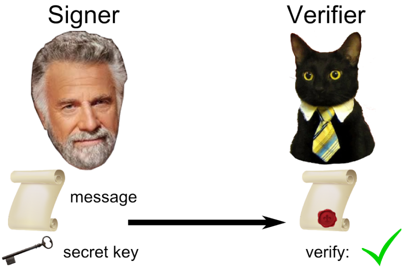
The Fiat–Shamir Transformation in a Quantum World

Özgür Dagdelen Marc Fischlin Tommaso Gagliardoni

CASED and EC-SPRIDE and TU Darmstadt

Asiacrypt'13, December 4th, 2013
Bengaluru, India

Signature scheme



Signer

Verifier

message

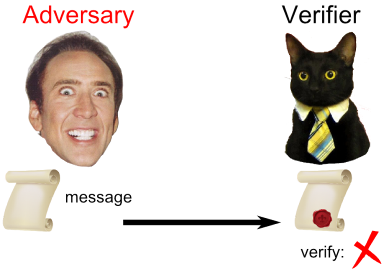
secret key

verify: ✓

Signature scheme

Security:

no efficient adversary can successfully forge a valid signature without knowing the secret key



Adversary

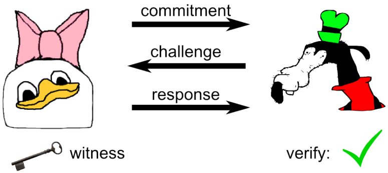
Verifier

message

verify: ✗

Identification scheme

Prover Verifier



commitment

challenge

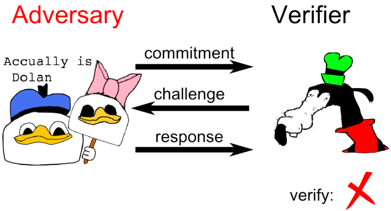
response

witness

verify: ✓

statement: "I am Daisy"

Identification scheme



Adversary

Verifier

commitment

challenge

response

verify: ✗

statement: "I am Daisy"

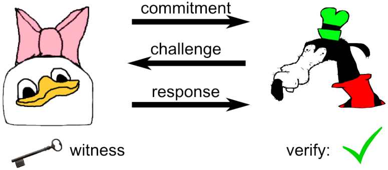
Security:

no efficient adversary can successfully prove identity without valid witness

Identification scheme

Prover

Verifier



commitment

challenge

response

witness

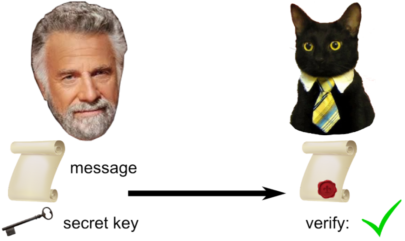
verify: ✓

statement: "I am Daisy"

Signature scheme

Signer

Verifier



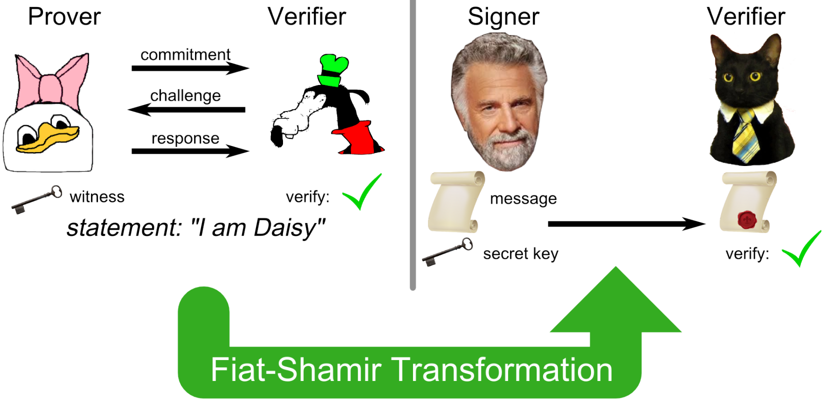
message

secret key

verify: ✓

Identification scheme

Signature scheme



Prover

Verifier

commitment

challenge

response

witness

verify: ✓

statement: "I am Daisy"

