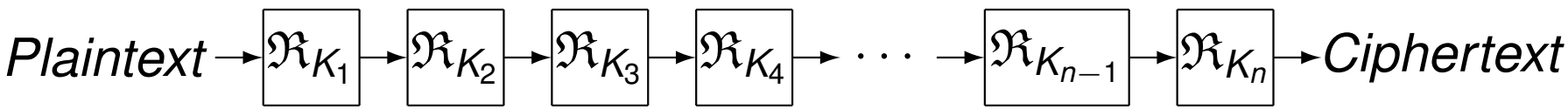


Block Cipher

Block cipher:

$$E_K(P) : \{0,1\}^k \times \{0,1\}^n \rightarrow \{0,1\}^n$$

Iterated block cipher:



$$C = \mathfrak{R}_{k_n} \circ \cdots \circ \mathfrak{R}_{k_2} \circ \mathfrak{R}_{k_1}(P)$$

Obsolescent Lightweight Ciphers

- **Crypto1:** Stream cipher with 48-bit key algorithm designed by NXP Semiconductors for Mifare RFID tags.
- **Cryptomeria cipher (C2):** 10-round Feistel block cipher which used to be employed for encrypting DVD Audio discs and Secure Digital cards.
- **DECT:** Stream cipher with a 64-bit key which was used widely in handsets and base stations in Germany.
- **DST40** is a 200-round unbalanced Feistel block cipher with a 40-bit key which is developed by Texas Instruments and licensed by the 4C Entity.
- **Keeloq** has been used widely in authentication systems of the car locks by various car manufacturers.
- **Kindle** is a stream cipher with 128-bit key which is used in the Amazon Kindle e-book reader.

Efficiency Parameters

- **Area:** Technology-independent area based on a unit called *gate equivalent* (GE) which corresponds to a two-input NAND gate.

Efficiency Parameters

- **Area:** Technology-independent area based on a unit called *gate equivalent* (GE) which corresponds to a two-input NAND gate.
- **Throughput:** Rate of a new ciphertext produced over time that is expressed in bits-per-second.

Efficiency Parameters

- **Area:** Technology-independent area based on a unit called *gate equivalent* (GE) which corresponds to a two-input NAND gate.
- **Throughput:** Rate of a new ciphertext produced over time that is expressed in bits-per-second.
- **Latency:** Delay time between an initial request of the encryption of a plaintext and producing a corresponding ciphertext. The latency is expressed by the clock cycles of the overhead. [Knezevic, et.al 2012][Borghoff, et.al 2012]

Efficiency Parameters

- **Area:** Technology-independent area based on a unit called *gate equivalent* (GE) which corresponds to a two-input NAND gate.
- **Throughput:** Rate of a new ciphertext produced over time that is expressed in bits-per-second.
- **Latency:** Delay time between an initial request of the encryption of a plaintext and producing a corresponding ciphertext. The latency is expressed by the clock cycles of the overhead. [Knezevic, et.al 2012][Borghoff, et.al 2012]
- **Power Consumption:** Either rely on a strictly limited battery or they utilize an external electromagnetic field without an internal power source which makes low power consumption highly desirable.

Popular Design Approaches

- **Non-linear layer:**

Popular Design Approaches

- **Non-linear layer:**
  - Identical S-boxes

Popular Design Approaches

- **Non-linear layer:**
  - Identical S-boxes
  - 4-bit bijective S-boxes [PRESENT]

Popular Design Approaches

- **Non-linear layer:**
  - Identical S-boxes
  - 4-bit bijective S-boxes [PRESENT]
- **Key Schedule:** mostly linear key-schedules, or even without key schedules

Popular Design Approaches

- **Non-linear layer:**
  - Identical S-boxes
  - 4-bit bijective S-boxes [PRESENT]
- **Key Schedule:** mostly linear key-schedules, or even without key schedules
  - Related-key setting is entirely alien

