Round Optimal Blind Signatures

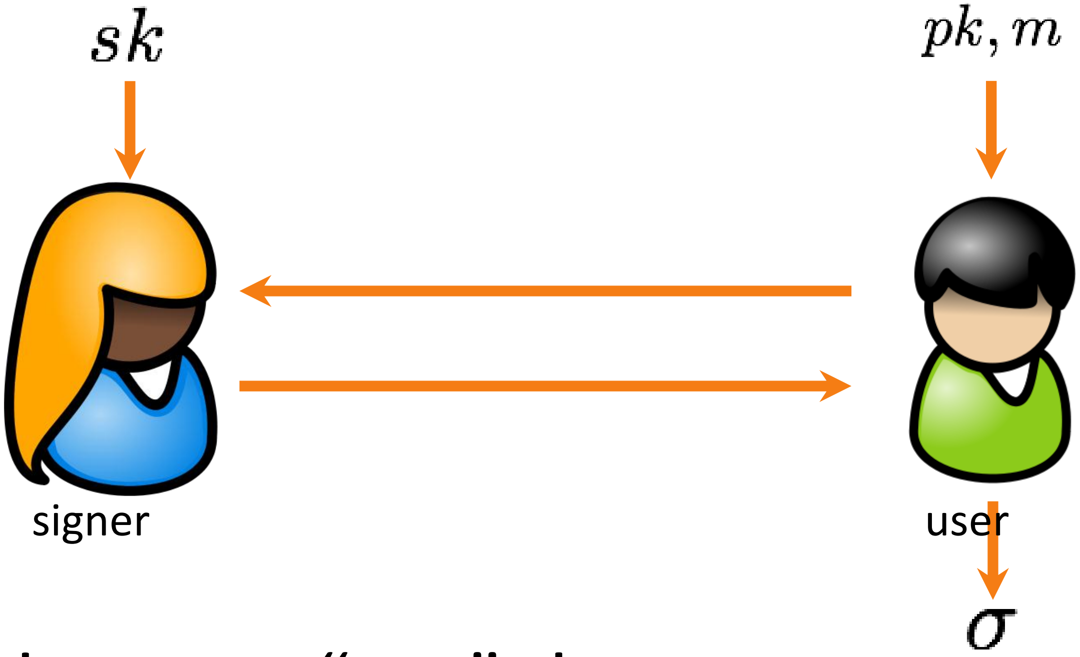
Sanjam Garg Vanishree Rao Amit Sahai
UCLA

Dominique Schroeder* Dominique Unruh
University of Maryland University of Tartu

(http://eprint.iacr.org/2011/264)

