Introduction to Cryptology

4.1 - Block Ciphers

Federico Pintore

Mathematical Institute, University of Oxford (UK)

UNIVERSITY OF OXFORD

Michaelmas term 2020

Block Ciphers

Block ciphers are designed to be concrete instantiations of (strong) pseudorandom permutations.

Block Ciphers

Block ciphers are designed to be concrete instantiations of (strong) pseudorandom permutations.

A block cipher is a keyed map $F : \{0,1\}^n \times \{0,1\}^\ell \to \{0,1\}^\ell$ s.t.

- $F_k : \{0,1\}^\ell \to \{0,1\}^\ell$, $x \mapsto F(k,x)$ is a permutation for all $k \in \{0,1\}^n$;
- F_k and F_k^{-1} are efficiently computable for all $k \in \{0,1\}^n$.

Naming: n is the key length, ℓ is the block length.

Concrete security of Block Ciphers

Let Perm_ℓ be the set of all permutations of $\{0,1\}^\ell$, and consider a block cipher $F : \{0,1\}^k \times \{0,1\}^\ell \to \{0,1\}^\ell$.

Concrete security of Block Ciphers

Let Perm_ℓ be the set of all permutations of $\{0,1\}^\ell$, and consider a block cipher $F : \{0,1\}^k \times \{0,1\}^\ell \to \{0,1\}^\ell$.

For a PPT distinguisher D, we define their advantage as

$$\mathrm{Adv}^{PRP}_{F,\mathrm{D}} = |\,\Pr(\mathrm{D}^{f()} = 1) - \Pr(\mathrm{D}^{F_k()} = 1)|$$

where the first probability is taken over a uniform choice of f in Perm_ℓ and the randomness of D, the second one over a uniform choice of k in $\{0,1\}^n$ and the randomness of D.

Concrete security of Block Ciphers

For any integers t and q, we define

$$\mathrm{Adv}_F^{PRP}(t,q) = \max_{\mathrm{D}}\{\mathrm{Adv}_{F,\mathrm{D}}^{PRP}\}$$

where the maximum is over all distinguishers D with time complexity at most t and making at most q queries.

Concrete security of Block Ciphers

For any integers t and q, we define

$$\mathrm{Adv}_F^{PRP}(t,q) = \max_{\mathrm{D}}\{\mathrm{Adv}_{F,\mathrm{D}}^{PRP}\}$$

where the maximum is over all distinguishers D with time complexity at most t and making at most q queries.

The terminology "F is a secure block cipher" indicates that $\mathrm{Adv}_F^{PRP}(t,q)$ is *low* for *reasonable* values of t and q.

Concrete security of Block Ciphers

For any integers t and q, we define

$$\mathrm{Adv}_F^{PRP}(t, q) = \max_{\mathrm{D}}\{\mathrm{Adv}_{F,\mathrm{D}}^{PRP}\}$$

where the maximum is over all distinguishers D with time complexity at most t and making at most q queries.

The terminology "F is a secure block cipher" indicates that $\mathrm{Adv}_F^{PRP}(t, q)$ is *low* for *reasonable* values of t and q.

Currently, a block cipher is considered secure if the best known attack has time complexity approximately equal to a brute-force attack to recover the key.

Constructing Block Ciphers

The permutations of a block cipher must:

- behave like random permutations;
- have a concise representation.

Constructing Block Ciphers

The permutations of a block cipher must:

- behave like random permutations;
- have a concise representation.

Representing an arbitrary permutation of $\{0,1\}^\ell$ needs $\ell \cdot 2^\ell$ bits (infeasible for $\ell > 50$; for modern block ciphers $\ell \geq 128$).

Confusion-Diffusion Paradigm

Confusion: use random-looking permutations f_i with smaller block length (e.g. 8 bits) than F_k to construct F_k.

Confusion-Diffusion Paradigm

Confusion: use random-looking permutations f_i with smaller block length (e.g. 8 bits) than F_k to construct F_k.

- Example: given x $\in \{0,1\}^{128}$, split it into 16 bytes $x_1, \cdots, x_{16}$ and define

$$F_k(x) = f_1(x_1) || \cdots || f_{16}(x_{16}).$$

- $F_k(x)$ and $F_k(x')$ have only one different byte if $w(x, x') = 1$.

Confusion-Diffusion Paradigm

Confusion: use random-looking permutations f_i with smaller block length (e.g. 8 bits) than F_k to construct F_k.

- Example: given $\mathrm{x} \in \{0,1\}^{128}$, split it into 16 bytes $x_1, \cdots, x_{16}$ and define

$$F_k(x) = f_1(x_1)||\cdots||f_{16}(x_{16}).$$

- $F_k(x)$ and $F_k(x')$ have only one different byte if $w(x, x') = 1$.

Diffusion: use a mixing permutation to make a change in one bit affect the entire output!

