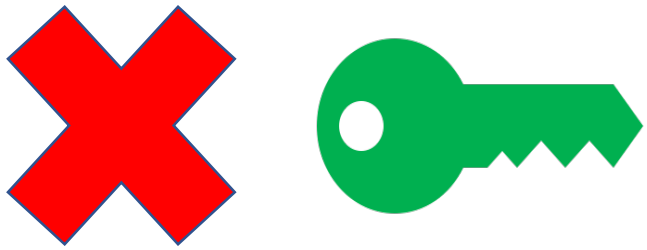
Security Definitions on Time-Lock Puzzles

Daiki Hiraga*1 Keisuke Hara*1*2 Masayuki Tezuka*1
Yusuke Yoshida*1 Keisuke Tanaka*1

*1:Tokyo Institute of Technology
*2:AIST

Time Lock

Time Lock



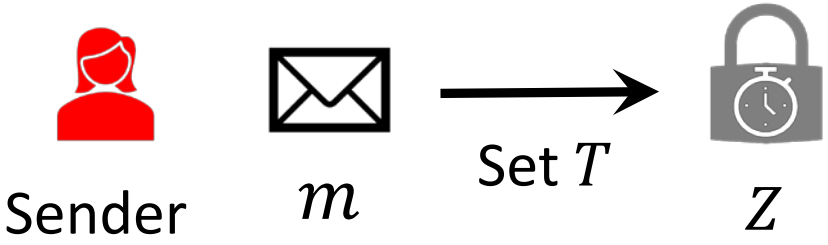
The key does not exist and no one can open it for a certain period of time

Time-Lock Puzzle[RSW96]

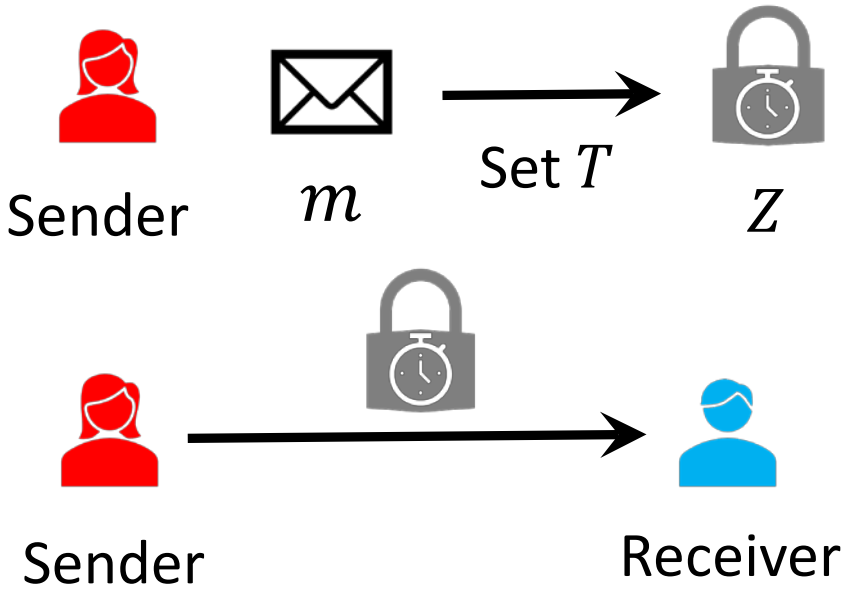
Sender

Receiver

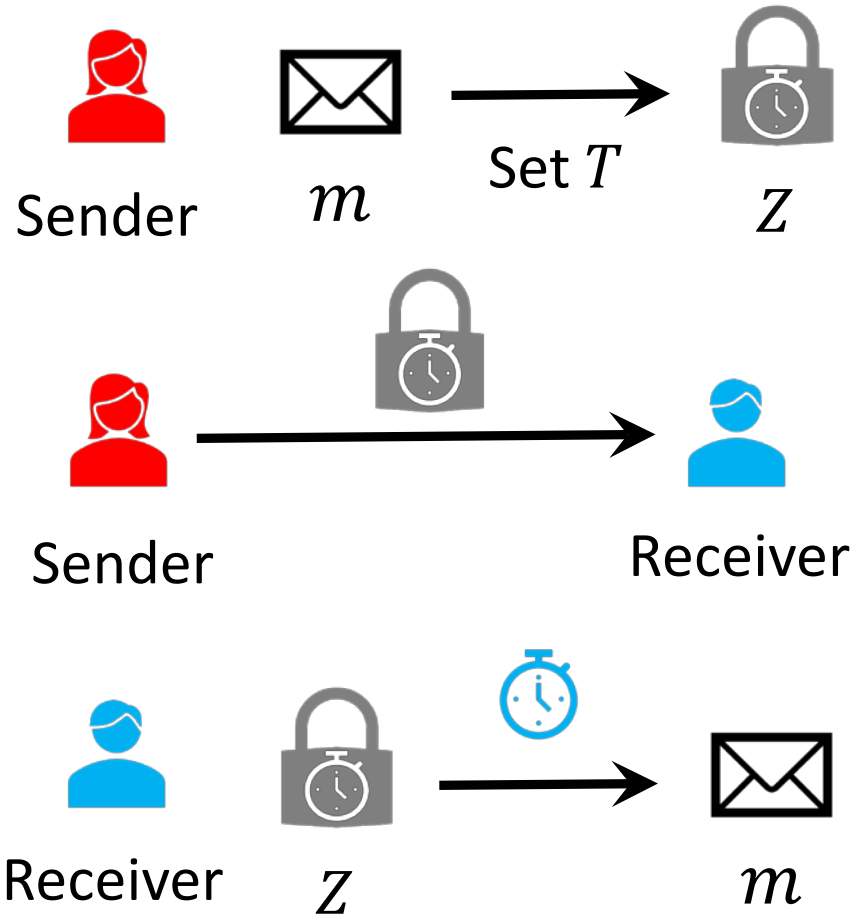
Time-Lock Puzzle[RSW96]



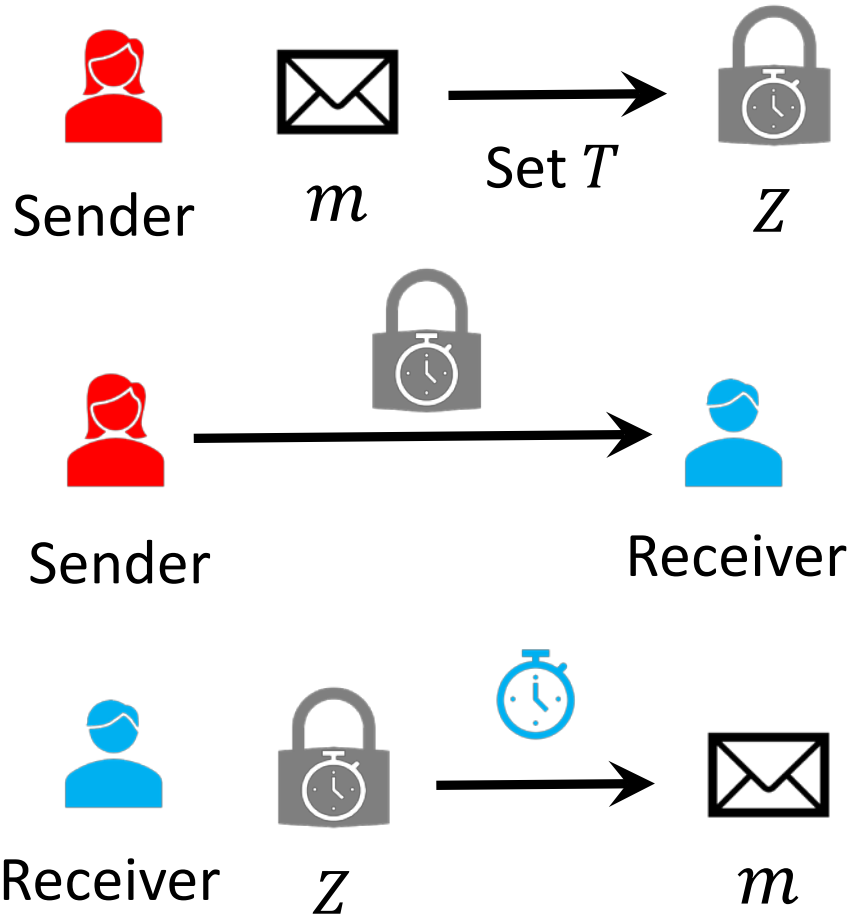
Time-Lock Puzzle[RSW96]



Time-Lock Puzzle[RSW96]

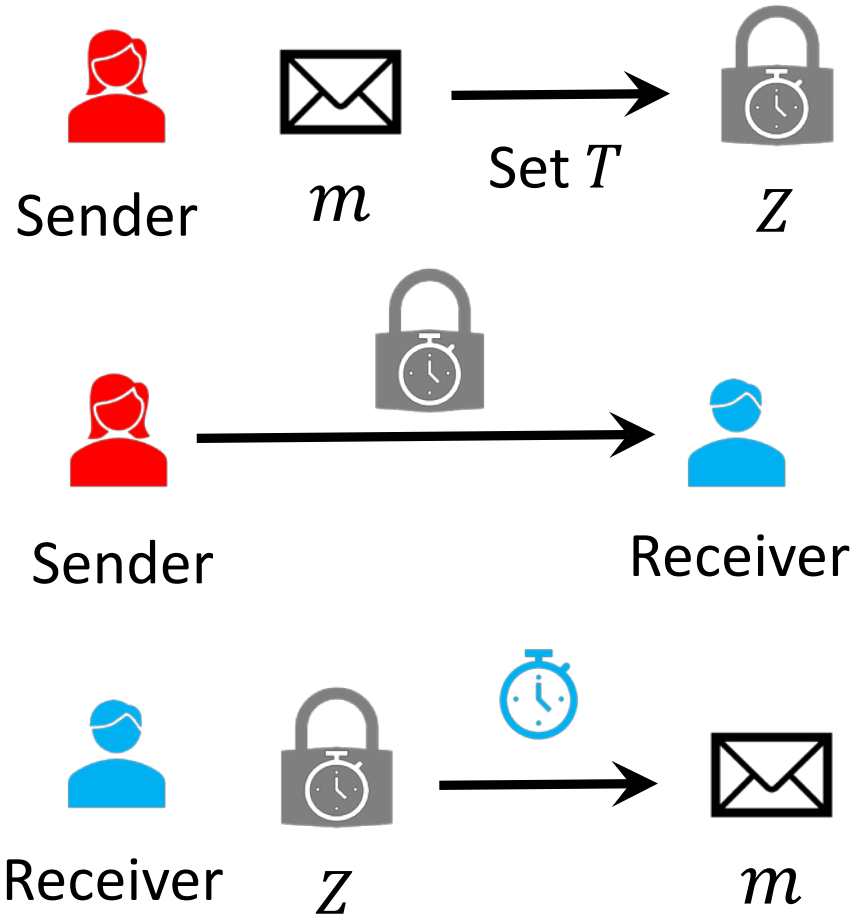


Time-Lock Puzzle[RSW96]



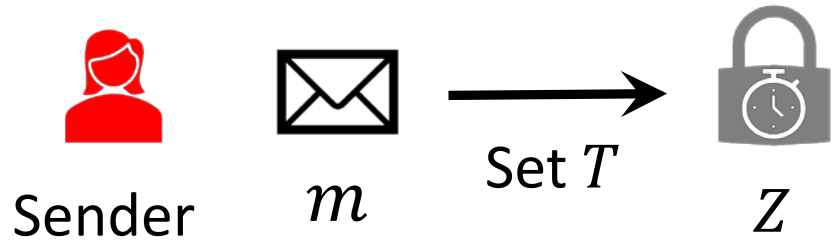
- Puzzle generation takes much shorter than T.