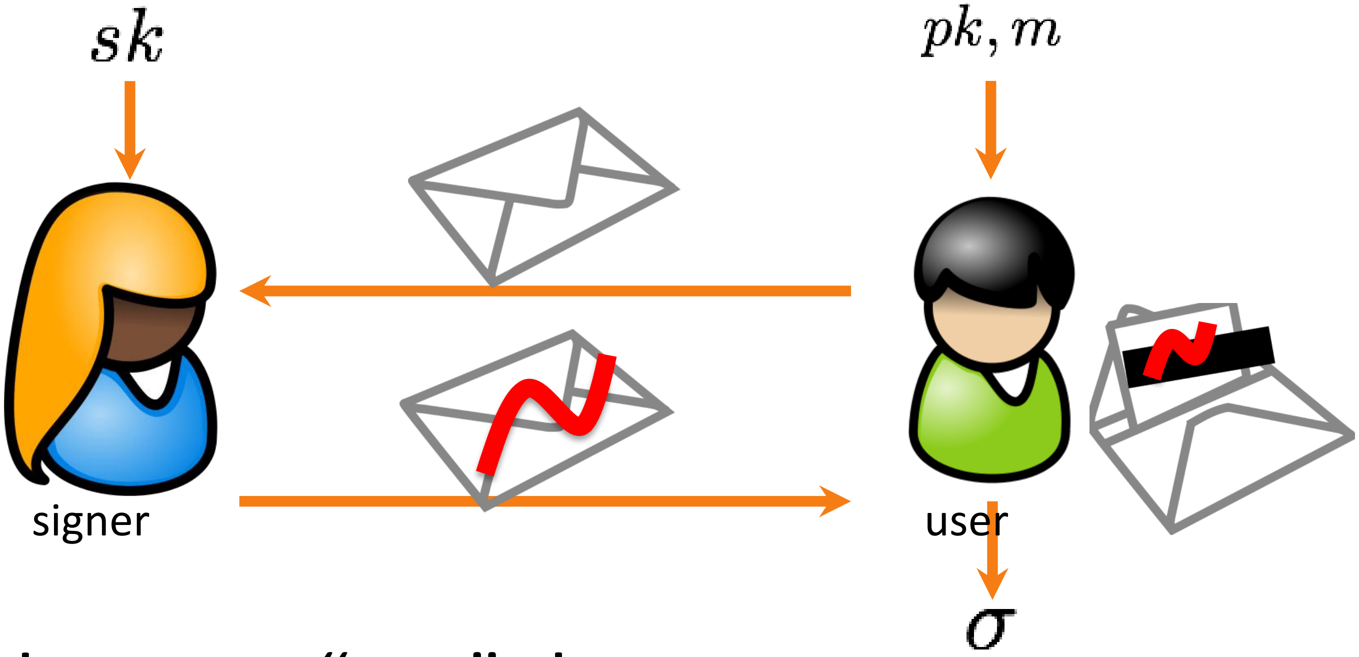
*Postdoctoral Fellow of the DAAD

Blind signatures [C85]



- Signer does not "see" the message m
- User cannot produce more signatures then # interactions

Blind signatures [C85]



- Signer does not "see" the message m
- User cannot produce more signatures then # interactions

Applications

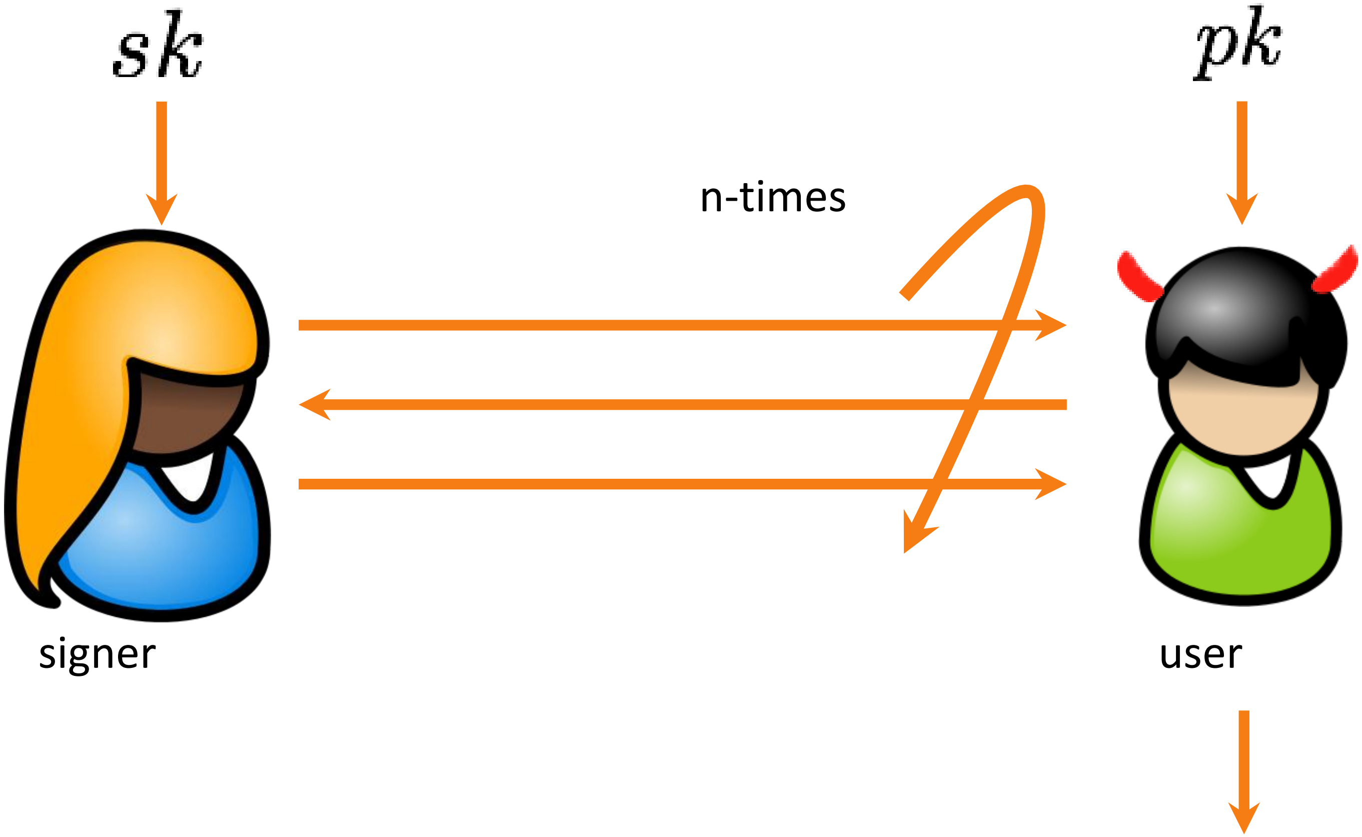
- eCash
- eVoting
  - User cannot vote for an additional candidate (unforgeability), voting agency does not see the vote (blindness)
  - FIFA world soccer cup selected in 2002 Most Valuable Player using Votopia
- Anonymous credentials
  - Microsoft U-PROVE
  - National Strategy for Trusted Identities in Cyberspace - NISTIC