Popular Design Approaches

- **Non-linear layer:**
  - Identical S-boxes
  - 4-bit bijective S-boxes [PRESENT]
- **Key Schedule:** mostly linear key-schedules, or even without key schedules
  - Related-key setting is entirely alien
  - self-similarity cryptanalysis can be prevented by simple operations like round-dependent constants

Popular Design Approaches

- **Non-linear layer:**
  - Identical S-boxes
  - 4-bit bijective S-boxes [PRESENT]
- **Key Schedule:** mostly linear key-schedules, or even without key schedules
  - Related-key setting is entirely alien
  - self-similarity cryptanalysis can be prevented by simple operations like round-dependent constants
    - Probabilistic self-similarity cryptanalysis: Reflection on PRINCE [FSE 2013] and ITUbee, Slide cryptanalysis on EM structure [FSE 2014].

Popular Design Approaches

- **Non-linear layer:**
  - Identical S-boxes
  - 4-bit bijective S-boxes [PRESENT]
- **Key Schedule:** mostly linear key-schedules, or even without key schedules
  - Related-key setting is entirely alien
  - self-similarity cryptanalysis can be prevented by simple operations like round-dependent constants
    - Probabilistic self-similarity cryptanalysis: Reflection on PRINCE [FSE 2013] and ITUbee, Slide cryptanalysis on EM structure [FSE 2014].
- **Linear Layer:**

Popular Design Approaches

- **Non-linear layer:**
  - Identical S-boxes
  - 4-bit bijective S-boxes [PRESENT]
- **Key Schedule:** mostly linear key-schedules, or even without key schedules
  - Related-key setting is entirely alien
  - self-similarity cryptanalysis can be prevented by simple operations like round-dependent constants
    - Probabilistic self-similarity cryptanalysis: Reflection on PRINCE [FSE 2013] and ITUbee, Slide cryptanalysis on EM structure [FSE 2014].
- **Linear Layer:**
  - Bit permutation instead of MDS matrices.

Popular Design Approaches

- **Non-linear layer:**
  - Identical S-boxes
  - 4-bit bijective S-boxes [PRESENT]
- **Key Schedule:** mostly linear key-schedules, or even without key schedules
  - Related-key setting is entirely alien
  - self-similarity cryptanalysis can be prevented by simple operations like round-dependent constants
    - Probabilistic self-similarity cryptanalysis: Reflection on PRINCE [FSE 2013] and ITUbee, Slide cryptanalysis on EM structure [FSE 2014].
- **Linear Layer:**
  - Bit permutation instead of MDS matrices.
  - MDS matrices produced by iterating the multiplication of one light matrix [Guo et.al. 2011]

Security Goals

- **Moderate Security:** 64-bit block, 80-bit key
  - Unlikely to require encryption of a large amount of data.
  - The value of the data.
  - Keeping the information secret forever is not required
- **Side Channel:**
  - It is challenging for low-resource applications.
  - Zorro: consists of AES operations, uses only partial non-linear layers.
  - LS block ciphers use look-up tables for the linear layer and implements S-boxes by logical operations

Key Scheduling

- Several design criteria have been presented to provide security against known cryptanalysis –> wide-trail strategy
- A properly designed key schedule is still out of reach [Jean, et.al 2014][Huang et.al 2014]
- Even more critical when it comes to authenticated encryption via tweakable block ciphers
- Several CAESAR candidates make use of tweakable block ciphers (e.g. Deoxys, SCREAM, Joltik, KIASU, Silver).
- Also important for side-channel attacks since key scheduling can be an easy target for Simple Power Analysis [Mangard 2002][Veyrat-Charvillon, et.al. 2014]

Future Work

- Design a (lightweight) block cipher by considering side-channel attacks.
- Connection between classical and side-channel
- Impact of the key scheduling algorithms on the security of primitives against both mathematical and side-channel attacks.
- How well a related-key distinguishers can lead to serious vulnerabilities in practice?

Questions?