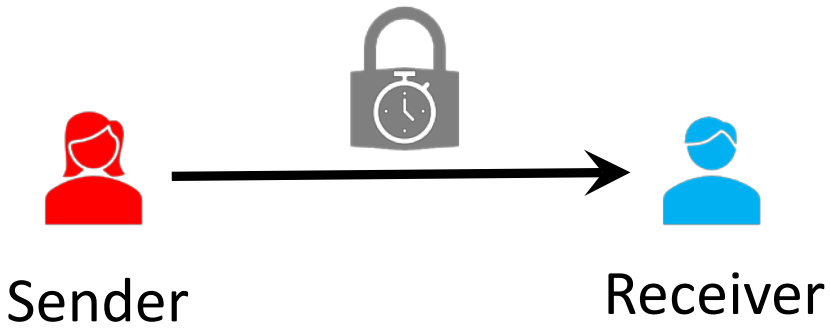
Time-Lock Puzzle[RSW96]

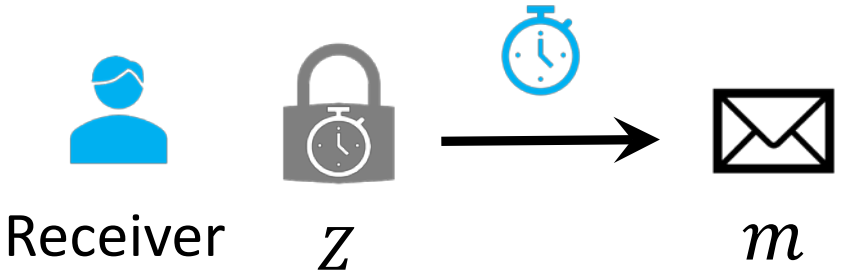


- Puzzle generation takes much shorter than T.
- Receiver cannot get information about the message in less than time T.

Time-Lock Puzzle[RSW96]



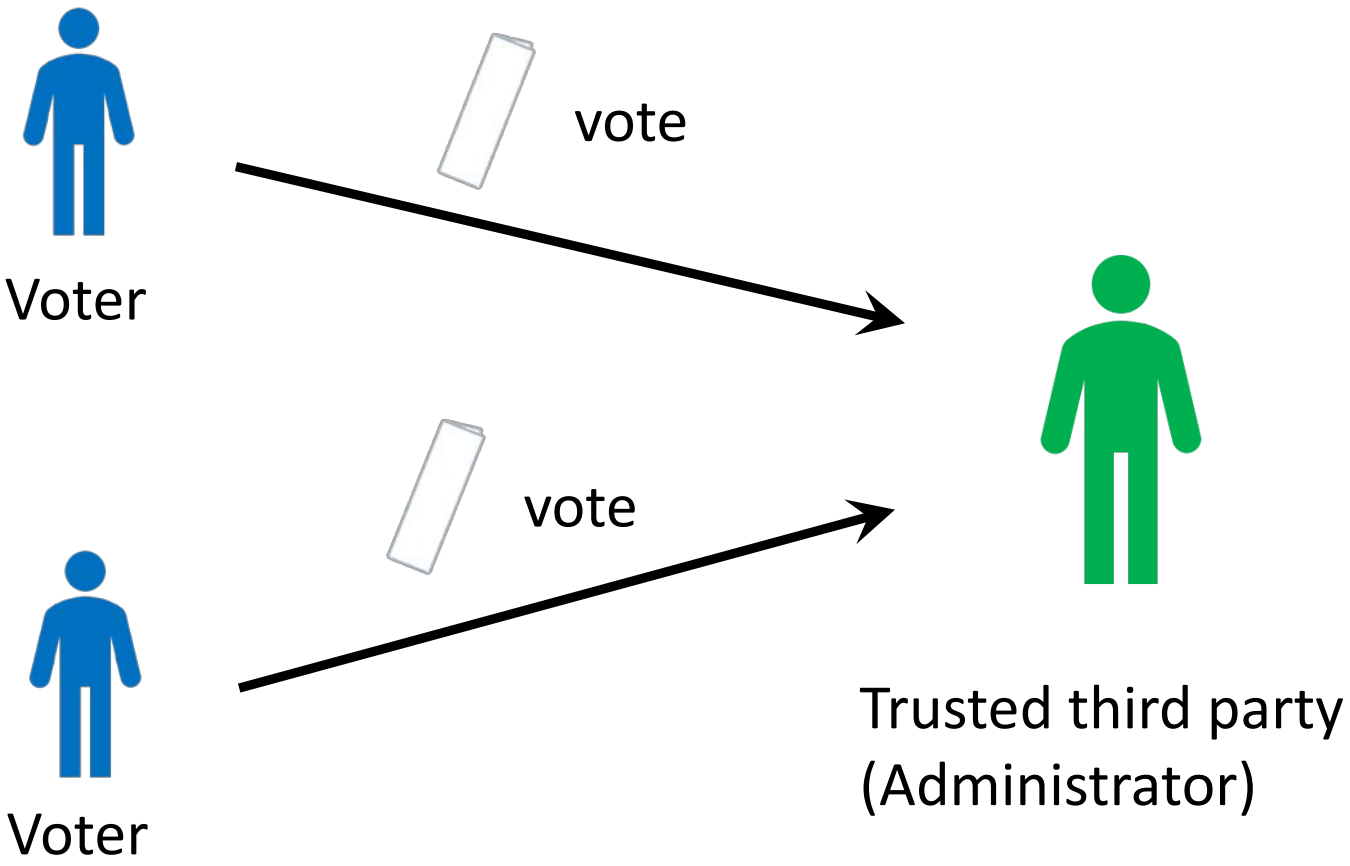




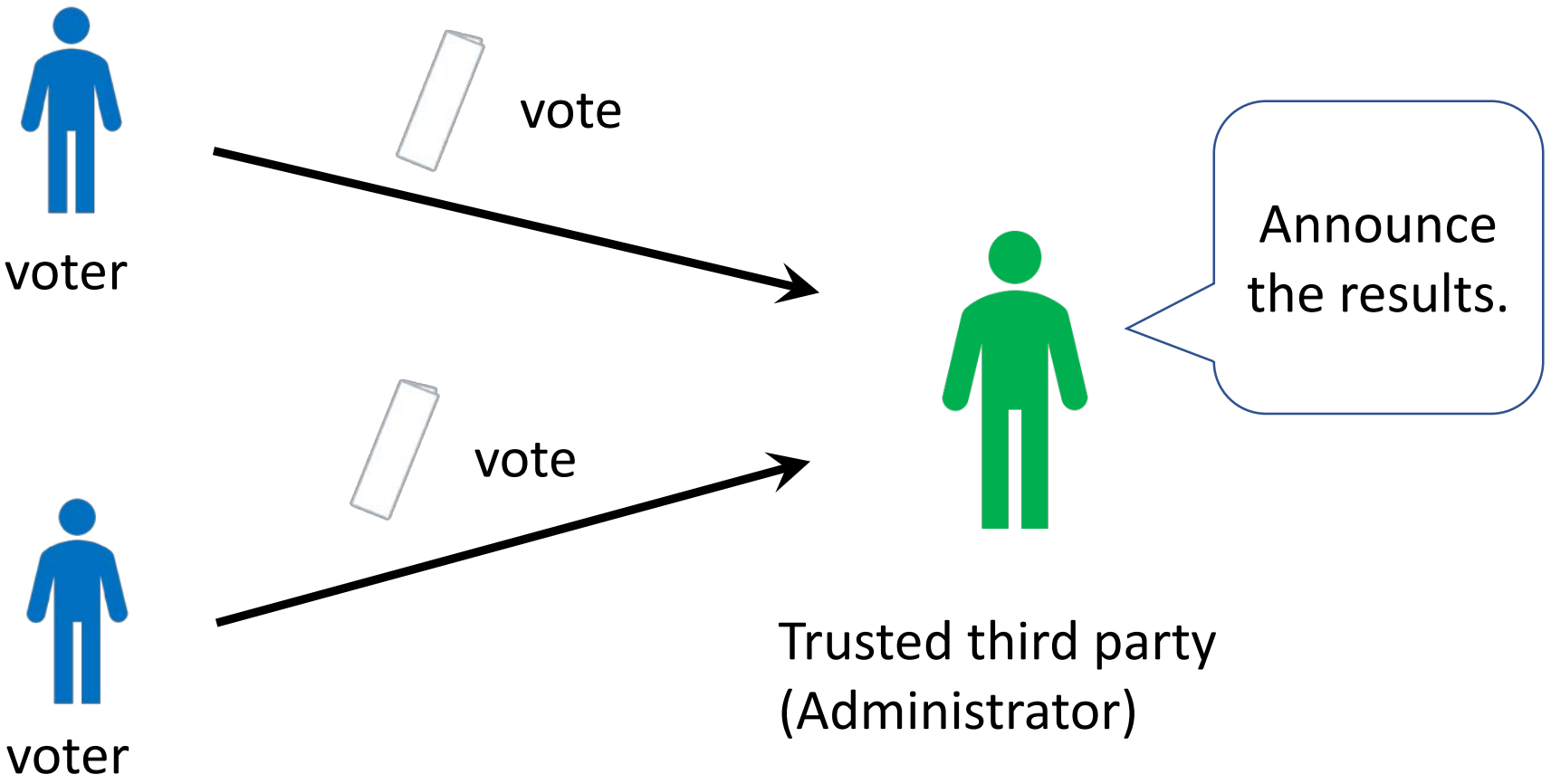
- Puzzle generation takes much shorter than T.
- Receiver cannot get information about the message in less than time T.