What’s next?

- Security model
- Our contribution
- Related work
- Construction
- Relation to FS [10]

Security model

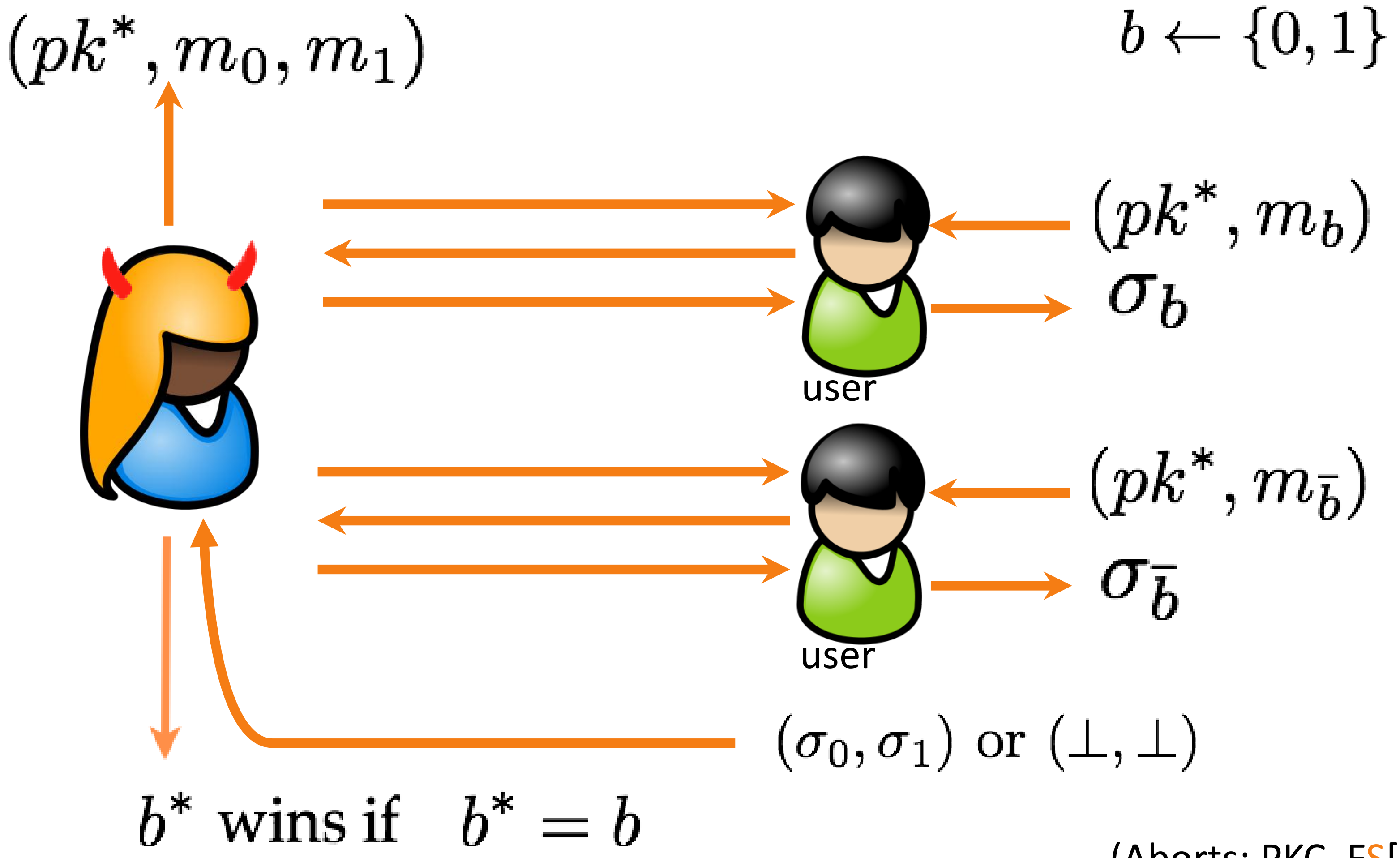
Unforgeability [JLO97,PS00]



