Applied Cryptography

thgoebel@ethz.ch

ETH Zürich, FS 2021

This documents is a **short** summary for the course *Applied Cryptography* at ETH Zurich. It is intended as a document for quick lookup, e.g. during revision, and as such does not replace reading the slides or a proper book.

We do not guarantee correctness or completeness, nor is this document endorsed by the lecturers. Feel free to point out any erratas.

Contents

List of Figures

1 Symmetric Cryptography

One-time pad Plaintext p, key k such that $|p| = |k|$. Ciphertext $c = p \oplus k$.

If k u.a.r. and only used once then the OTP is **perfectly secure**, i.e. $\Pr[P = p|C = c] = \Pr[P = p]$.

Note: keys can re-occur (as a result of random sampling) but they must not be re-used (i.e. the adversary must not be aware that the same key is used).

Issues: same lengths, key distribution, single use.

1.1 Block Ciphers

Block cipher A block cipher with key length k and block size n consists of two efficiently computable permutations[1]:

$$E : \{0,1\}^k \times \{0,1\}^n \mapsto \{0,1\}^n \quad D : \{0,1\}^k \times \{0,1\}^n \mapsto \{0,1\}^n$$

such that for all keys K D_K is the inverse of E_K (where we write E_K short for $E(K, \cdot)$).

Security notions Known plaintext attack, chosen plaintext attack, chosen ciphertext attack. Exhaustive key search on (P, C) pairs – no attack should be better, else we throw the cipher away.

Pseudo-randomness

- Adversary $\mathcal{A}$ interacts either with block cipher (E_K, D_K) or a truly random permutation (Π, Π^{-1}).
- A block cipher is called a **pseudo-random permutation PRP** if no efficient[2] $\mathcal{A}$ can tell the difference between E_K and Π (no access to the inverse).
- A block cipher is called a **strong-PRP** if no efficient $\mathcal{A}$ can tell the difference between (E_K, D_K) and (Π, Π^{-1}).

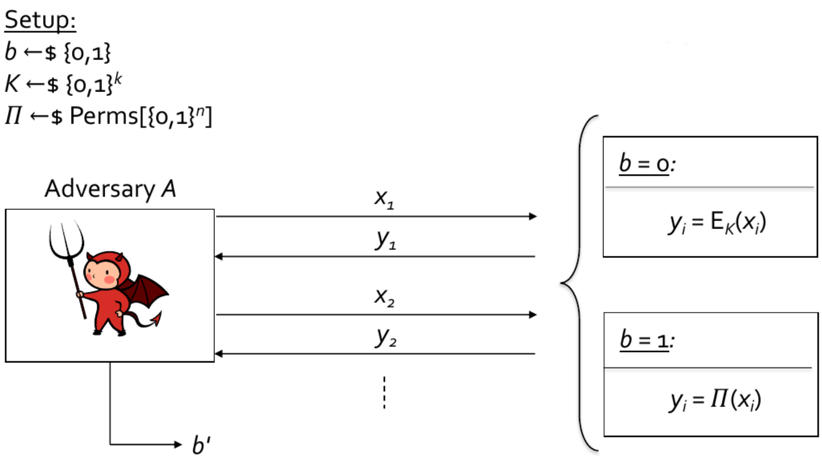

Figure 1: PRP game

[1]Encipher and decipher

[2]Quantified by runtime + number of oracle queries.

The advantage is defined as:

$$\mathbf{Adv}_E^{PRP}(\mathcal{A}) = 2 \cdot \left| \Pr[\text{Game } \mathbf{PRP}(\mathcal{A}, E) \Rightarrow \text{true}] - \frac{1}{2} \right|$$

where the probability is over the randomness of $b, K, \Pi, \mathcal{A}$. Note that $\Pr[\text{Game } \mathbf{PRP}(\mathcal{A}, E) \Rightarrow \text{true}] = \Pr[b' = b]$.

Constructing block ciphers In general: keyed round function that is repeated many times.

- Feistel cipher: halved blocks crossing back and forth, e.g. DES
- Substitution-permutation network: confusion + diffusion, e.g. AES

Electronic Code Book (ECB) mode Same plaintext always maps to the same ciphertext (deterministic). Thus serious leakage, don't use.

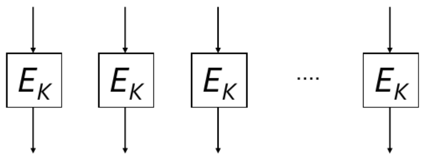

Figure 2: ECB mode

Cipher Block Chaining (CBC) mode Use u.a.r. IV/previous ciphertext block to randomise encryption.

A bit flip in C_i completely scrambles/randomises P_i and flips the same bit in P_{i+1}.

Caveats: non-random IV, padding oracle attack, ciphertext block collisions (after using the same key for $2^{n/2}$ blocks by the birthday bound).

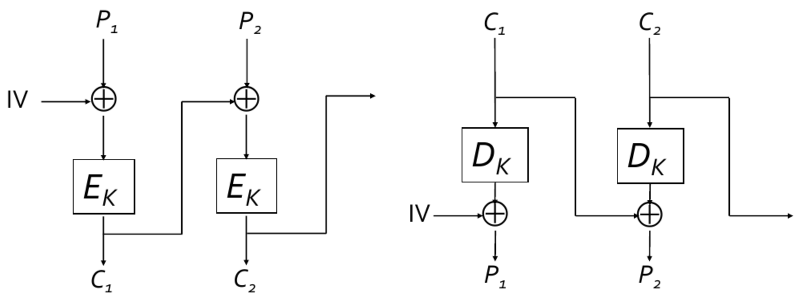

Figure 3: CBC mode (left: encipher, right: decipher)

Counter (CTR) mode Incrementing counter is encrypted with block cipher to produce a pseudo-random value to xor the plaintext block with.

