1. Public key Encryption

Public key encryption

Key exchange task

Alice and Bob want to generate a shared key k_{ab} without a central trusted party

Eavesdropper Eve that listen to the conversation must be unable to find the shared key

Trapdoor function

- G - key generation algoritm - *probabilistic* - $(k_{pub}, k_{priv}) \overset{R}{=} G()$
- $F : \mathcal{X} \rightarrow \mathcal{Y}$ - a function - *deterministic* - $y{=}F(k_{pub}, x)$
- $I : \mathcal{Y} \rightarrow \mathcal{X}$ - Inverse trapdoor - *deterministic* - $x{=}I(k_{priv}, y)$
- F is one way -> given y you can't find x without knowing I

Corectness property
$Pr[\ I(k_{priv},\ (F(k_{pub},\ x))) = x] = 1$

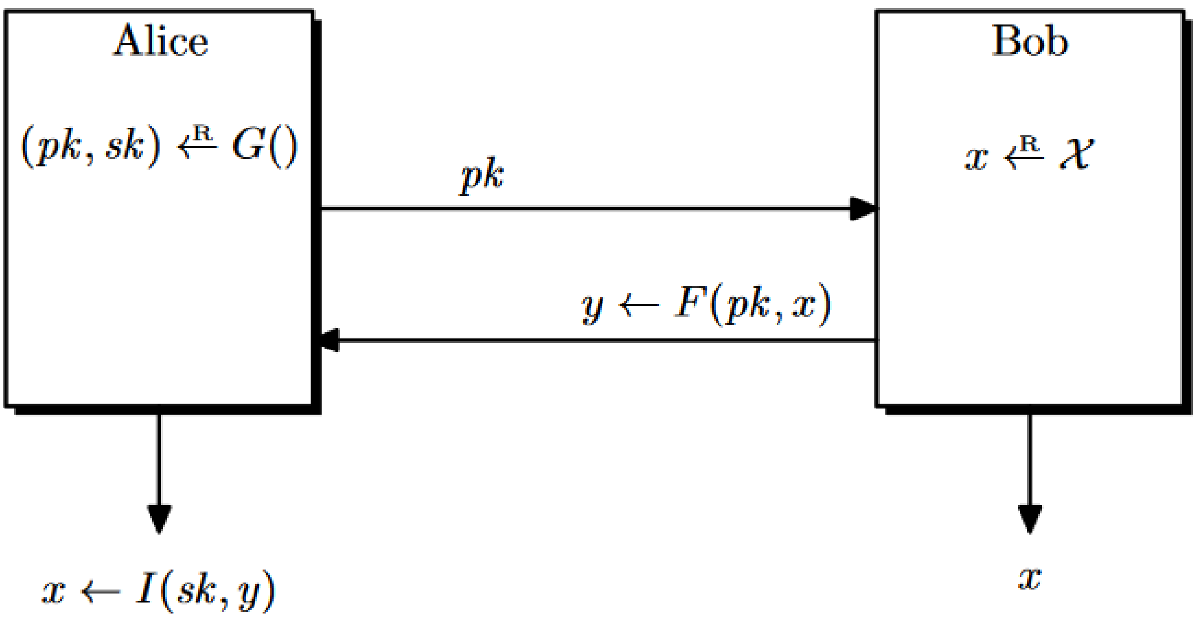


Figure 10.1: Key exchange using a trapdoor function scheme

Public key algorithm

A **public key encryption scheme** is a triple of algorithms (G, E, D)

- G - key generation algoritm - *probabilistic* - $(k_{pub}, k_{priv}) \stackrel{R}{=} G()$
- E - Encryption algoritm - *probabilistic* - $c \stackrel{R}{=} E(k_{pub}, m)$
- D - Decryption algoritm - *deterministic* - $y{=}D(k_{priv}, c)$