$$m_i \neq m_j \;,\; (m_1,\sigma_1),\ldots,(m_{n+1},\sigma_{n+1})$$

Security model

Blindness [JLO97,PS00]



(pk^*, m_0, m_1)

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

(pk^*, m_b)

σ_b

user

$(pk^*, m_{\bar{b}})$

$\sigma_{\bar{b}}$

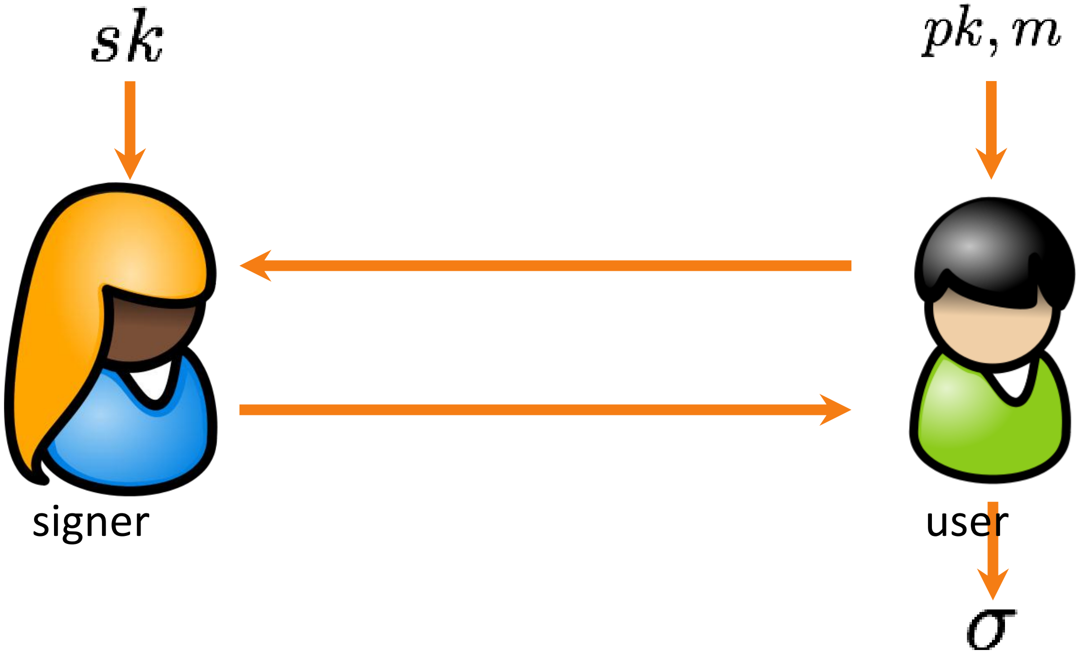
user

(σ_0, σ_1) or $(\perp, \perp)$

b^* wins if $b^* = b$

(Aborts: PKC, FS[09])

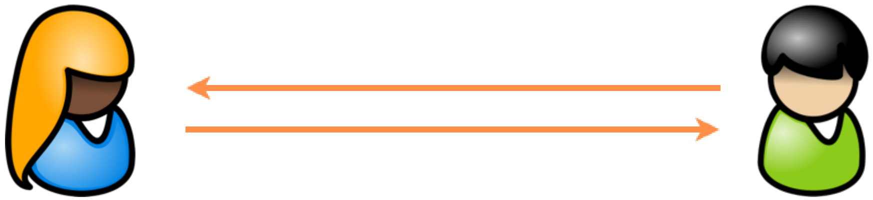
Simple question:



Two moves?