Effectively a stream cipher producing OTP keys. E_K does not even need to be invertible. No padding needed, can just truncate the last block. A bit flip it C_i flips the same bit in P_i.

Caveats: counter must not repeat/wrap around (else xor of ciphertexts = xor of plaintexts).

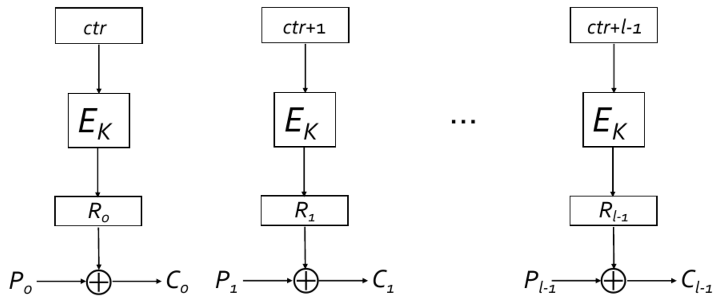

Figure 4: CTR mode

1.2 Symmetric Encryption

Symmetric Encryption Scheme is a triple $SE = (KGen, Enc, Dec)$. We have key space $\mathcal{K} = \{0,1\}^k$, message space $\mathcal{M} = \{0,1\}^{*}$[3] and ciphertext space $\mathcal{C} = \{0,1\}^*$. For correctness, we have $Dec_K(Enc_K(m)) = m$.

IND-CPA Security Informally: computational version of perfect security – an efficient adversary cannot compute anything useful from a ciphertext (e.g. hide every bit of the plaintext. Equivalent to *semantic security*.

Formally: For any efficient adversary $\mathcal{A}$, given the encryption of one of two equal-length messages of its choice, $\mathcal{A}$ is unable to distinguish which one of the two messages was encrypted.

In the security game, $\mathcal{A}$ gets access to a *Left-or-Right encryption oracle*. The advantage of $\mathcal{A}$ is:

$$\mathbf{Adv}_{SE}^{IND-CPA}(\mathcal{A}) = 2 \cdot \left| \Pr[\text{Game } \mathbf{IND\text{-}CPA}(\mathcal{A}, SE) \Rightarrow \text{true}] - \frac{1}{2} \right|$$

Notes: Deterministic schemes **cannot** be IND-CPA secure (why?). CBC and CTR mode (if used properly) can be proven to be IND-CPA secure (assuming that Enc is a PRP-secure block cipher).

Caveats: No integrity. Says nothing about messages of non-equal length. No chosen ciphertexts.

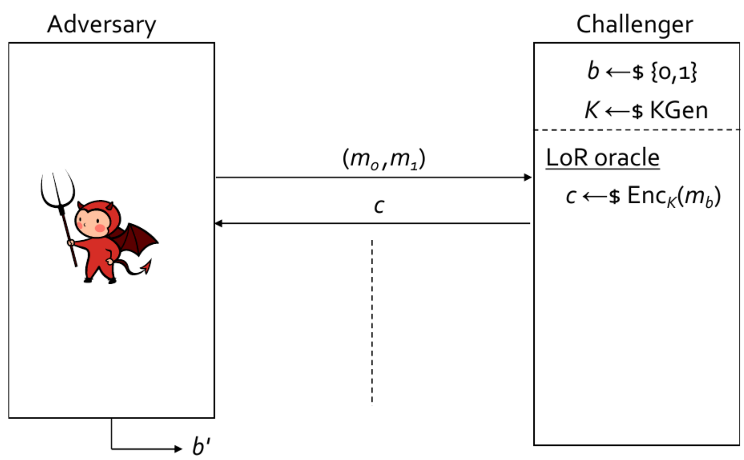

Figure 5: IND-CPA game

[3] In reality we might have a maximum plaintext length.

Advantage Rewriting Lemma Let b be a uniformly random bit and b' the output of some algorithm. Then:

$$2\left|\Pr[b' = b] - \frac{1}{2}\right| = \left|\Pr[b' = 1|b = 1] - \Pr[b' = 1|b = 0]\right|$$

Difference Lemma Let Z, W_1, W_2 be events. If

$$(W_1 \wedge \neg Z) \text{ occurs if and only if } (W_2 \wedge \neg Z) \text{ occurs}$$

then

$$\left|\Pr[W_2] - \Pr[W_1]\right| \leq \Pr[Z]$$

In practice: Z is a bad event that rarely happens, W_1, W_2 are when $\mathcal{A}$ wins in security games G_1, G_2. Useful for *game hopping* proofs.

PRP-PRF Switching Lemma Let E be a block cipher. Then for any algorithm $\mathcal{A}$ making q queries:

$$\left|\mathbf{Adv}_E^{PRP}(\mathcal{A}) - \mathbf{Adv}_E^{PRF}(\mathcal{A})\right| \leq \frac{q^2}{2^{n+1}}$$

1.3 Hash Functions

1.4 Message Authentication Codes MACs

1.5 Authenticated Encryption