# Colluding Attacks to a Payment Protocol and Two Signature Exchange Schemes

Feng Bao

Institute for Infocomm Research ($I^2R$)

Singapore

# Overview

Presenting a colluding attack against

1. C H Wang, Untraceable fair network payment protocol with off-line TTP, Asiacrypt'03
2. N Ateniese, Efficient verifiable encryption and fair exchange of digital signatures, ACM CCS'99.

The attack is more serious against 1 than 2.

# Untraceable Fair Network Payment Protocol

- Account opening
- Withdrawal
- Payment
- Disputes
- Deposit

A*STAR I²R

# Untraceable Fair Network Payment Protocol

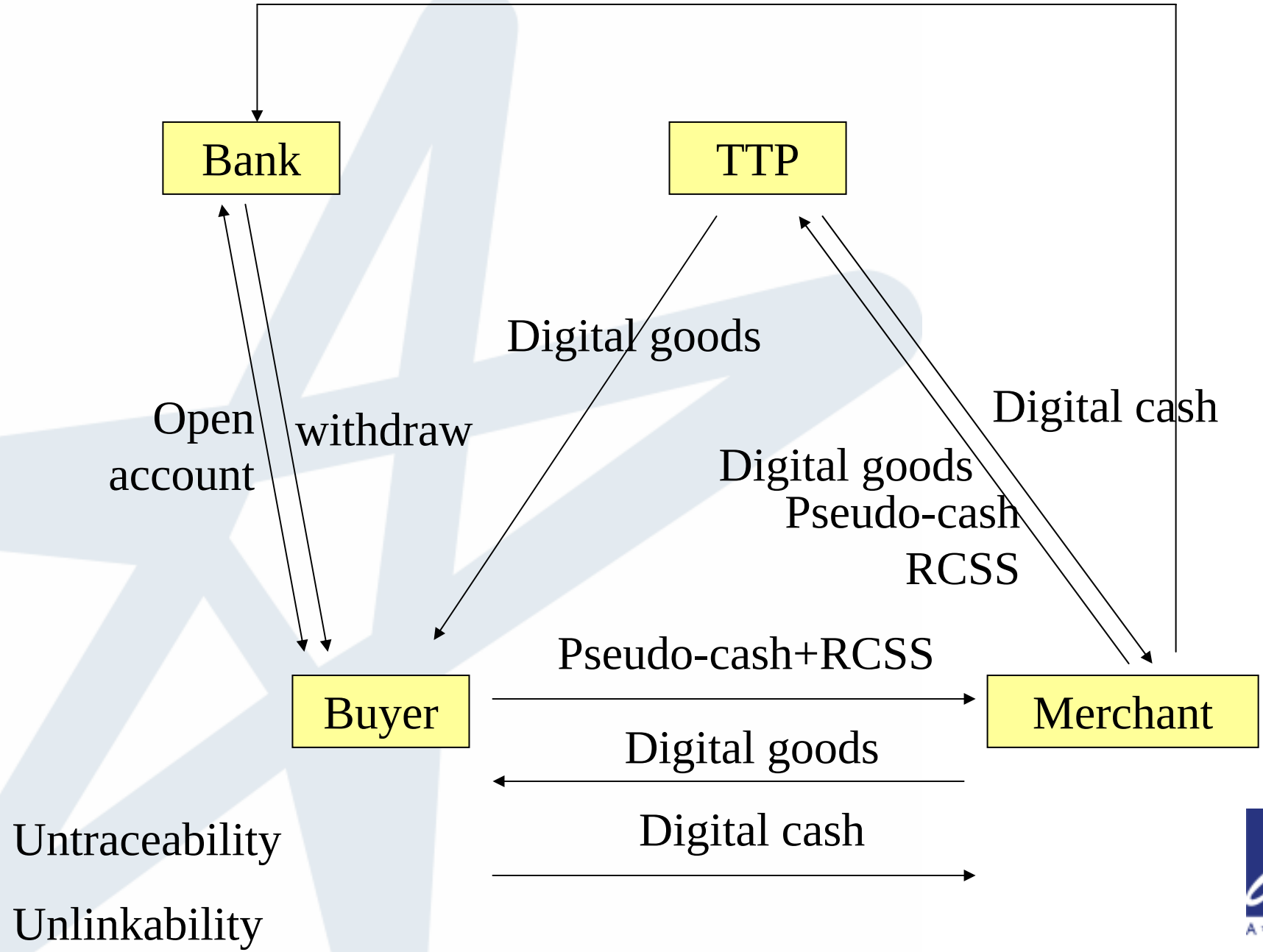
## The Main Building Block – RCSS

Restrictive confirmation signature scheme: A signature signed by S can be confirmed by C, and C can convince only some specified verifier V the the signature is valid and truly signed by S.