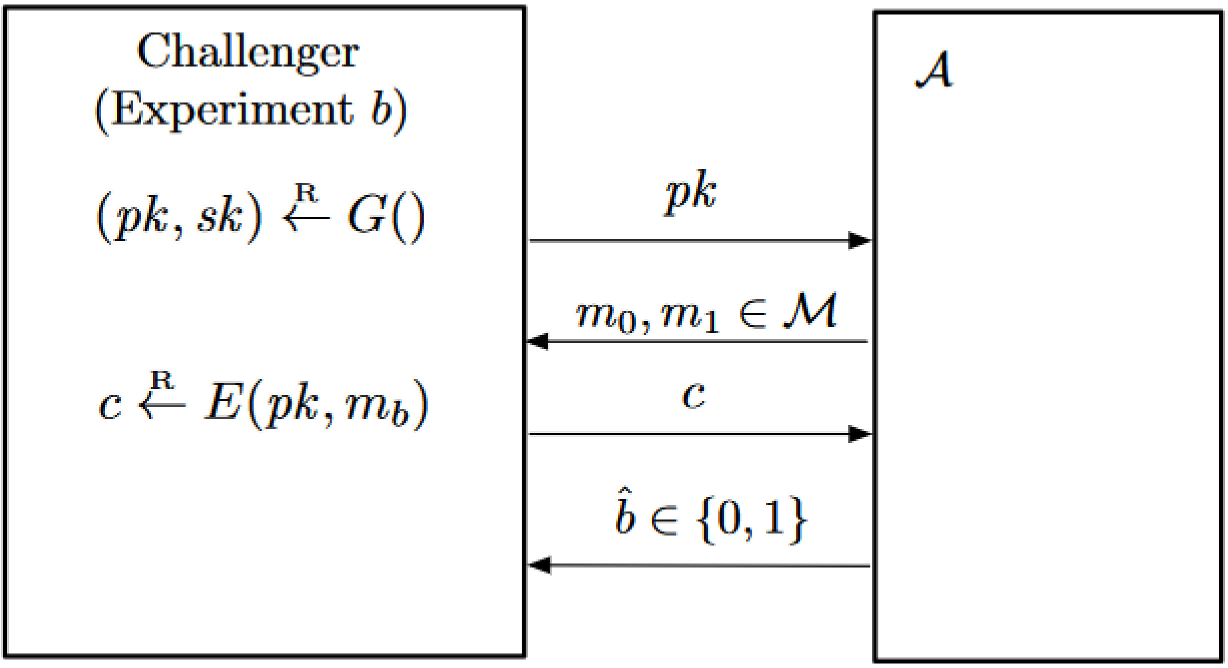
Corectness property
$Pr[\ D(k_{priv},\ (E(k_{pub},\ m))) = m] = 1$

Security

Semantic security

For (G, E, D)

- The challenger computes $(k_{pub}, k_{priv}) \stackrel{R}{=} G()$, and sends k_{pub} to the adversary.
- The adversary computes $m_0, m_1 \in \mathcal{M}$, of the same length, and sends them to the challenger.
- The challenger chooses one of the messages m_0, m_1 and computes $c \stackrel{R}{=} E(k_{pub}, m_b)$, and sends c to the adversary.
- The adversary must find out which message was encrypted



> (G, E, D) is secure if all efficient adversaries have neglijable advantage

Intuition

- The attacker can't distinguish the encryption of a message from random

CPA security

There is not CPA since there is a public key therefore the attacker can encrypt messages at his will

Note

- One type security(Semantic) $\Rightarrow$ Many time security(CPA)

- (Deterministic encryption) If E is not randomized then the attacker can compute the $c_0 = E(k_{pub}, m_0)$ and can compare it with what he gets back. If he gets the encryption of m_0 then he knows what message was encrypted

CCA security

For (G, E, D)

- The challenger computes $(k_{pub}, k_{priv}) \stackrel{R}{=} G()$, and sends k_{pub} to the adversary.
- The Attacker can make
  - *encryption queries*: Send pair of messages and get encryption of one of them at random
  - *decryption queries*: Decrypt ciphertexts not found in the previous encryption queries
- The attacker mustn't be able to distinguish what message was encrypted from a pair of messages

> (G, E, D) is secure against CCA if for all efficient adversaries their advantage is neglijable

- https://en.wikipedia.org/wiki/Malleability_(cryptography)

Resources

- https://en.wikipedia.org/wiki/Public-key_cryptography