Introduction to Provable Security

Hao Chung (鍾豪)
National Taiwan University
October 31, 2017

Quantum Cryptography

Outline

① Concepts of Security Definition

② DDH problem and El Gamal

③ Security Proof of El Gamal

Questions

What do we mean by “an encryption is secure?”

How about key agreement?

How we define security? How we prove it?

Security Proof

What constitutes a security proof?

Formal Definition **Precise Assumptions** **Proof of Security**

Formal Definition

Intuitively, a security definition is the security that you want to achieve.

In general, a security definition has two components: a security guarantee and a threat model.

For example, how do you define the security for ``bicycle lock?”

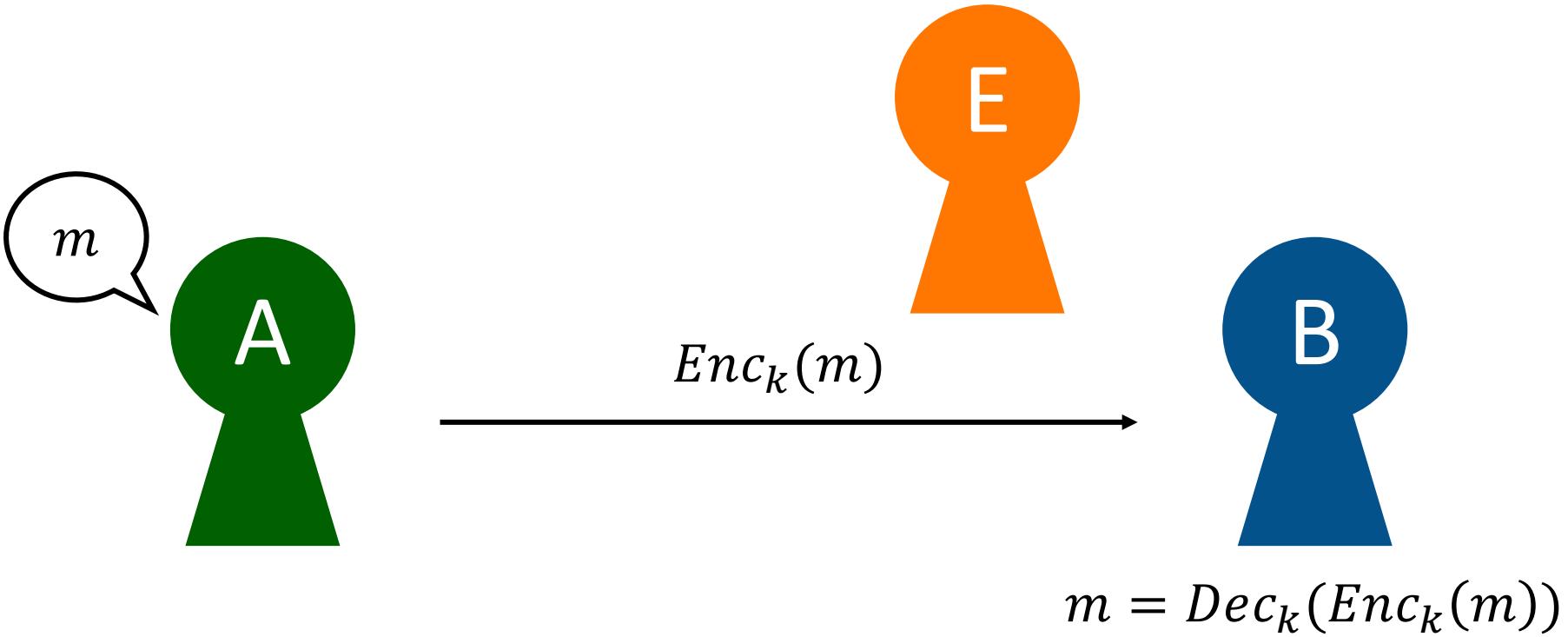
Formal Definition

How about this……

What is a good definition?

What should a good definition guarantee?

Let's consider an encryption scheme:



What should a secure encryption scheme guarantee?

What should a good definition guarantee?

What should a secure encryption scheme guarantee?

Trial 1: It should be impossible for an attacker to recover the key.