Known constructions

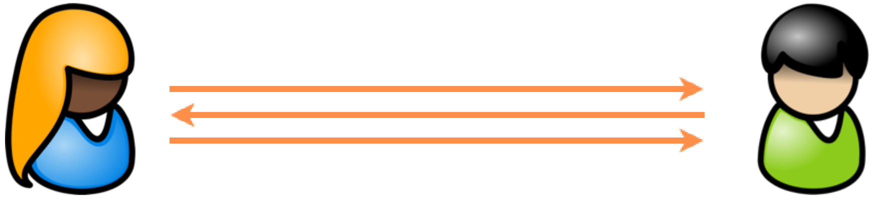
over 80 papers published



2 moves (optimal):

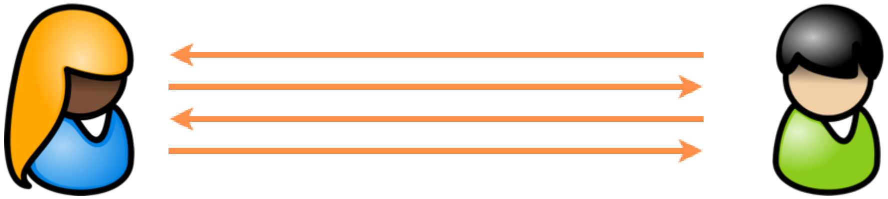
Chaum, Boldyreva:
interactive assumption, ROM

Fischlin: CRS



3 moves:

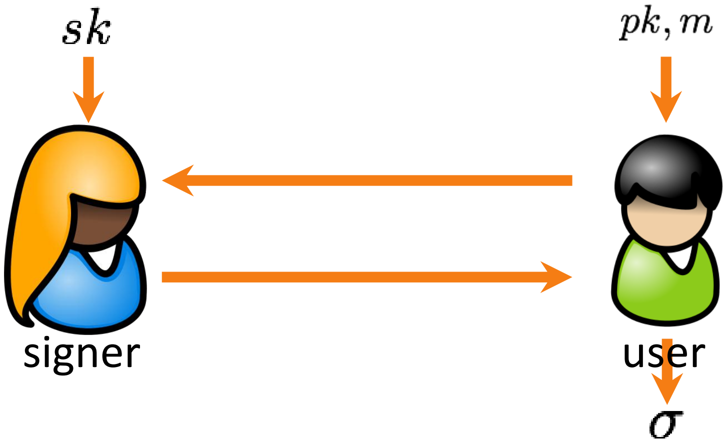
Pointcheval Stern,
Abe ROM



4 moves:

Okamoto TCC06

Simple question:



Reduce the round complexity of a known scheme.

Prove the security of a known two move scheme in the standard model.

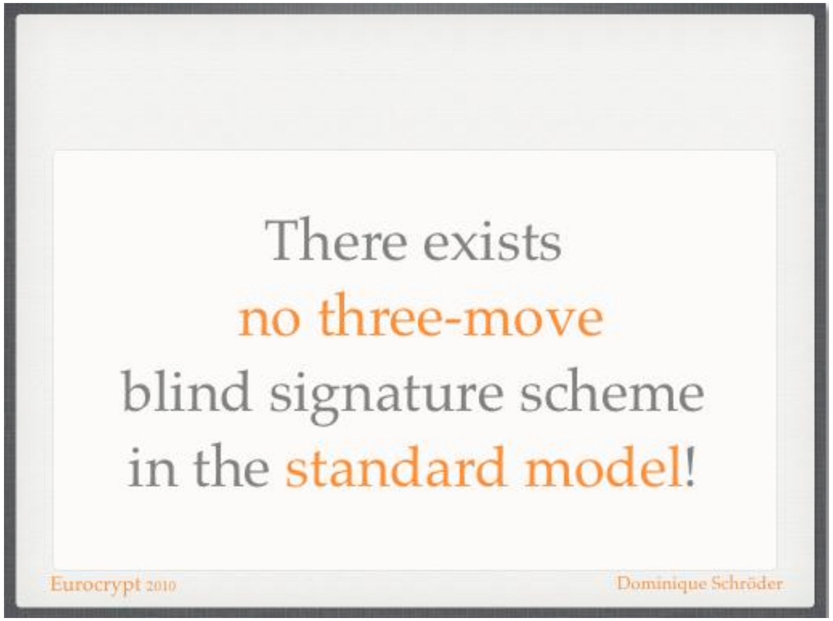
Construct a completely new scheme.