Confusion-Diffusion Paradigm

Each function f_i is called round function.

The confusion-diffusion steps together are called round.

Substitution-permutation Networks (SPNs)

A substitution-permutation network is an implementation of the confusion-diffusion paradigm.

- Using a fixed public algorithm called key schedule, sub-keys $k_1, \ldots, k_{r+1}$ are derived from the key k.
- Different permutations $\{S_i\}$ with small block length are used to define the round functions:

$$f_i(x_i) = S_i(x_i \oplus k_{j,i})$$

  where $k_{j,i}$ denotes the i-th *chunk* of the sub-key k_j.
- S_i is called S-box

Key Schedule: a simple example

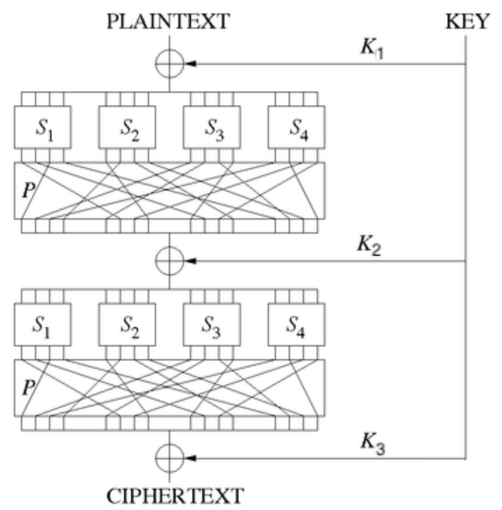
Let the key k be as follows:

$$k = 1110\ 0111\ 0110\ 0111\ 1001\ 0000\ 0011\ 1101.$$

Define k_i as the 16 consecutive bits of k starting at bit $4i - 3$:

- $k_1 = 1110\ 0111\ 0110\ 0111$
- $k_2 = 0111\ 0110\ 0111\ 1001$
- $k_3 = 0110\ 0111\ 1001\ 0000$
- $k_4 = 0111\ 1001\ 0000\ 0011$
- $k_5 = 1001\ 0000\ 0011\ 1101$

SPN - Example



Input : m, S-boxes,

mixing permutation P,

$(k_1, \ldots, k_{r+1})$.

Output : c.

state $= m$

for $j = 1, \ldots, r$;

state $=$ state $\oplus\ k_j$ (key-mixing)

apply S-boxes to the t sub-strings..

..of state (substitution)

apply P to state (permutation)

$c =$ state $\oplus\ k_{r+1}$

SPNs - Avalanche effect

Some design principles are followed when constructing a SPN:

SPNs - Avalanche effect

Some design principles are followed when constructing a SPN:

S-boxes: a change of one bit in the input determines a change of at least two bits in the output.

SPNs - Avalanche effect

Some design principles are followed when constructing a SPN:

S-boxes: a change of one bit in the input determines a change of at least two bits in the output.

mixing permutation P: the bits of the output of one S-box are fed to multiple S-boxes in the next round.

SPNs - Miscellaneous

- The Advanced Encryption Standard (AES) has a similar structure (will see it soon).
- The security of a SPN depends on the number of rounds.
  - for a SPN with a single round with no key mixing as final step, it is easy to recover the key k;
  - a one round SPN is also not secure;
  - same for a two round SPN.

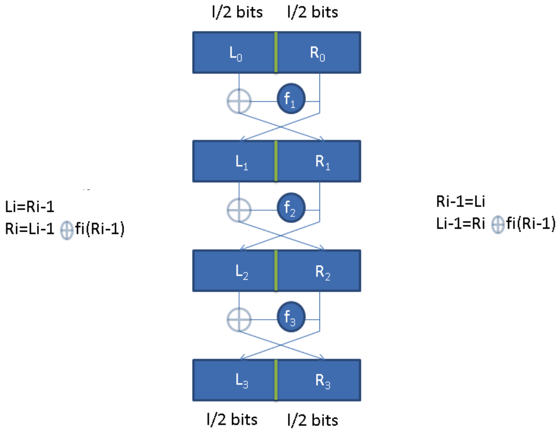
Feistel Networks

Different approach to construct block ciphers following the confusion-diffusion paradigm.

Advantage over SPNs: the round functions do not need to be permutations.

For a permutation $F_k : \{0,1\}^\ell \to \{0,1\}^\ell$, r key-dependent round functions $f_1, \cdots, f_r$, where $f_i : \{0,1\}^{\ell/2} \to \{0,1\}^{\ell/2}$, are used.

Feistel Networks - An example



Attacks on Block Ciphers

Linear Attacks

Exploit linear combinations of input, output and key bits.

- The linearity here refers to $\oplus$ (the mod 2 bit-wise sum).
- Goal: collect combinations whose probabilities of holding[1] (linear probability biases) are as close to 0 or 1 as possible.
- The relations are used in conjunction with known input-output pairs to recover the key.