However, a trivial scheme

$$Enc_k(m) = m$$

achieve the definition. But it does not protect the message at all!

What should a good definition guarantee?

What should a secure encryption scheme guarantee?

Trial 2: It should be impossible for an attacker to recover the entire plaintext from the ciphertext.

However, the ciphertext may reveal last few bits. These may be the code for the nuclear missile and we are not satisfied with that.

What should a good definition guarantee?

What should a secure encryption scheme guarantee?

Trial 3: It should be impossible for an attacker to recover any character of the plaintext from the ciphertext.

However, we may still know which message is larger given two ciphertexts. It is not good if the message is your weight or score.

What should a good definition guarantee?

What should a secure encryption scheme guarantee?

Final answer: Regardless of any information an attacker already has, a ciphertext should leak no additional information about the underlying plaintext.

This informal definition captures all the concerns outlined above.

It still need to define what ``no information'' means.

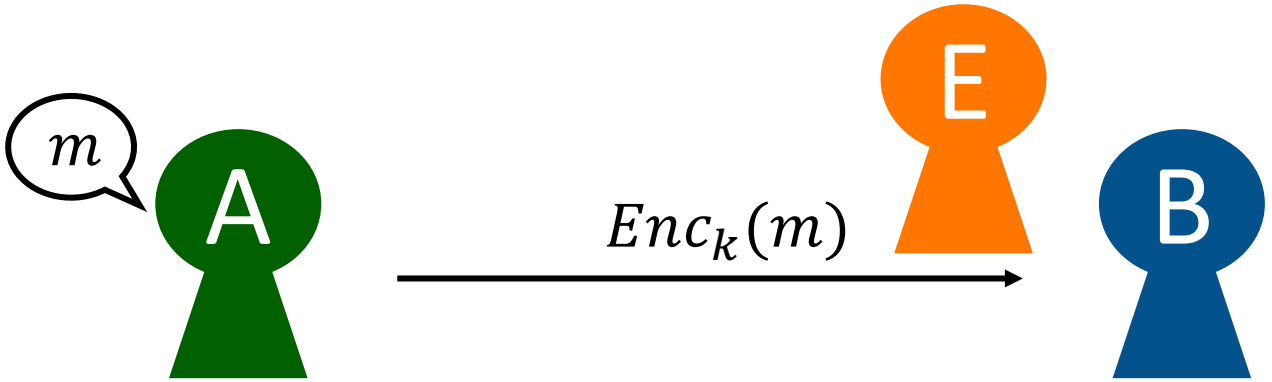
What is threat model?

A threat model specify the “power” of adversaries, but it does not restrict the strategy (how to use the power) of adversaries.

Take an encryption scheme for example:

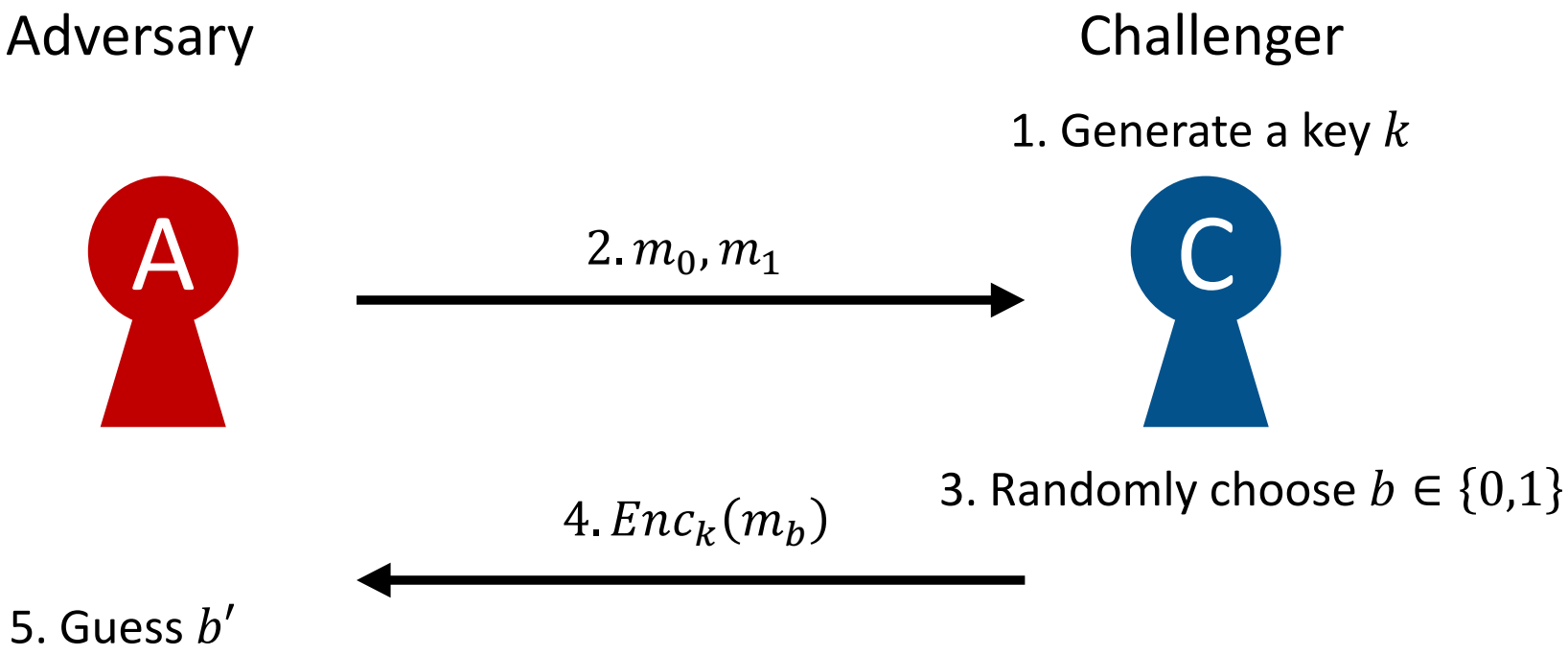
Does adversaries have unbounded power? Or polynomial-time power?

Does adversaries access to a encryption function?