$$\mathrm{Sign}_{\mathrm{RCSS}}(S, C, V, m)$$

A*STAR I²R

# Untraceable Fair Network Payment Protocol

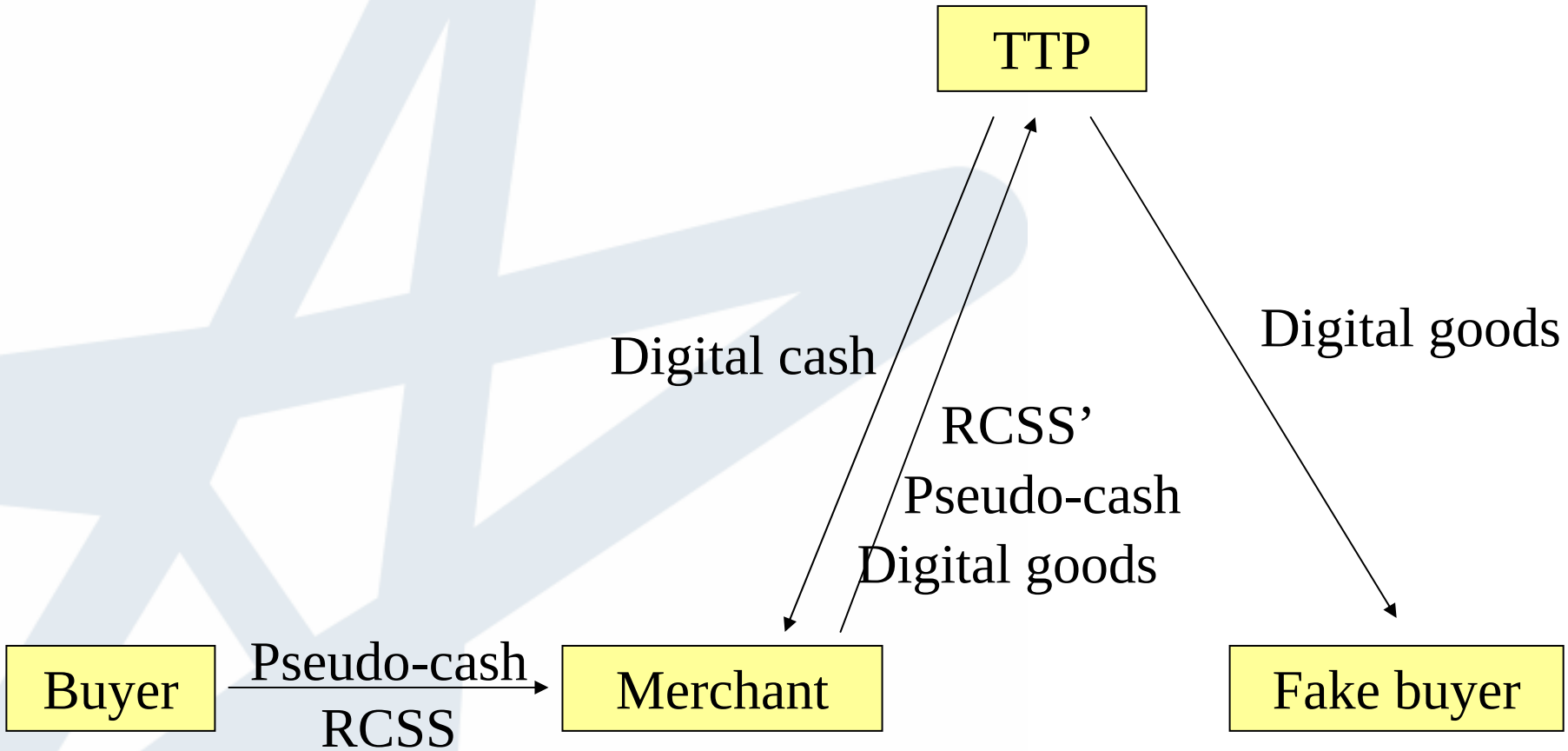



Untraceability

Unlinkability

A*STAR I²R

# Untraceable Fair Network Payment Protocol



# About the Security

The protocol is secure if the system contains only one buyer. It is not secure if there are multiple buyers, especially when a merchant collude with some buyer. Not secure in the sense that untraceability, unlinkability and fairness cannot be satisfied simultaneously

# 6 fair exchange of digital signature schemes – ACM CCS'99

- Two of them are not secure (fairness can be breached)
- The attack shares the same principle
- Key point: Vef(m, X, Y, PK)=1
- Normal security definition: difficult to find X,Y; or X; or Y.
- X, m➔Y, PK not necessarily hard

A*STAR I²R

Schnorr signature:

$y=g^x \bmod p$, where y is PK and x is SK

A signature (s,e) on m under y satisfies

$$e=H(m||g^s y^{-e})$$

It's hard to find such (s,e) without x.