Parallel computing cannot speed up the time to solve puzzles.

E-voting(trusted third party)

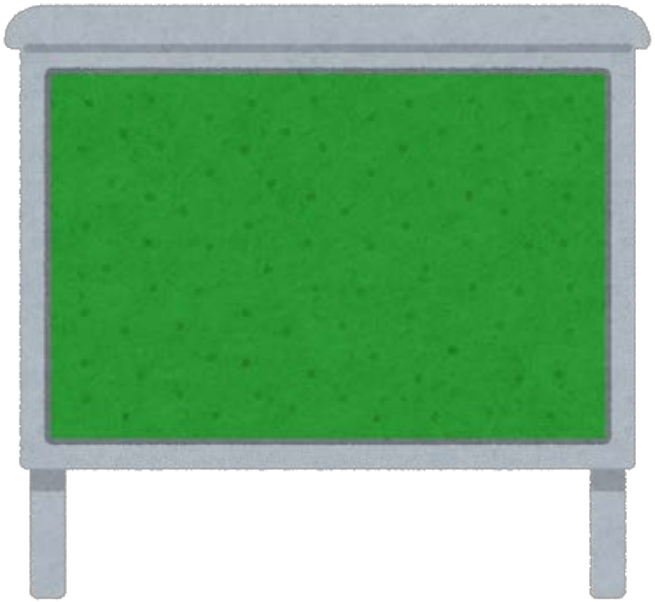


E-voting(trusted third party)



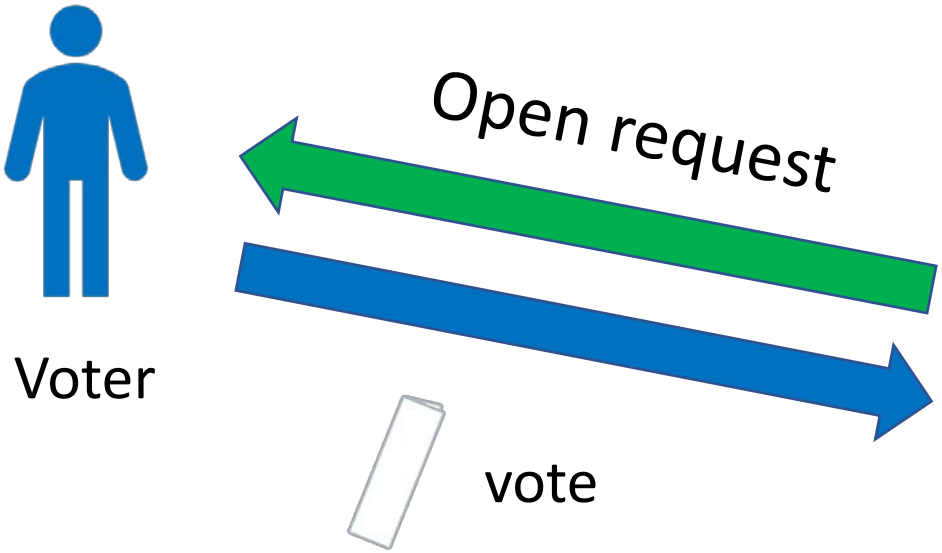
E-voting（commitment）

Voting phase

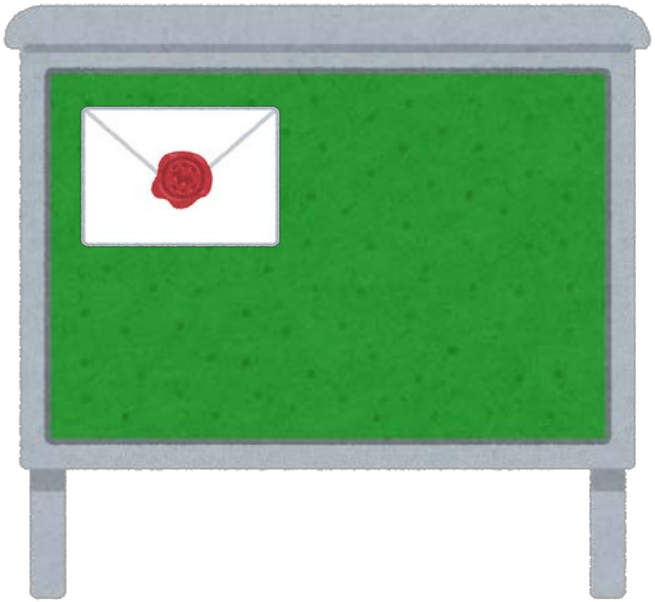


bulletin board

E-voting（commitment）



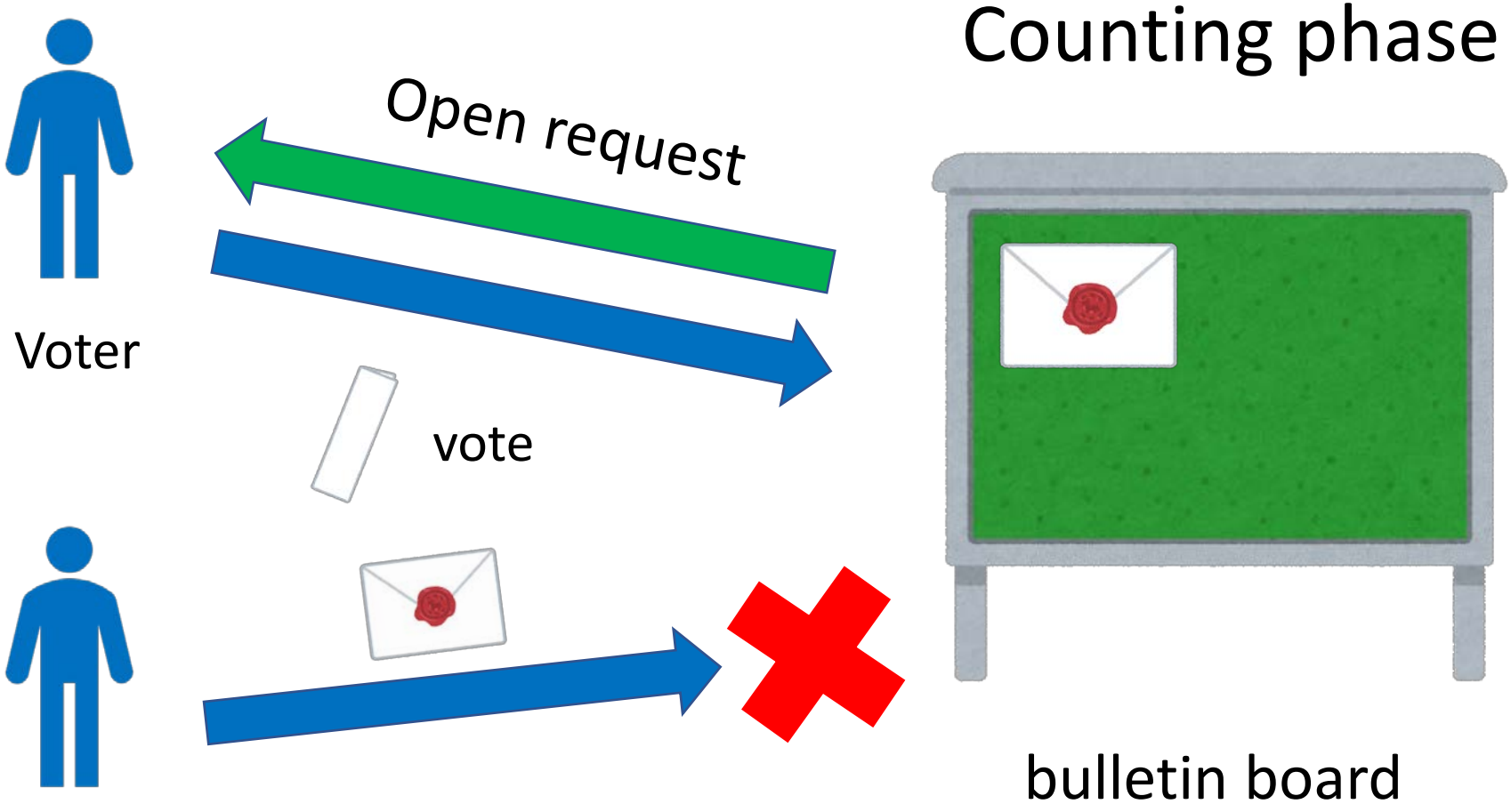
Counting phase



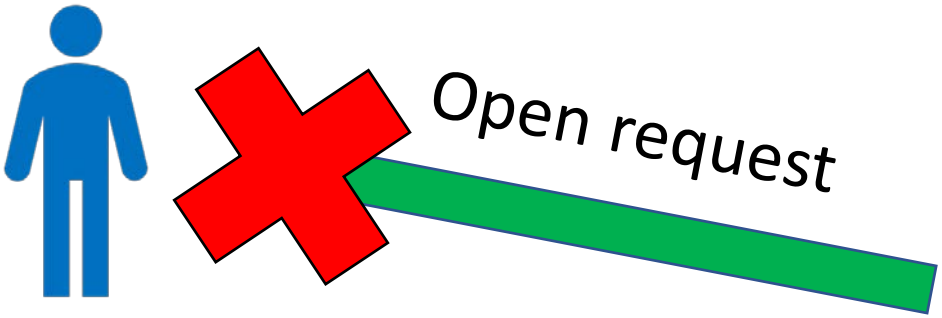
bulletin board

E-voting（commitment）

Counting phase

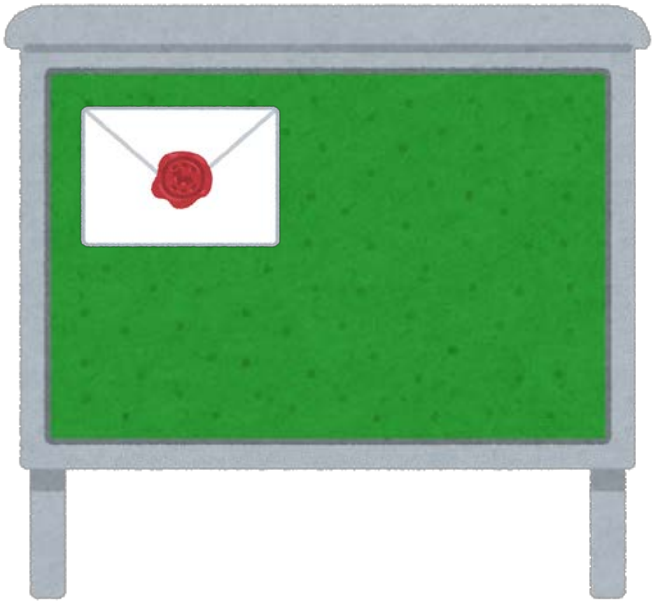


E-voting（commitment）



No one can know the result.