$$m = Dec_k(Enc_k(m))$$

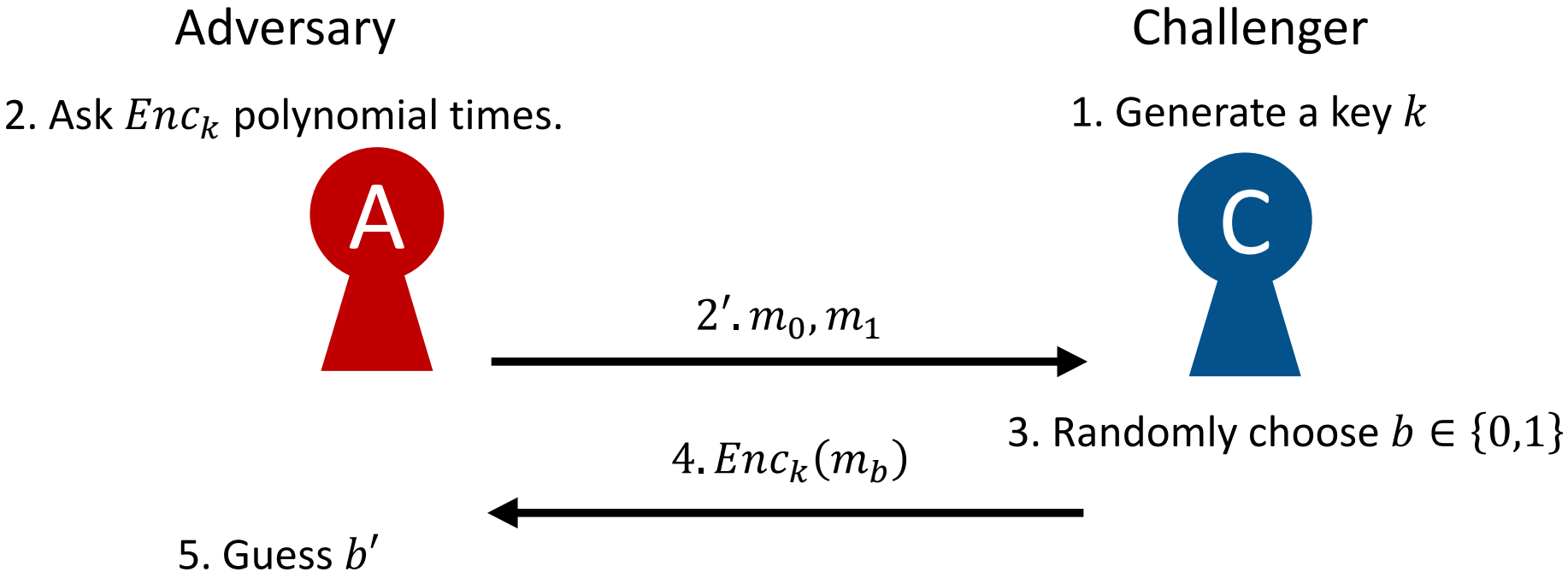
Indistinguishability Game



We say the adversary A wins the indistinguishability game if $b' = b$.

CPA Indistinguishability Game

What if we give the adversary more power? For example, if the adversary have encryption oracle.



We say the adversary A wins the indistinguishability game if $b' = b$.

Remark

In public key encryption scheme, since any one can encrypt the messages by public key, it seems that the adversary has the power of encryption oracle.

To achieve CPA-secure, we need randomized encryption.

Formal Definition

In practice, “giving any information to an attacker” may be too strong.

A probabilistic polynomial-time (PPT) adversary who can access encryption oracle could be a sound definition in reality.

Here we have the following definition:

Definition (CPA-secure)

An encryption scheme is secure under chosen-plaintext attack, if for all probabilistic polynomial-time adversaries, there exists a negligible function such that

$$\Pr[A\ wins\ CPA\ game] \leq \frac{1}{2} + \epsilon.$$

Precise Assumptions

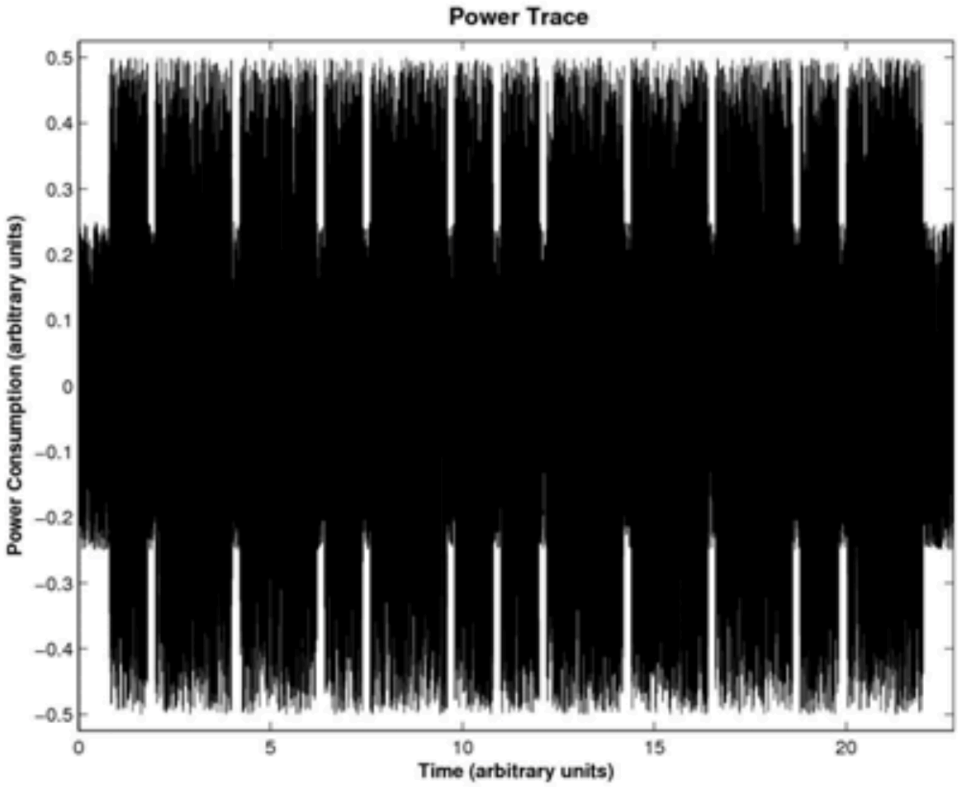
Precise assumptions describe the environment of adversaries and all involved parties, including

① the resource we have

② how the adversaries interact with all involved parties.