Simple question:

Prove the security of a known two move scheme in the standard model.

Fischlin, S[FS10]:

No security reduction for one of the known two/three moves schemes to any non-interactive problem in the standard model.



There exists
no three-move
blind signature scheme
in the standard model!

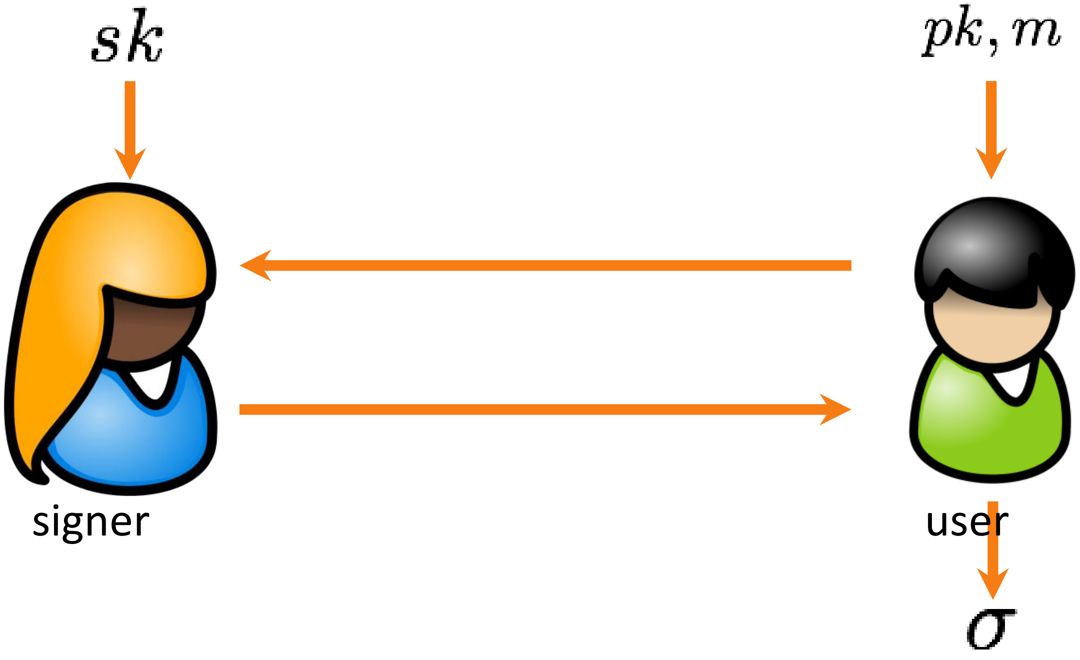
Eurocrypt 2010

Dominique Schröder

Extension: Pass (STOC 11): unique blind signature.

EUROCRYPT 2010

Simple question:



sk

pk, m

signer

user

σ

Two moves?

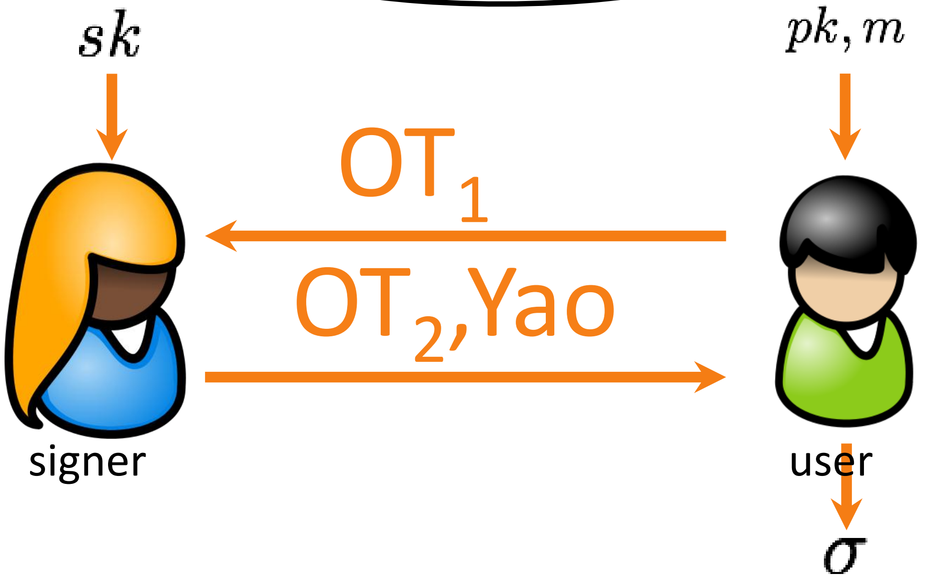
(Caution: actual results may vary)