Counting phase

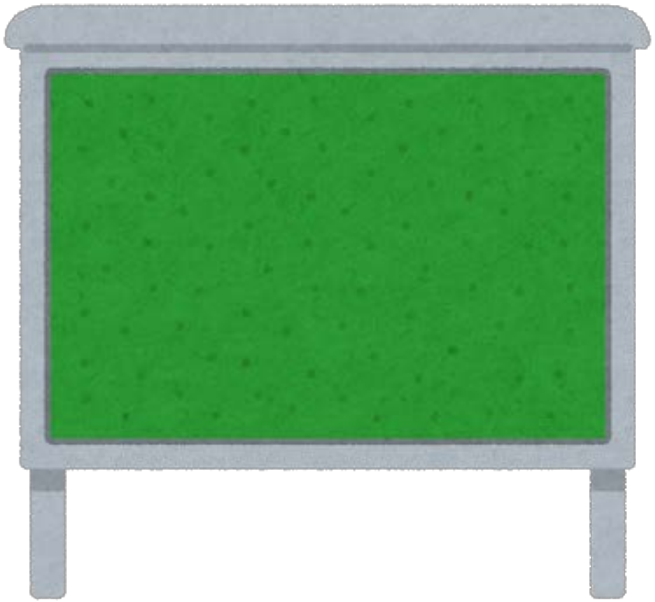


bulletin board

E-voting（Time-Lock Puzzle）

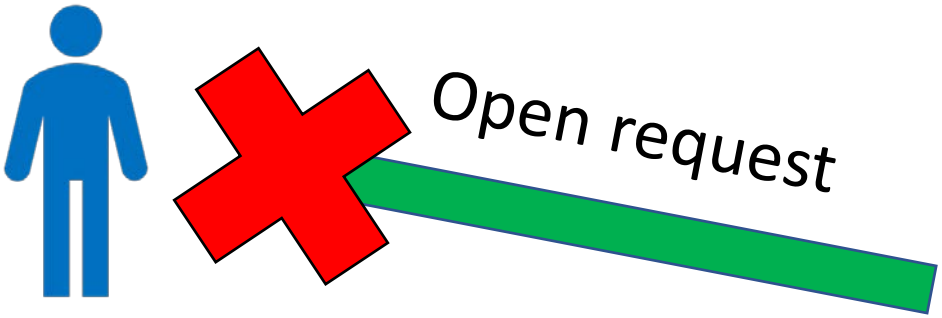
Voter

Voting phase



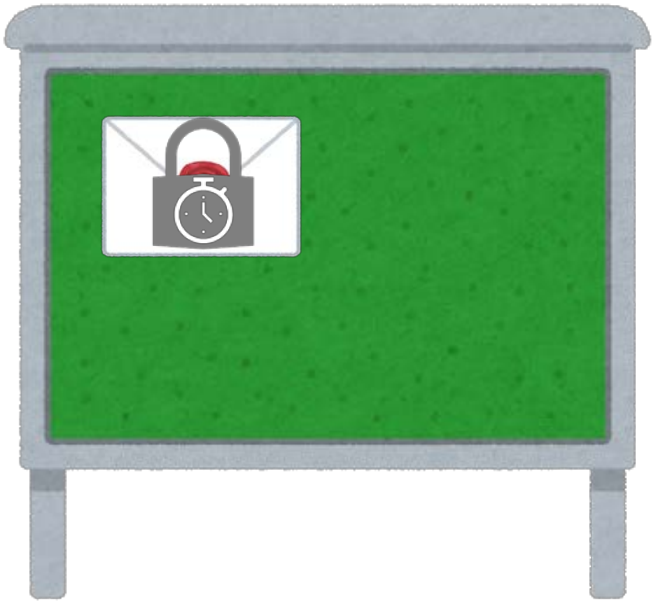
bulletin board

E-voting（Time-Lock Puzzle）



Voter

Counting phase



bulletin board

We can know the result by solving the puzzle

Related Works

Construction

・A time-lock puzzle from the inherent sequentiality of repeated squaring in the RSA group[RSW96]

Related Works

Construction

・A time-lock puzzle from the inherent sequentiality of repeated squaring in the RSA group[RSW96]

・Time-lock puzzles from non-parallelizable languages and randomized encodings [BGJ+16]

Related Works

Construction

・A time-lock puzzle from the inherent sequentiality of repeated squaring in the RSA group[RSW96]

・Time-lock puzzles from non-parallelizable languages and randomized encodings [BGJ+16]

Advanced functionality

・A fully homomorphic time-lock puzzle[MT19],[BDG+19]

Related Works

Construction

・A time-lock puzzle from the inherent sequentiality of repeated squaring in the RSA group[RSW96]

・Time-lock puzzles from non-parallelizable languages and randomized encodings [BGJ+16]

Advanced functionality

・A fully homomorphic time-lock puzzle[MT19],[BDG+19]

Application

・ A non-malleable commitment from a time-lock puzzle[LPS17]

Related Works

Construction

・A time-lock puzzle from the inherent sequentiality of repeated squaring in the RSA group[RSW96]

・Time-lock puzzles from non-parallelizable languages and randomized encodings [BGJ+16]

Advanced functionality

・A fully homomorphic time-lock puzzle[MT19],[BDG+19]

Application

・A non-malleable commitment from a time-lock puzzle[LPS17]

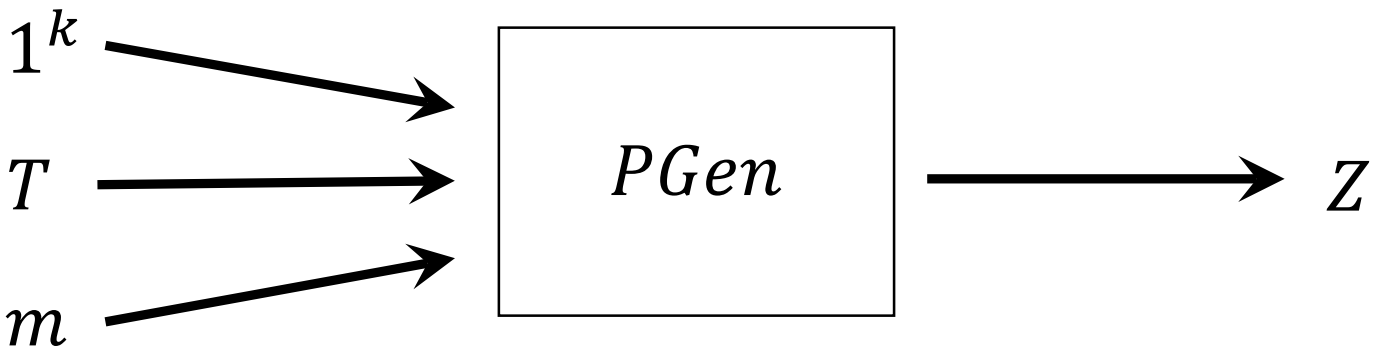
There are few works on the security models of time-lock puzzles.

Our Contribution

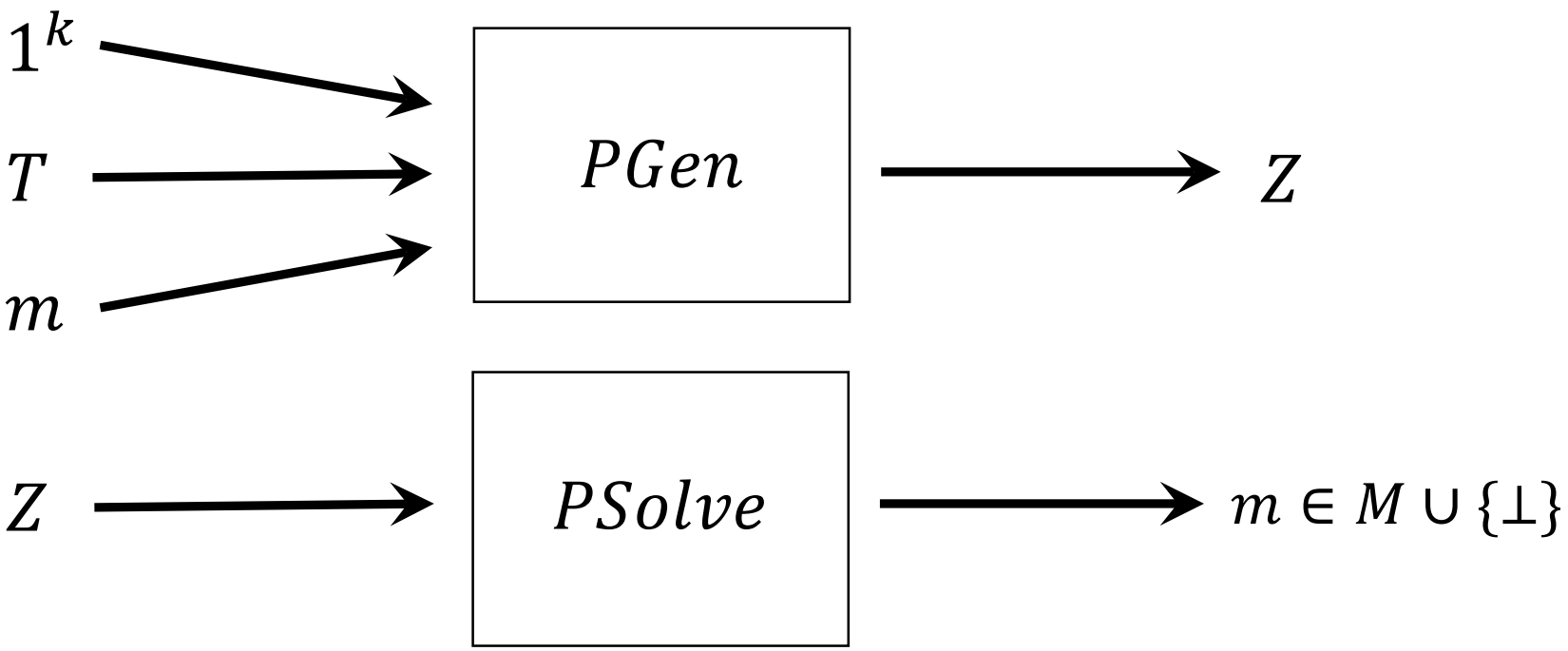
1. we define new security for time-lock puzzles (semantic security).