Signer

Verifier

message

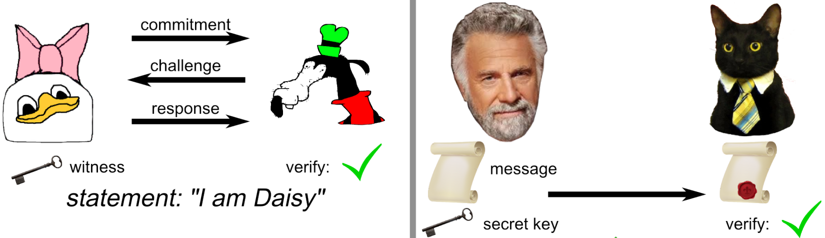
secret key

verify: ✓

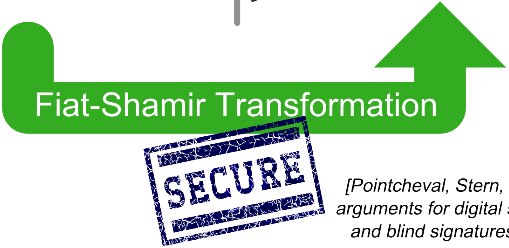
Fiat-Shamir Transformation

Identification scheme

Signature scheme

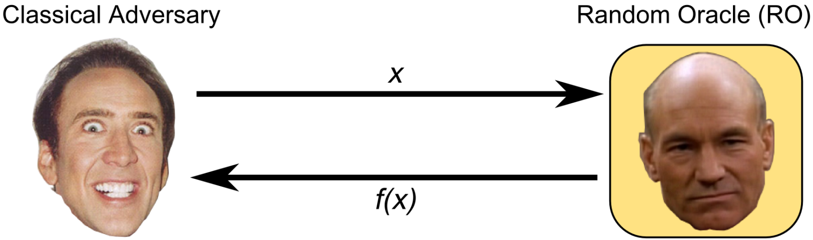


statement: "I am Daisy"



[Pointcheval, Stern, "Security arguments for digital signatures and blind signatures", 2000]
(ROM)

Classical VS Quantum



Classical Adversary

Random Oracle (RO)

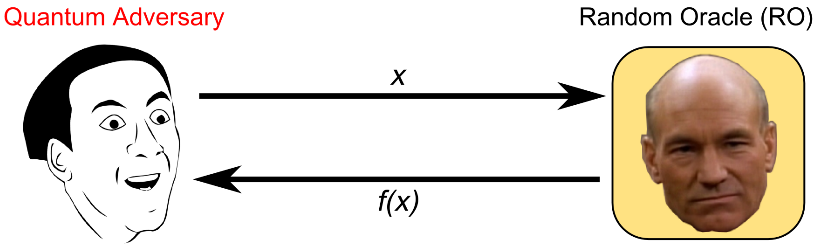
x

$f(x)$

Fiat-Shamir Transformation

SECURE

Classical VS Quantum



Quantum Adversary

Random Oracle (RO)