First stab

- Idea: Use Yao's garbled circuit with OT
- Yao allows private evaluation of any general circuit
  - Consider the signature evaluation circuit
- We also need a 2 round OT protocol [NP01, AIR01]
  - This protocol is not simulatable
  - Computational security for sender and statistical security for receiver

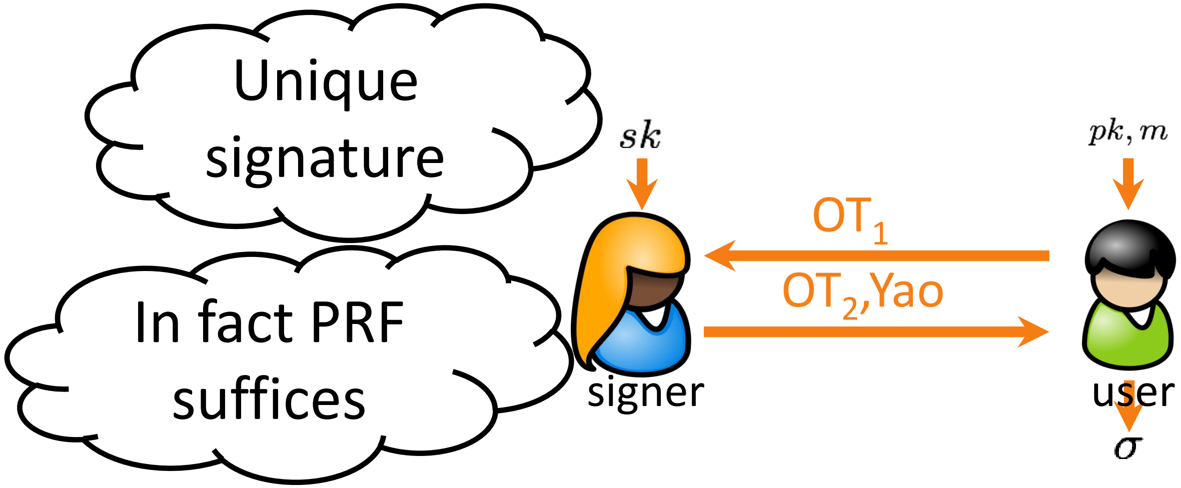
First stab

Need to make it fully secure.



Problem: 1) Yao is only semi-honest secure and 2) OT is not simulatable

Cheating signer



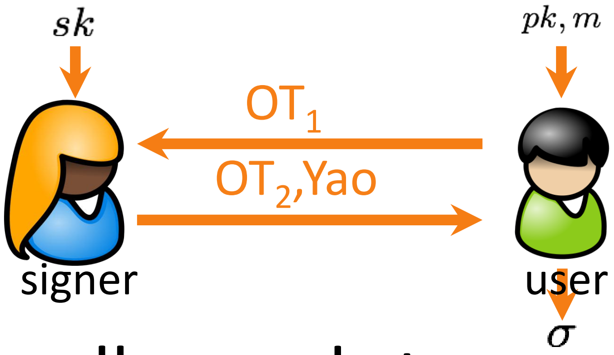
Unique signature

In fact PRF suffices

- What can a cheating signer do to break blindness?
  - Encode any arbitrary function inside the Yao's garbled circuit.
  - Manipulate the randomness used in signing to break blindness