2. we investigate the security relationship for time-lock puzzles.

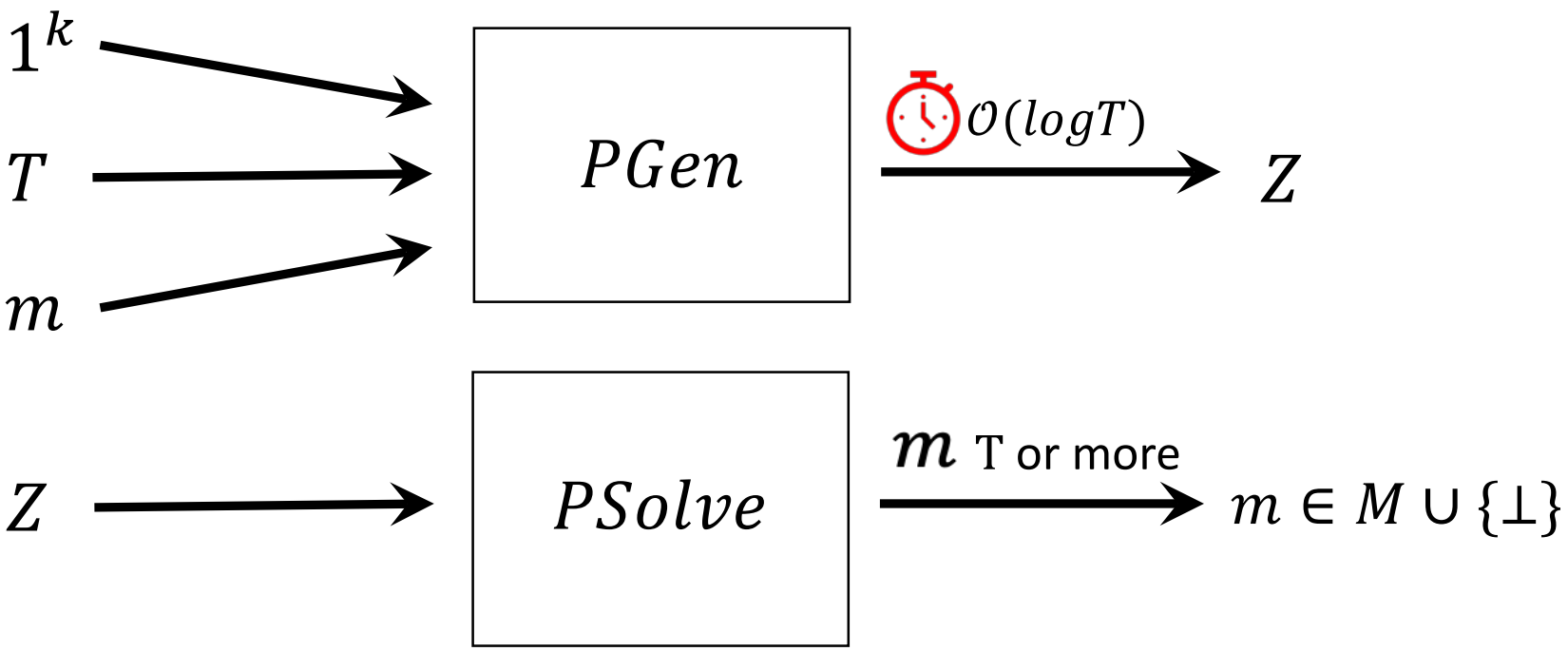
Definition



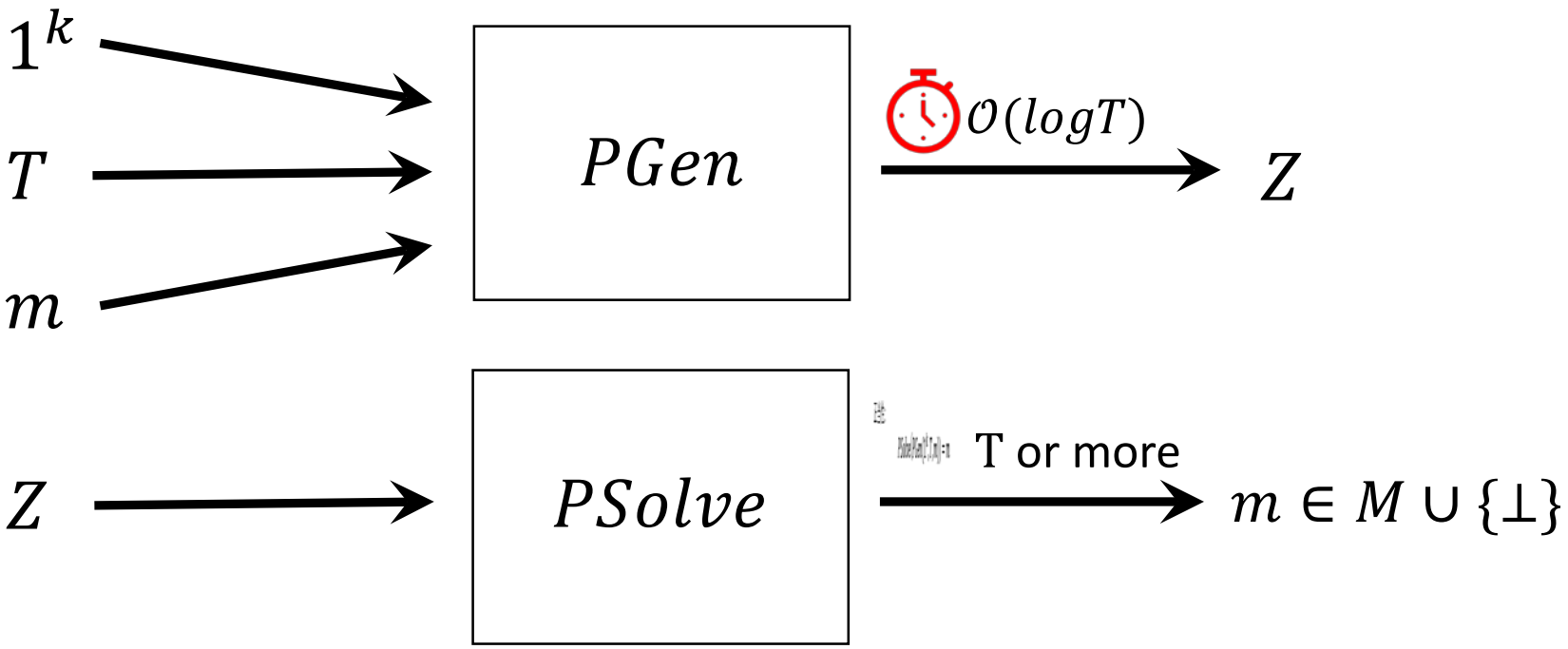
Definition



Definition



Definition



correctness:

$$PSolve(PGen(1^k, T, m)) = m$$

Indistinguishability[BGJ+16]

Challenger

Adversary

(m_0, m_1)

Indistinguishability[BGJ+16]

Challenger

Adversary

(m_0, m_1)

$b \leftarrow \{0,1\}$

$Z \leftarrow PGen(1^k, T, m_b)$

Z

Indistinguishability[BGJ+16]

Challenger

Adversary

(m_0, m_1)

$b \leftarrow \{0,1\}$

$Z \leftarrow PGen(1^k, T, m_b)$

Z

less than T^{ϵ}
$(0 < \epsilon < 1)$

b’

$b = b'$?

Motivation

Time-lock puzzle

Security Requirement = Indistinguishabiility ?