[1] Over the space of all possible values of their variables.

Differential Attacks

Exploit relationship between $\Delta X = X_1 \oplus X_2$ and $\Delta Y = Y_1 \oplus Y_2$ for pairs of inputs (X_1, X_2) and corresponding outputs (Y_1, Y_2).

- Ideally, $P_{d_1,d_2} = \Pr(\Delta Y = d_2 | \Delta X = d_1) = 1/2^\ell$, for every d_1, d_2.
- Pairs (d_1, d_2) s.t. $P_{d_1,d_2} \gg 1/2^\ell$ are collected.
- It is a chosen plaintext attack, so an attacker aims at encrypting pairs (X_{i_1}, X_{i_2}) for which they know that a certain ΔY_i occurs with high probability.

Quantum attacks

Search problem: given $A \subset X$ and $f : X \to \{0, 1\}$ s.t. $f(x) = 1$ iff $x \in A$, find A having oracle accesso to f.

Quantum attacks

Search problem: given $A \subset X$ and $f : X \to \{0, 1\}$ s.t. $f(x) = 1$ iff $x \in A$, find A having oracle accesso to f.

- Classical computers: the best known algorithm runs in time $\mathcal{O}(|X|)$.

Quantum attacks

Search problem: given $A \subset X$ and $f : X \to \{0,1\}$ s.t. $f(x) = 1$ iff $x \in A$, find A having oracle accesso to f.

- Classical computers: the best known algorithm runs in time $\mathcal{O}(|X|)$.
- Quantum computers: according to [Grover'96], the runnning time is $\mathcal{O}\left(\sqrt{|X|}\right)$ (quadratic speedup).

Quantum attacks

Search problem: given $A \subset X$ and $f : X \to \{0,1\}$ s.t. $f(x) = 1$ iff $x \in A$, find A having oracle accesso to f.

- Classical computers: the best known algorithm runs in time $\mathcal{O}(|X|)$.
- Quantum computers: according to [Grover'96], the runnning time is $\mathcal{O}\left(\sqrt{|X|}\right)$ (quadratic speedup).
- Given input-output pairs (m_i, c_i), $i = 1, \ldots, t$, define $f(k) = 1$ if $F_k(m_i) = c_i \ \forall i$, and 0 otherwise.

Quantum attacks

Search problem: given $A \subset X$ and $f : X \to \{0, 1\}$ s.t. $f(x) = 1$ iff $x \in A$, find A having oracle accesso to f.

- Classical computers: the best known algorithm runs in time $\mathcal{O}(|X|)$.
- Quantum computers: according to [Grover'96], the runnning time is $\mathcal{O}\left(\sqrt{|X|}\right)$ (quadratic speedup).
- Given input-output pairs (m_i, c_i), $i = 1, \ldots, t$, define $f(k) = 1$ if $F_k(m_i) = c_i\ \forall i$, and 0 otherwise.

Key length should be doubled
to protect against quantum attacks.

Further Reading I

- Nadhem J AlFardan, Daniel J Bernstein, Kenneth G Paterson, Bertram Poettering, and Jacob CN Schuldt.
  On the security of RC4 in TLS.
  In 22nd USENIX Security Symposium (USENIX Security 13), pages 305–320, 2013.

- Boaz Barak and Shai Halevi.
  A model and architecture for pseudo-random generation with applications to/dev/random.
  In Proceedings of the 12th ACM conference on Computer and communications security, pages 203–212. ACM, 2005.

- Mihir Bellare, Anand Desai, Eron Jokipii, and Phillip Rogaway.
  A concrete security treatment of symmetric encryption.
  In Proceedings 38th Annual Symposium on Foundations of Computer Science, 1997, pages 394–403, 1997.

Further Reading II

Daniel J Bernstein.
The Salsa20 Family of Stream Ciphers.
In New stream cipher designs, pages 84–97. Springer, 2008.

Lenore Blum, Manuel Blum, and Mike Shub.
A simple unpredictable pseudo-random number generator.
SIAM Journal on computing, 15(2):364–383, 1986.

Christian Cachin.
Entropy measures and unconditional security in cryptography.
PhD thesis, ETH Zurich, 1997.

Scott Fluhrer, Itsik Mantin, and Adi Shamir.
Weaknesses in the key scheduling algorithm of RC4.
In Selected areas in cryptography, pages 1–24. Springer, 2001.

Further Reading III

- Christina Garman, Kenneth G Paterson, and Thyla Van der Merwe.
  Attacks only get better: Password recovery attacks against RC4 in TLS.
  In 24th USENIX Security Symposium (USENIX Security 15), pages 113–128, 2015.
- Itsik Mantin and Adi Shamir.
  A practical attack on broadcast RC4.
  In Fast Software Encryption, pages 152–164. Springer, 2002.