But we can find e' and y' different from e and y such that

$$e'=H(m||g^s y'^{-e'})$$

For random t, set $e'=H(m||g^s g^t)$, $x'=-t/e'$, $y'=g^{x'}$

ElGanmal signature:

$y=g^x \bmod p$, where y is PK and x is SK

A signature (s,r) on m under y satisfies

$$g^s=r^{H(m)}y^r$$

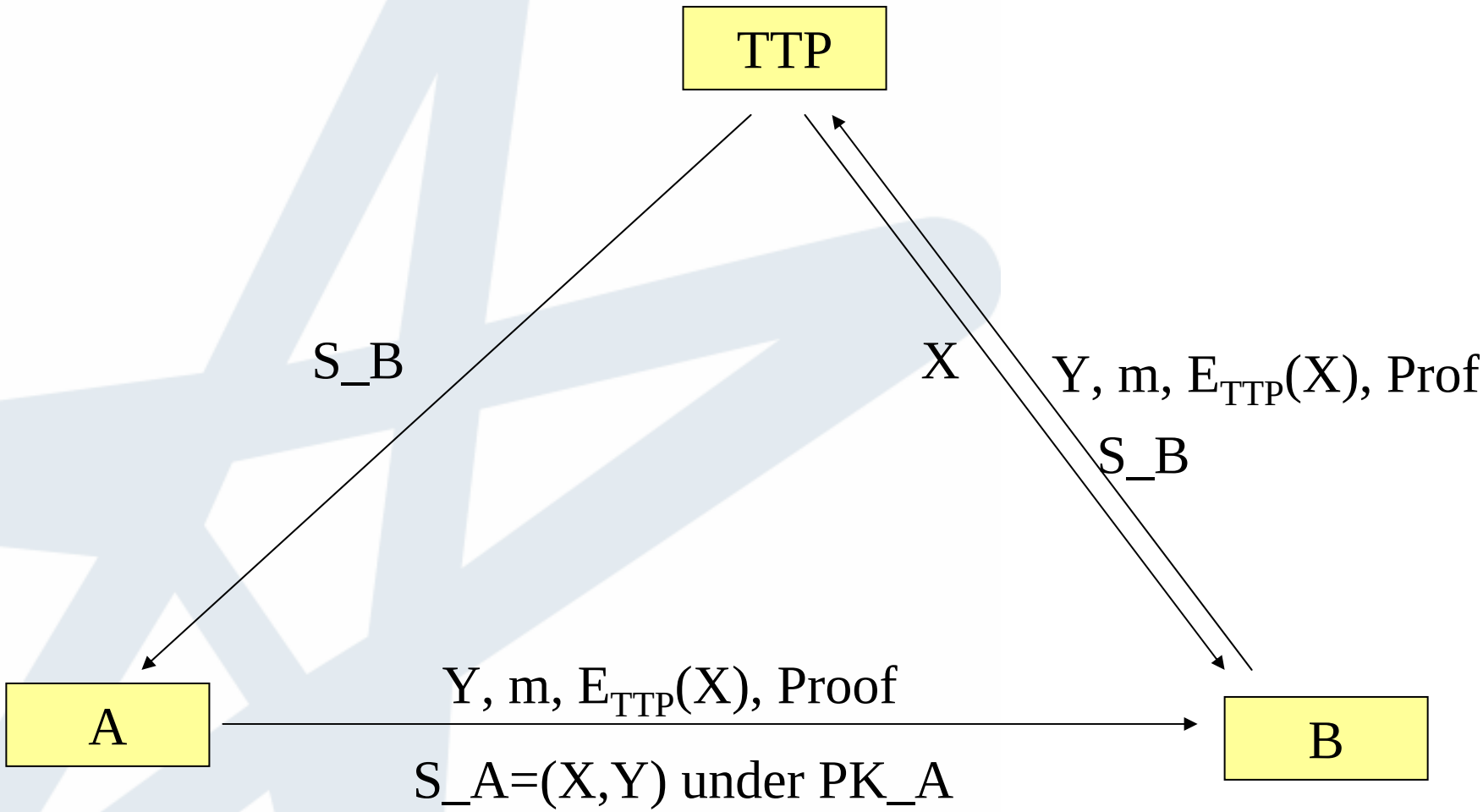
It's hard to find such (s,r) without x.