Motivation

Public-key encryption

- Security Requirement

Information about plaintext does not leak from ciphertext. = Semantic Security

Motivation

Public-key encryption

- Security Requirement

Information about plaintext does not leak from ciphertext. = Semantic Security

= Indistinguishability

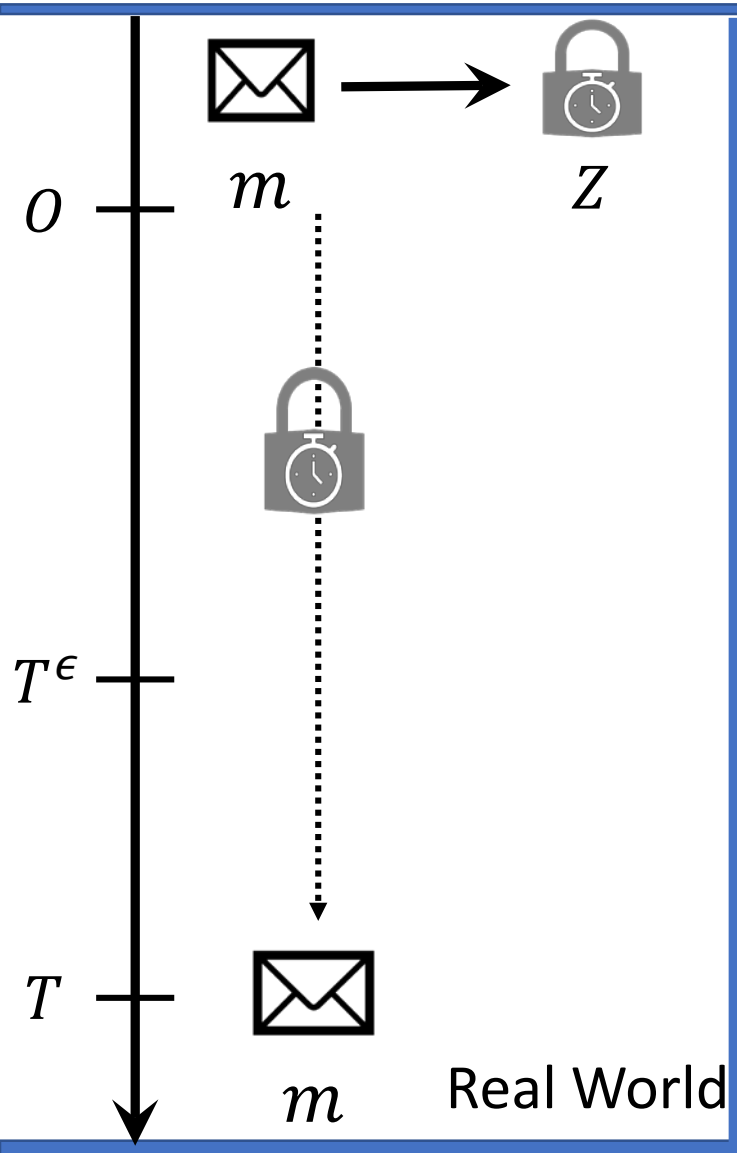
Motivation

Time-lock puzzle

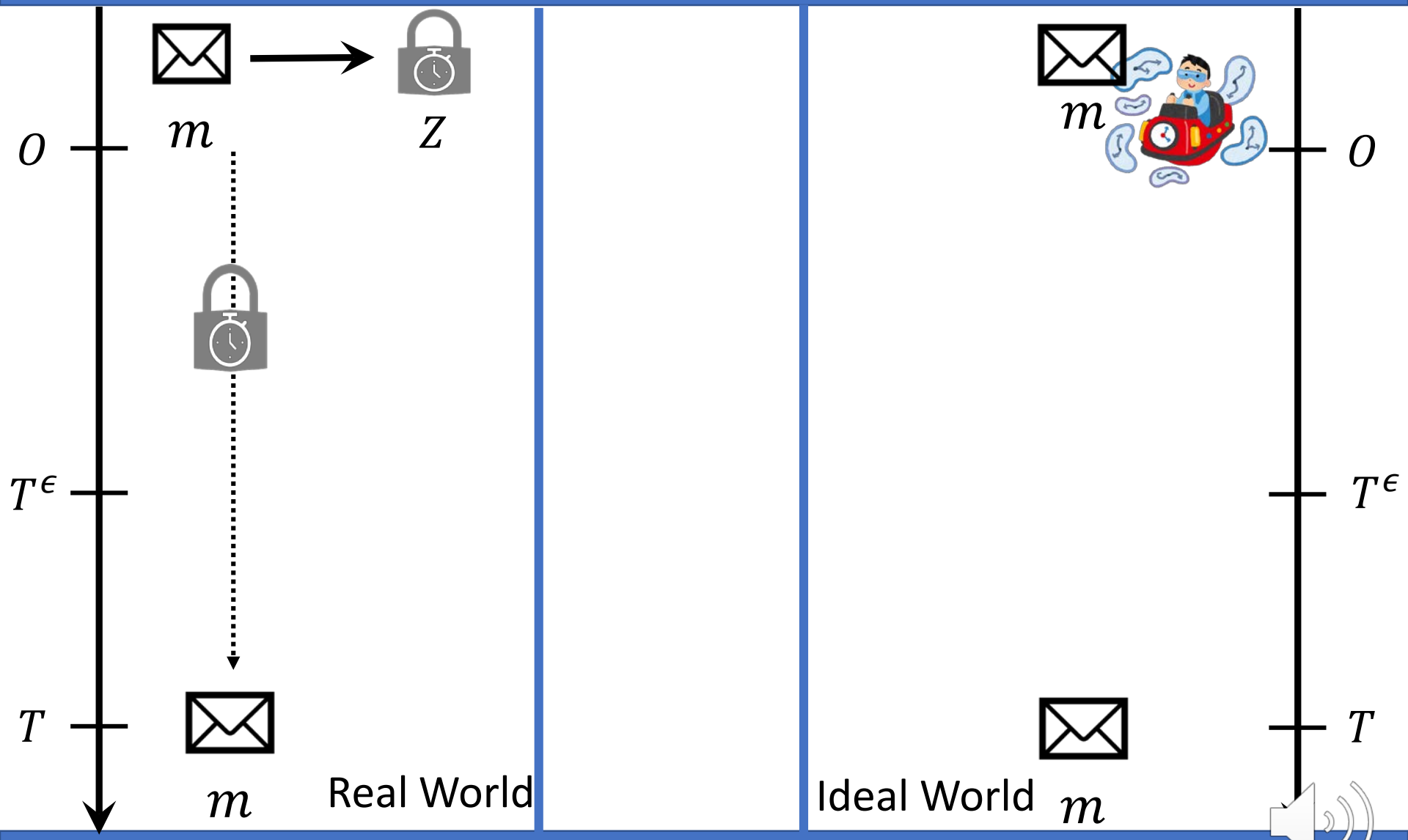
Security Requirement = Semantic Security

= Indistiguishability?

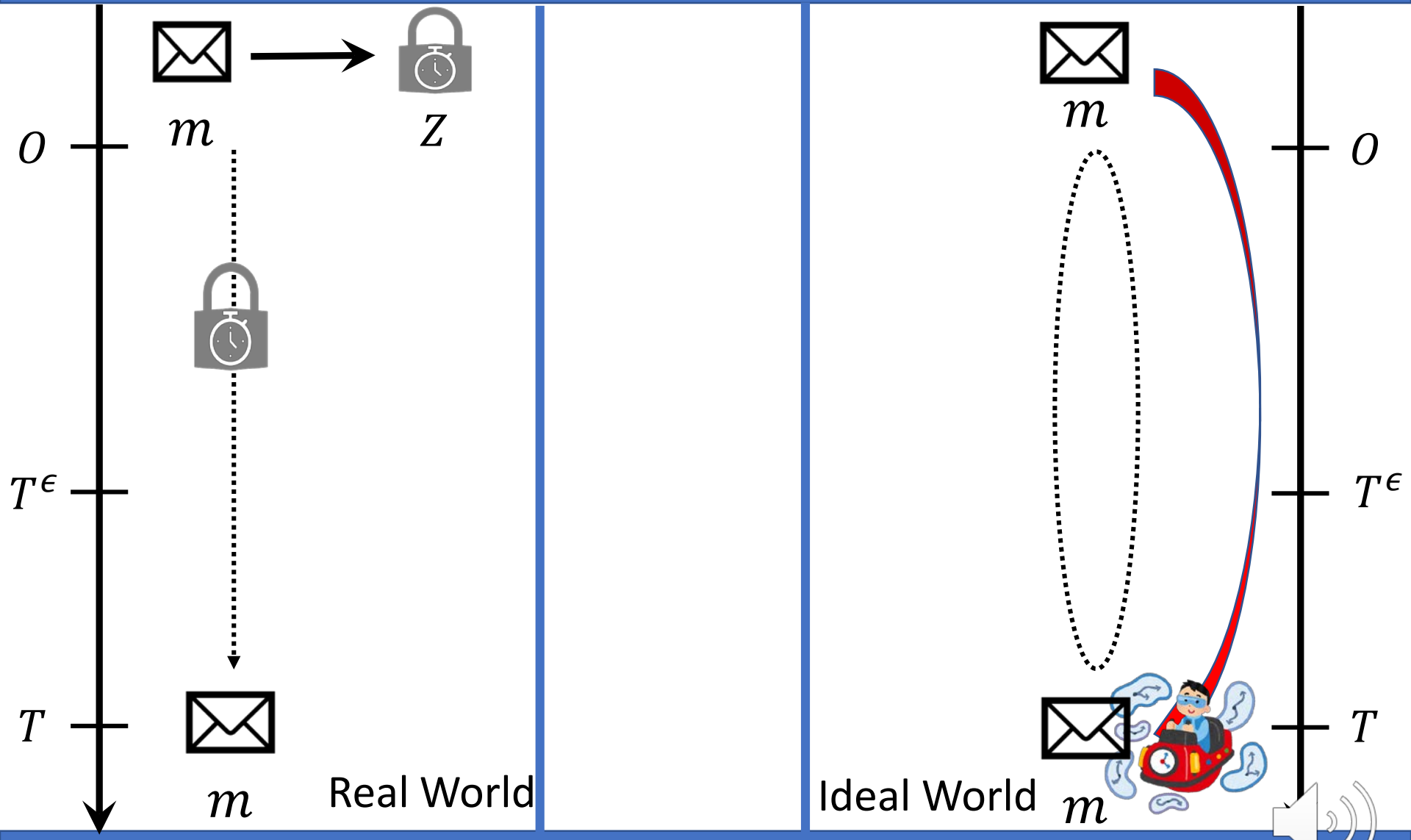
What is Semantic Security?



