Cryptography

Corso di Laurea Magistrale in Informatica

Perfectly-Secret Encryption

Ugo Dal Lago

Academic Year 2023-2024

Perfectly-Secret Encryption

- In this part of the course we will study **a first way** to formalize the concept of security (perfect-secrecy) for an encryption scheme.
- We will show that, even if it is very strong, such a notion of security is indeed **implementable**.
- However, we will show that perfect secrecy suffers from some very strict **limitations**.
  - For this reason, although it was introduced and studied well before the Seventies, it never caught on, with the exception of very specific contexts

Let Us Set the Scene

- The definition of encryption scheme is the one we have already seen, namely a triple of algorithms (Gen, Enc, Dec).
- In the context of perfect-secrecy, Enc may be probabilistic, Dec remains deterministic, while there is no other limitation on the algorithms involved.
- In perfect-secrecy, the choice of the message and of the key, the encryption and decryption are seen as a a *probabilistic process*. In this way we can define three random variables:
  1. First of all $\mathbf{K}$, that corresponds to the key used, and that depends on the algorithm Gen
  2. Then $\mathbf{M}$, that corresponds to the message produced by the sender.
  3. Finally $\mathbf{C}$, which corresponds to the ciphertext, and thus depends on $\mathbf{K}$, $\mathbf{M}$ and Enc.
- We can then calculate quantities such as $Pr(\mathbf{K} = k)$ where $k \in \mathcal{K}$ is a key, or $Pr(\mathbf{K} = k \mid \mathbf{M} = m)$, where $m \in \mathcal{M}$.

The Definition

- The key and message are *always* considered to be **independently** chosen.
- What about the variables $\mathbf{M}$ and $\mathbf{C}$ instead? Of course, the value of the latter depends on the former, but how?
- We would like to catch the point that knowing the value of $\mathbf{C}$ does not change our knowledge of $\mathbf{M}$.

The Definition

- The key and message are *always* considered to be **independently** chosen.
- What about the variables $\mathbf{M}$ and $\mathbf{C}$ instead? Of course, the value of the latter depends on the former, but how?
- We would like to catch the point that knowing the value of $\mathbf{C}$ does not change our knowledge of $\mathbf{M}$.

Definition (Perfect Secrecy)

An encryption scheme (Gen, Enc, Dec) is **perfectly secret** if for every message $m \in \mathcal{M}$ and every ciphertext $c \in \mathcal{C}$ for which $Pr(\mathbf{C} = c) > 0$ we have that $Pr(\mathbf{M} = m \mid \mathbf{C} = c) = Pr(\mathbf{M} = m)$.

A Couple of Characterizations

Lemma

An encryption scheme (Gen, Enc, Dec) *is perfectly secret if and only if for every message* $m \in \mathcal{M}$ *and for every ciphertext* $c \in \mathcal{C}$ *we have that* $Pr(\mathbf{C} = c \mid \mathbf{M} = m) = Pr(\mathbf{C} = c)$*.*

Lemma

An encryption scheme (Gen, Enc, dec) *is perfectly secret if and only if for every messages* $m_0, m_1 \in \mathcal{M}$ *and for every* $c \in \mathcal{C}$ *we have that* $Pr(\mathbf{C} = c \mid \mathbf{M} = m_0) = Pr(\mathbf{C} = c \mid \mathbf{M} = m_1)$*.*

Vernam's cipher

- Is it possible to construct a concrete cipher that is perfectly secret?
- The answer is undoubtedly yes: we can consider the Vernam's cipher (also known as the One-Time Pad):

$$\mathcal{K} = \mathcal{M} = \mathcal{C} = \{0,1\}^n \qquad Pr(\mathbf{K} = k) = \frac{1}{2^n}$$

$$Enc(m,k) = m \oplus k \qquad Dec(c,k) = c \oplus k$$

- The cipher is undoubtedly correct

$$Dec(Enc(m,k),k) = (m \oplus k) \oplus k = m \oplus (k \oplus k) = m \oplus 0^n = m$$

Theorem

The Vernam's cipher is perfectly-secret.

- Let's observe how messages and keys have *the same* length, a very strong limitation.

A General Limitation?

- We could wonder if the aforementioned limitations are specific to Vernam's cipher or are inherent to any scheme achieving perfect secrecy

Theorem

Let (Gen, Enc, Dec) be a perfectly secret encryption scheme over a message space $\mathcal{M}$ and a key space $\mathcal{K}$. Then $|\mathcal{K}| \geq |\mathcal{M}|$.

- It is therefore the notion of perfect security that has strong limitations.
- However, the use of Vernam's cipher makes sense, *in case of* extreme security needs
  - A typical example is the so-called *'Moscow-Washington hotline"*.

A Third Characterization — Indistinguishability

- A further characterization is obtained by considering the experiment $\mathsf{PrivK}^{eav}_{A,\Pi}$, i.e., a kind of "game" in which a hypothetical aversary A and a scheme $\Pi = (Gen, Enc, Dec)$ are pitted against each other:

  $\mathsf{PrivK}^{eav}_{A,\Pi}$
  $(m_0, m_1) \leftarrow A;$
  $k \leftarrow Gen;$
  $b \leftarrow \{0, 1\};$
  $c \leftarrow Enc(k, m_b);$
  $b^* \leftarrow A(c);$
  Result: $\neg(b \oplus b^*)$

- The experiment adds another level of probability and is therefore a random variable.
- We could ask ourselves, for example, what is the probability that the experiment has a positive outcome for the adversary with maximal probability, i.e:

$$Pr(\mathsf{PrivK}^{eav}_{A,\Pi} = 1)$$

A Third Characterization — Indistinguishability

- Does it make sense to require that $Pr(\mathsf{PrivK}^{eav}_{A,\Pi} = 1) = 0$?

A Third Characterization — Indistinguishability

- Does it make sense to require that $Pr(\mathsf{PrivK}^{eav}_{A,\Pi} = 1) = 0$?
- Actually it does not!

A Third Characterization — Indistinguishability

- Does it make sense to require that $Pr(\mathsf{PrivK}^{eav}_{A,\Pi} = 1) = 0$?
- Actually it does not!

Definition

An encryption scheme $\Pi = (Gen, Enc, Dec)$ has *indistinguishable encryptions* iff for every adversary A we have that

$$Pr(\mathsf{PrivK}^{eav}_{A,\Pi} = 1) = \frac{1}{2}$$

A Third Characterization — Indistinguishability

- Does it make sense to require that $Pr(\mathsf{PrivK}^{eav}_{A,\Pi} = 1) = 0$?
- Actually it does not!

Definition

An encryption scheme $\Pi = (Gen, Enc, Dec)$ has *indistinguishable encryptions* iff for every adversary A we have that

$$Pr(\mathsf{PrivK}^{eav}_{A,\Pi} = 1) = \frac{1}{2}$$

Theorem

Π *is perfectly sercret iff* Π *has indistinguishable encryptions.*

- The notions of experiment and of indistinguishable encryptions will be fundamental in this course.