But we can find r' and y' different from r and y such that

$$g^s=r'^{H(m)}y'^{r'}$$

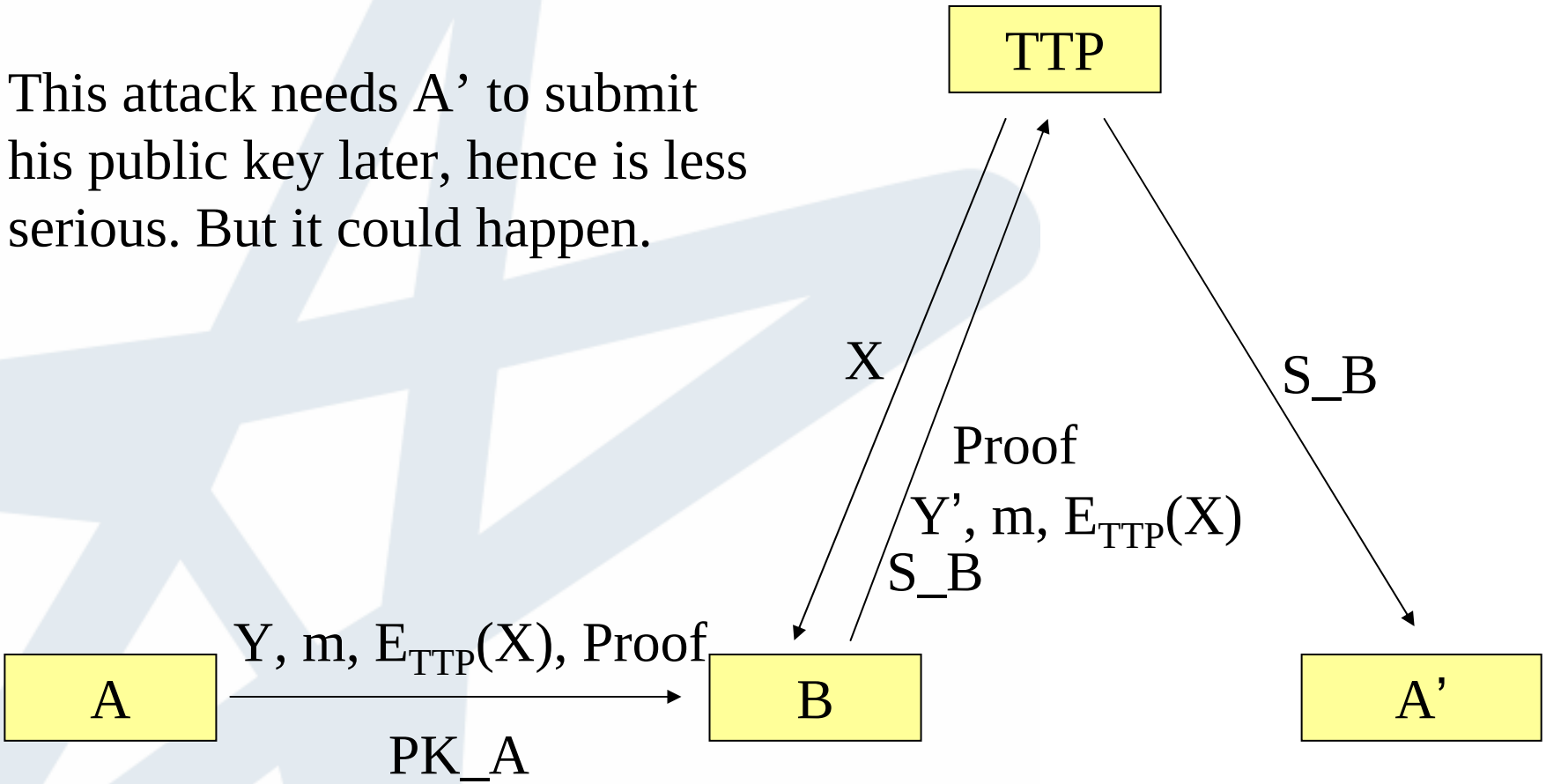
For random t, set $r'=g^{(s-t)/H(m)}$, $x'=t/r'$, $y'=g^{x'}$

For some signature schemes, given a signature *sign* under a public key *PK*,it is easy to generate a public key *PK'* and a signature *sign'* such that *sign'* shares a same component with *sign*.


TTP
S_B
X
Y, m, E_TTP(X), Prof
S_B
A
Y, m, E_TTP(X), Proof
B
S_A=(X,Y) under PK_A

# Colluding Attack

This attack needs A' to submit his public key later, hence is less serious. But it could happen.



# Remarks

- If m already includes the ID of A (or A's PK), the attack doesn't work. But TTP must check the semantics of m, which is unlikely possible.
- A simple remedy is to include A or A's public key in the Proof.

  $Proof=EQ\_DLOG(m||g^x, g'^x; g, g')$

  $Proof=EQ\_DLOG(PK_A||m||g^x, g'^x; g, g')$
- Security is very sensitive, can be affected by a small change. The engineers implementing a secure protocol should be educated.

# Thank you

# Q & A

A*STAR I²R