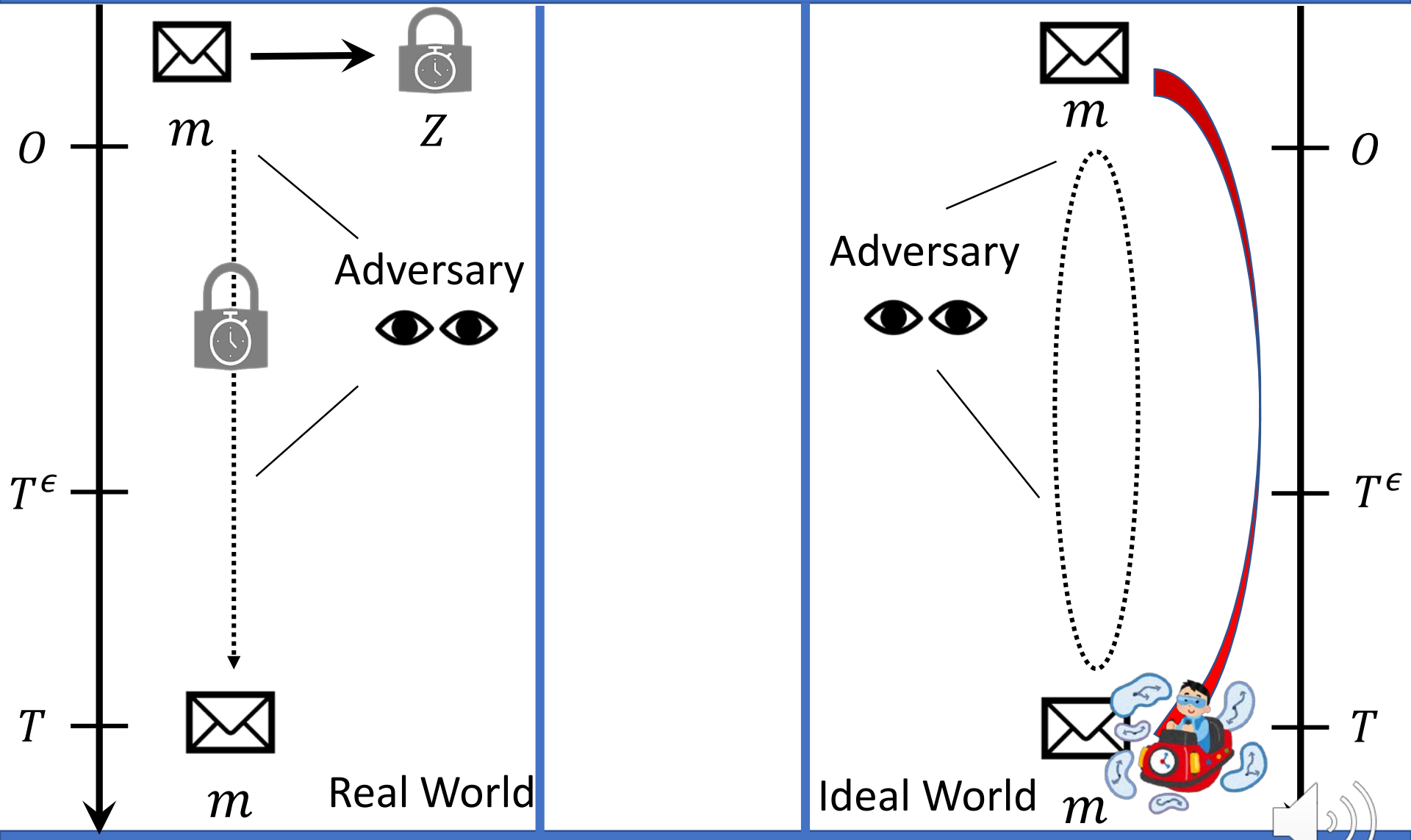
What is Semantic Security?



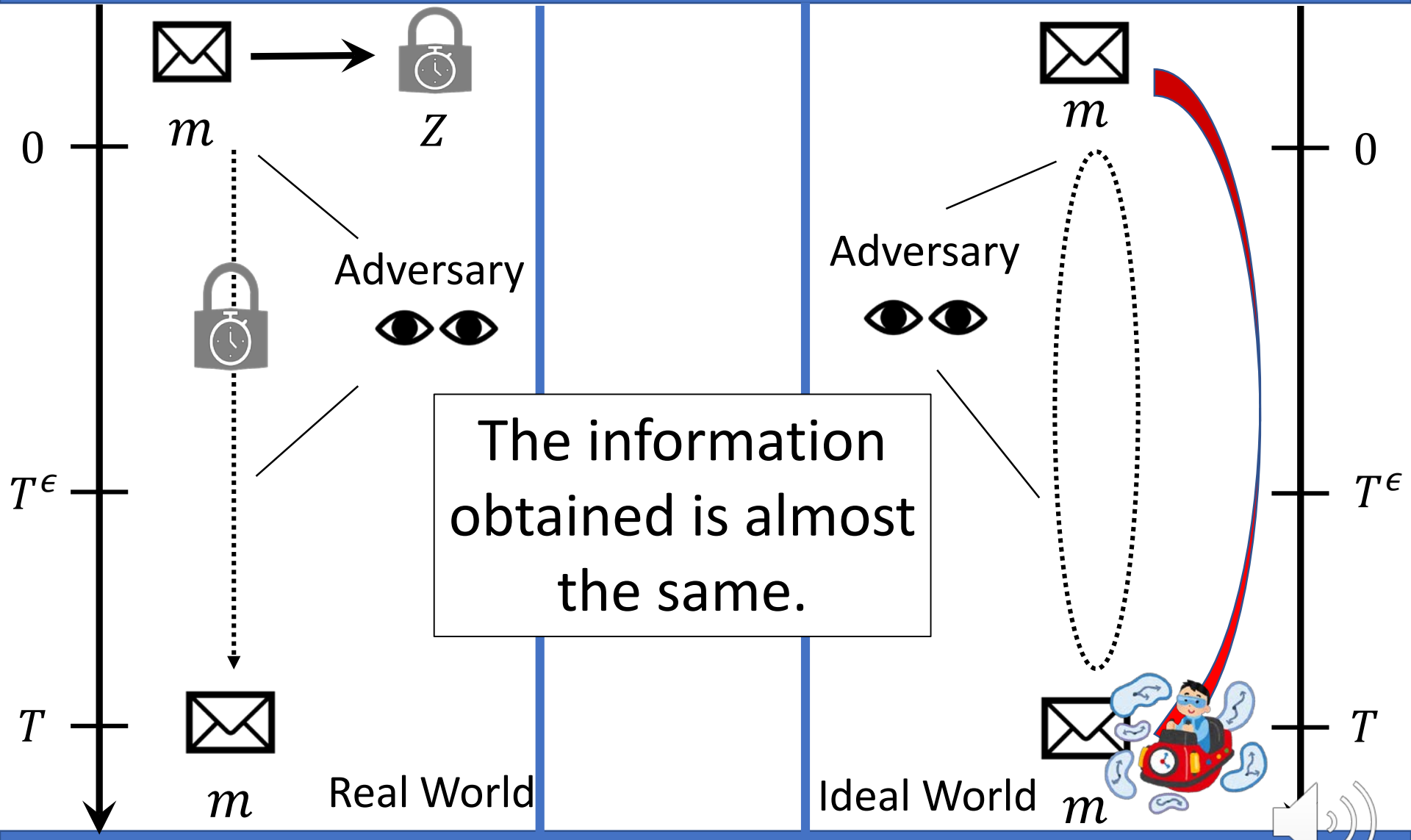
What is Semantic Security?



What is Semantic Security?



What is Semantic Security?