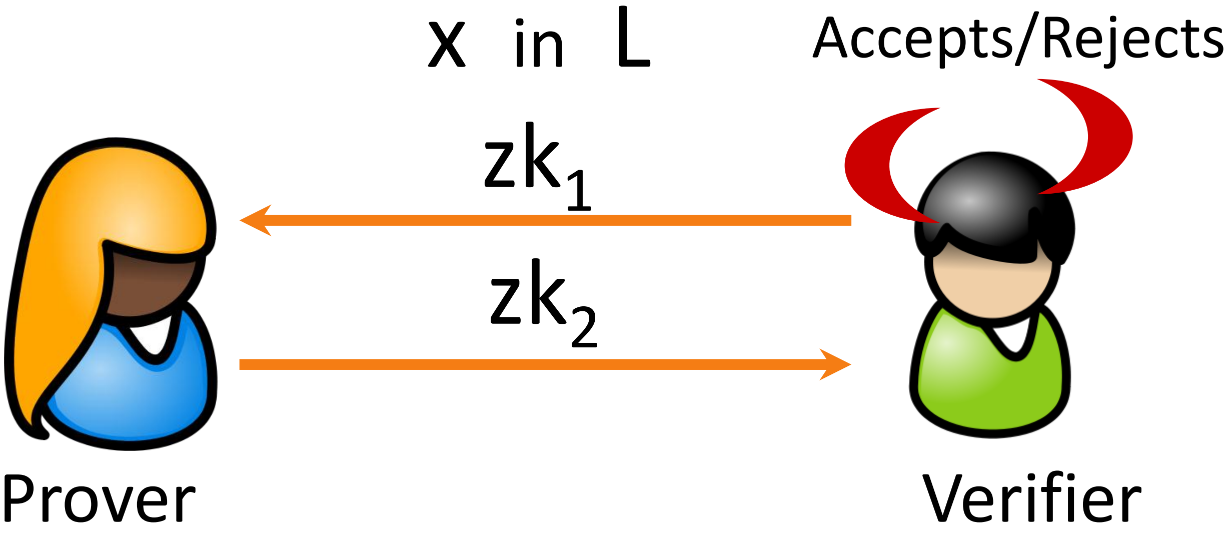
More fundamental issue

Enforcing correct behavior



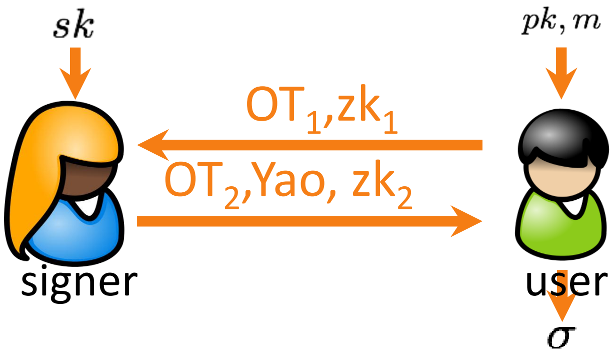
- Signer additionally needs to prove correctness of its actions.
- Idea: Use a proof protocol
  - What proof protocol can be used?
  - Standard ZK requires 3 rounds

Super-Poly Simulation based ZK [Pass03]



- Zero Knowledge – For every cheating verifier V there exists a simulator S running in super poly time that can simulate the view of the verifier

Protocol so far



- We have limited the signer in cheating by
  - Using deterministic signatures
  - Enforcing honest behavior by a Zero Knowledge protocol
- Have we solved the problem of cheating signer?
  - Subtle issue remains: in proof of security, need to extract signatures
  - Solution: Use super-poly-time extraction
  - But can avoid the use of super-poly-time by specific rewinding technique (see paper)

Cheating user – arguing unforgeability

- Simulator simulating the view of the verifier is super-polynomial
- Deal with this by using signature scheme that is unforgeable even by an adversary secure against super-poly time adversaries. (complexity leveraging)
- This allows us to argue unforgeability.

Relation to FS[10]

- FS[10] proved impossibility of three round blind signature schemes
- Restricted to blind signature schemes with some technical properties
  - Blindness holds with respect to a forgery oracle as well
- Our scheme avoids this, but still achieves full security.

Open Problems

- Improvements in terms of assumptions
  - We require sub-exponentially hard OWFs, trapdoor permutations and DDH

    (Impossible from OWP: Katz, S, Yerukhimovich, TCC 2011)

- Efficient constructions

Thanks

Vanishree Rao

Amit Sahai

Dominique Unruh