Side Channel Attack

Sometimes, a PPT adversary still can break the encryption system.



Proofs of Security

A security proof is a rigorous statement that is based on the assumptions and achieves the security definition.

Outline

① Concepts of Security Definition

② DDH problem and El Gamal

③ Security Proof of El Gamal

Discrete-logarithm problem

Given $\left(\mathbb{Z}_q, g, h = g^x\right)$, hard to find

$$\log_g h = x.$$

Diffie-Hellman problem

Given $\mathbb{Z}_q$ and $g \in \mathbb{Z}_q$.

If x, y, z are uniformly chosen from $\mathbb{Z}_q$, it is hard to distinguish

$$(g^x, g^y, g^{xy})$$

and

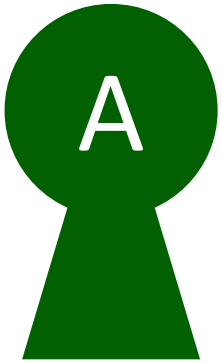
$$(g^x, g^y, g^z).$$

Definition (Decisional Diffie-Hellman)

We say decisional Diffie-Hellman problem is hard if for all efficient adversary, there exists a negligible function $\epsilon(n)$ such that

$$|\Pr[A(g^x, g^y, g^{xy}) = 1] - \Pr[A(g^x, g^y, g^z)] = 1| \leq \epsilon(n).$$

El Gamal Encryption



1. Choose $\left(\mathbb{Z}_q^*, g, x \in \mathbb{Z}_q\right)$

2. $pk = \left(\mathbb{Z}_q^*, g, h = g^x\right)$ →

3. Choose $y \in \mathbb{Z}_q$ and a plaintext m

4. $c = (g^y, h^y \cdot m)$ ←

5. Decrypt c by $m' = \frac{h^y \cdot m}{(g^y)^x} = \frac{g^{xy} \cdot m}{g^{xy}}$

Outline

① Concepts of Security Definition

② DDH problem and El Gamal

③ Security Proof of El Gamal

Security proof of El Gamal encryption

Theorem

If decisional Diffie-Hellman problem is hard, then the El Gamal encryption scheme is CPA-secure.

Proof idea:

If El Gamal is insecure, then DDH is not hard!

Reduce El Gamal to DDH

wants to distinguish (g^x, g^y, g^{xy}) and (g^x, g^y, g^z)

chooses m_0 and m_1
wants to guess b given $Enc_k(m_b)$

Reduce El Gamal to DDH

1. Get (g^x, g^y, h)

2. After using oracle, he chooses m_0, m_1.

3. (m_0, m_1)

$(g^y, h \cdot m_b)$

guessing bit b'

If $b' = b$, outputs $h = g^{xy}$;
If $b' \neq b$, outputs $h = g^z$.

Reduce El Gamal to DDH

Note that if $h = g^z$, $(g^y, h \cdot m_b)$ is not a valid ciphertext, Mr. El could only random guess. Thus,

$$\Pr[\text{Mr.DDH wins}] = \Pr[\text{Mr.El loses}] = \frac{1}{2},$$

that is

$$\Pr[DDH(g^x, g^y, g^z) = 1] = \frac{1}{2}.$$

On the other case, if $h = g^{xy}$, Mr.DDH wins if Mr.El also wins. Thus,

$$\Pr[\text{Mr.DDH wins}] = \Pr[\text{Mr.El wins}],$$

that is

$$\Pr[DDH(g^x, g^y, g^{xy}) = 1] = \Pr[\text{Mr.El wins}].$$

Reduce El Gamal to DDH

However, by assumption

$$|\Pr[A(g^x, g^y, g^{xy}) = 1] - \Pr[A(g^x, g^y, g^z)] = 1| \leq \epsilon(n).$$

Thus, we have

$$\left|\Pr[\text{Mr.El wins}] - \frac{1}{2}\right| \leq \epsilon(n).$$

This implies

$$\Pr[\text{Mr.El wins}] \leq \frac{1}{2} + \epsilon(n),$$

so El Gamal is CPA-secure.

Thanks for your attention