Definition of Semantic Security

Challenger

Adversary

$\mathcal{M}$

Real World

Definition of Semantic Security

Challenger

Adversary

$\mathcal{M}$

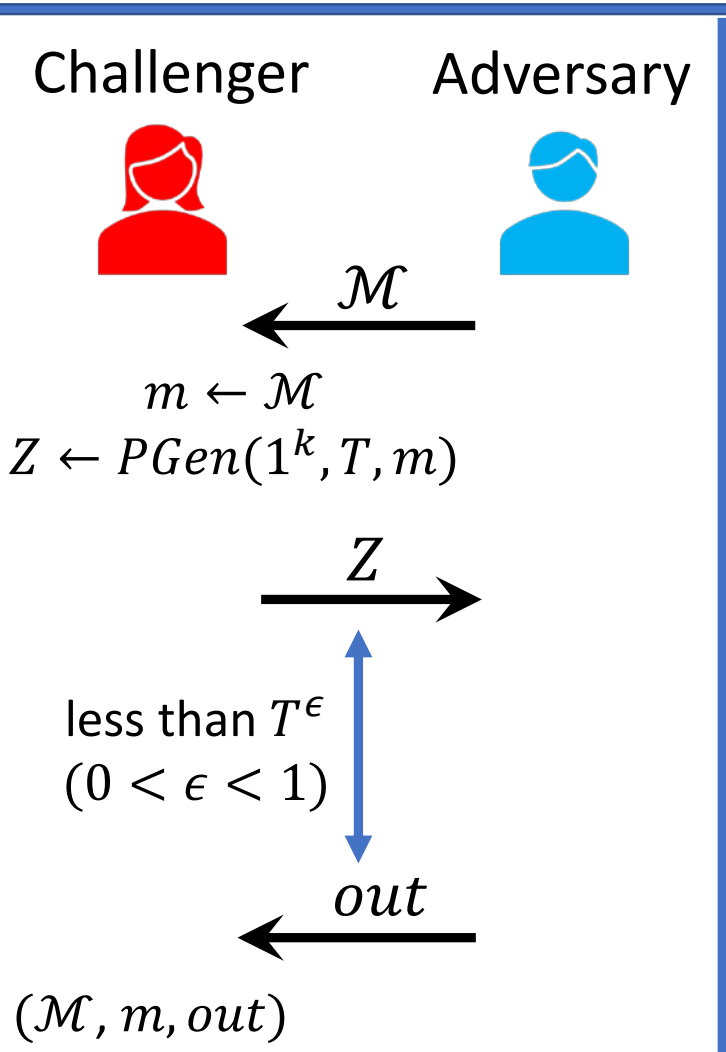
$m \leftarrow \mathcal{M}$

$Z \leftarrow PGen(1^k, T, m)$

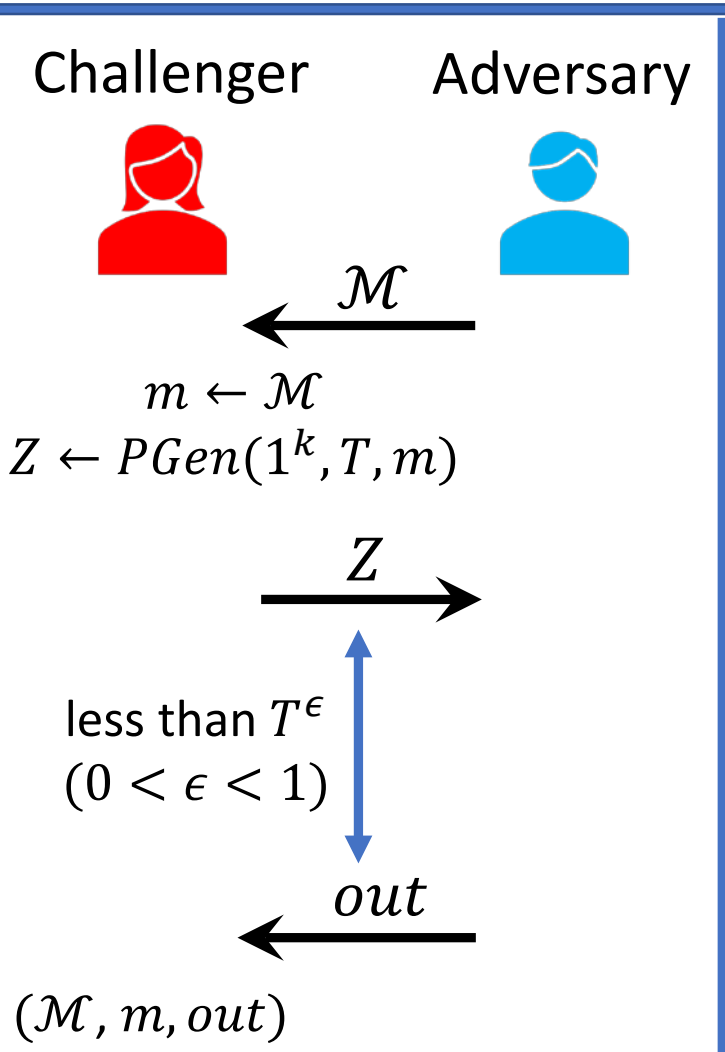
Z

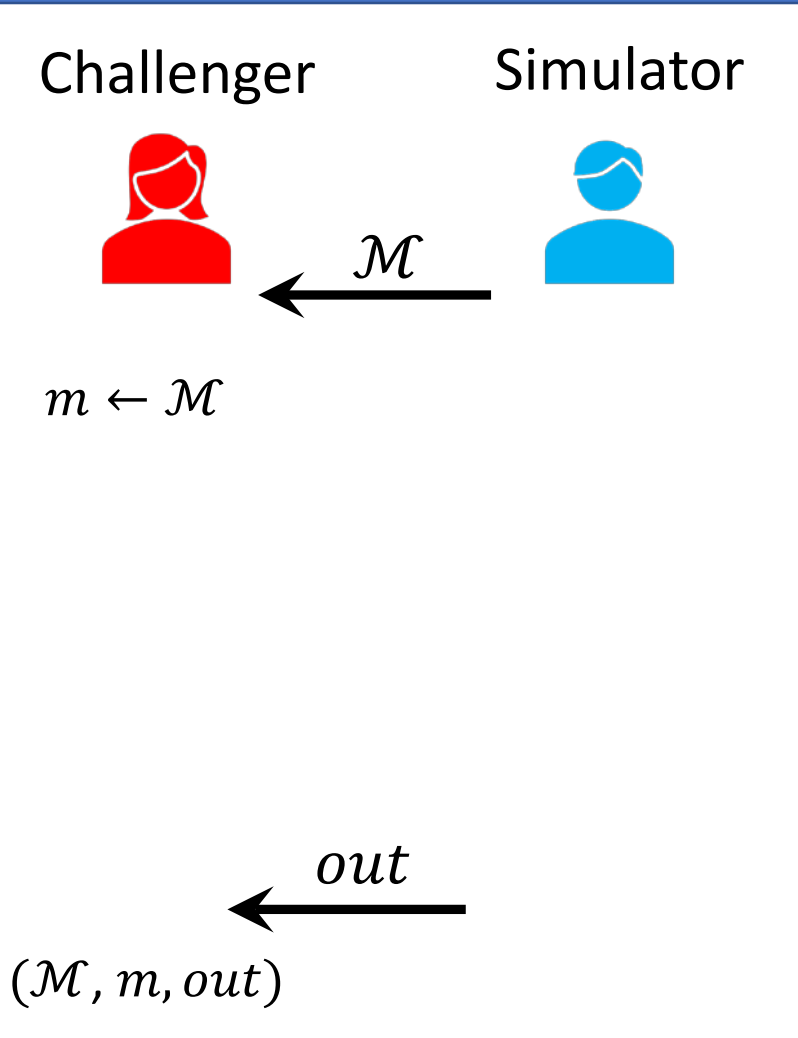
Real World

Definition of Semantic Security

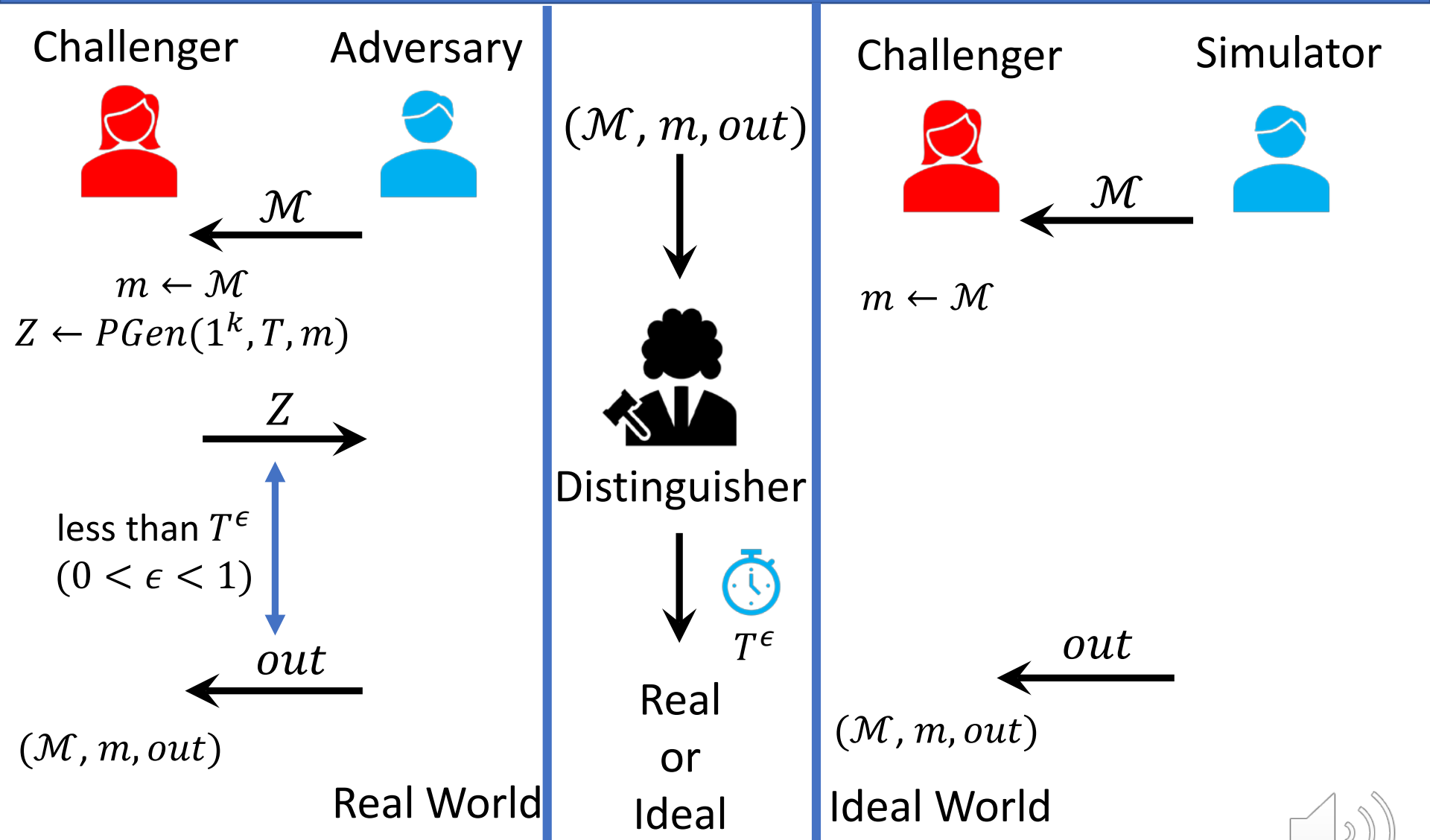


Definition of Semantic Security





Definition of Semantic Security



Security Relationship

Relationship between indistinguishability and semantic security?

Public-key Encryption

indistiinguishability = semantic security is provable

Security Relationship

Relationship between indistinguishability and semantic security?

Public-key Encryption

indistiinguishability ＝ semantic security is provable.

Time-Lock Puzzle

It is difficult to show the relationship between indistinguishability and semantic security.

Security Relationship

Relationship between indistinguishability and semantic security?

Public-key Encryption

Computational restriction $poly(k)$

Time-Lock Puzzle

Computational restriction T^{ϵ} or less

Security Relationship

Relationship between indistinguishability and semantic security?

Let‘s relax the restriction T^{ϵ}

Security Relationship

- (Adversary's computational time) $\leq T^{\epsilon}$

SS $\Rightarrow$ IND $\times$ IND $\Rightarrow$ SS $\times$

Security Relationship

- (Adversary's computational time) $\leq T^{\epsilon}$

  SS ⇒ IND ×　IND ⇒ SS ×

- (Adversary's computational time) $\leq T^{\epsilon} + \mathcal{O}(1)$

  SS ⇒ IND ○　IND ⇒ SS ×

Security Relationship

- (Adversary's computational time) $\leq T^{\epsilon}$

  SS ⇒ IND × IND ⇒ SS ×

- (Adversary's computational time) $\leq T^{\epsilon} + \mathcal{O}(1)$

  SS ⇒ IND ○ IND ⇒ SS ×

- (Adversary's computational time) $= \mathcal{O}(T^{\epsilon})$

  SS ⇒ IND ○ IND ⇒ SS ○

Summary

1 .Definition of Semantic Security

We define semantic security for time-lock puzzles.

2 . Security Relationship between IND and SS

Provability depends on the adversary's computational restriction.

・Open problem

- ○Which computational restrictions should be used in the definition?
- ○Define and formulate security for time-lock puzzles other than indistinguishabiility and semantic security