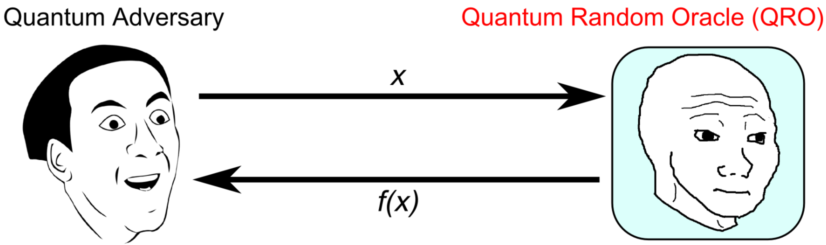
x

$f(x)$

Fiat-Shamir Transformation

SECURE

Classical VS Quantum



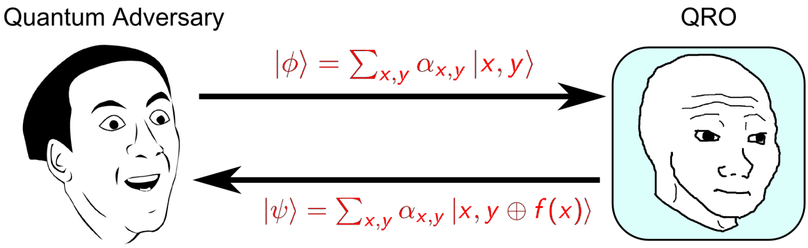
Quantum Adversary

Quantum Random Oracle (QRO)

Fiat-Shamir Transformation

SECURE

Classical VS Quantum



Quantum Adversary

QRO

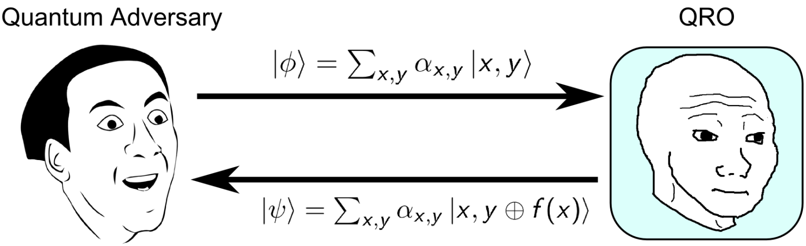
$|\phi\rangle = \sum_{x,y} \alpha_{x,y} |x, y\rangle$

$|\psi\rangle = \sum_{x,y} \alpha_{x,y} |x, y \oplus f(x)\rangle$

Fiat-Shamir Transformation

SECURE

Classical VS Quantum



$|\phi\rangle = \sum_{x,y} \alpha_{x,y} |x, y\rangle$

$|\psi\rangle = \sum_{x,y} \alpha_{x,y} |x, y \oplus f(x)\rangle$

Fiat-Shamir Transformation

Security in the QROM

Problem: in the QROM* many of the techniques we use for security proofs do not usually work:

[Boneh,Dagdelen,Fischlin,Lehmann,Schaffner,Zhandry,'Random Oracles in a Quantum World'*,2010]

Security in the QROM

Problem: in the QROM* many of the techniques we use for security proofs do not usually work:

- *'let us perform operation U over two copies of the variable...'*

[Boneh,Dagdelen,Fischlin,Lehmann,Schaffner,Zhandry,'Random Oracles in a Quantum World'*,2010]

Security in the QROM

Problem: in the QROM* many of the techniques we use for security proofs do not usually work:

- *'let us perform operation U over two copies of the variable...'*
- *'query after query, let's build a table with all the outcomes...'*

[Boneh,Dagdelen,Fischlin,Lehmann,Schaffner,Zhandry,'Random Oracles in a Quantum World'*,2010]

Security in the QROM

Problem: in the QROM* many of the techniques we use for security proofs do not usually work:

- *'let us perform operation U over two copies of the variable...'*
- *'query after query, let's build a table with all the outcomes...'*
- *machine state snapshots*

[Boneh,Dagdelen,Fischlin,Lehmann,Schaffner,Zhandry,'Random Oracles in a Quantum World'*,2010]

Security in the QROM

Problem: in the QROM* many of the techniques we use for security proofs do not usually work:

- *'let us perform operation U over two copies of the variable...'*
- *'query after query, let's build a table with all the outcomes...'*
- *machine state snapshots*
- *'normal' rewinding*

[Boneh,Dagdelen,Fischlin,Lehmann,Schaffner,Zhandry,'Random Oracles in a Quantum World'*,2010]

Security in the QROM

Problem: in the QROM* many of the techniques we use for security proofs do not usually work:

- *'let us perform operation U over two copies of the variable...'*
- *'query after query, let's build a table with all the outcomes...'*
- *machine state snapshots*
- *'normal' rewinding*
- *Forking Lemma (used to prove security of Fiat–Shamir)*

[Boneh,Dagdelen,Fischlin,Lehmann,Schaffner,Zhandry,'Random Oracles in a Quantum World'*,2010]

Security in the QROM

Problem: in the QROM* many of the techniques we use for security proofs do not usually work:

- *'let us perform operation U over two copies of the variable...'*
- *'query after query, let's build a table with all the outcomes...'*
- *machine state snapshots*
- *'normal' rewinding*
- *Forking Lemma (used to prove security of Fiat–Shamir)*

All these things do not work!

[Boneh,Dagdelen,Fischlin,Lehmann,Schaffner,Zhandry,'Random Oracles in a Quantum World'*,2010]

Security in the QROM

Problem: in the QROM* many of the techniques we use for security proofs do not usually work:

- *'let us perform operation U over two copies of the variable...'*
- *'query after query, let's build a table with all the outcomes...'*
- *machine state snapshots*
- *'normal' rewinding*
- *Forking Lemma (used to prove security of Fiat–Shamir)*

All these things do not work!

Open question

Is the Fiat–Transformation secure in the QROM?

[Boneh,Dagdelen,Fischlin,Lehmann,Schaffner,Zhandry,'Random Oracles in a Quantum World'*,2010]

Outline of our work

Impossibility result

For certain schemes, we use a **meta-reduction** to rule out the existence of (a large class of) possible security proofs.

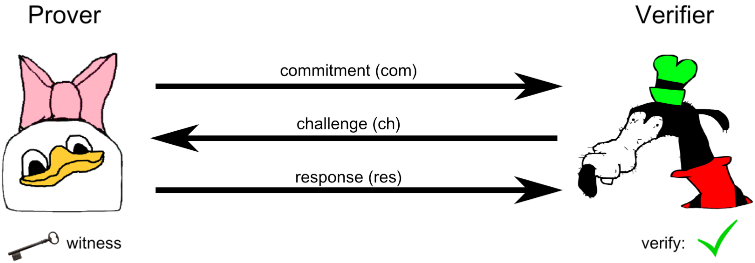
Positive result

For other schemes, we give a proof of security by defining and using **oblivious commitments**.

Secure instantiation

We provide a **generic patch** to harden existing schemes with a small overhead, and we give an **example instantiation** based on a recent lattice-based signature scheme.

Identification scheme



Prover

Verifier

commitment (com)

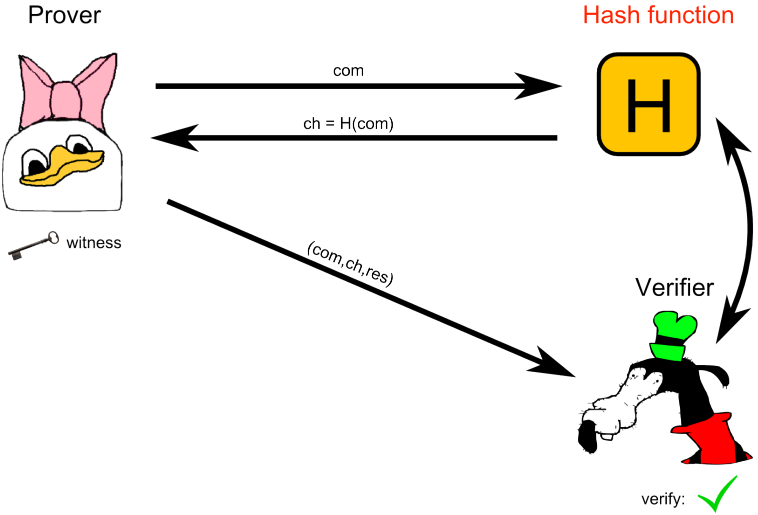
challenge (ch)

response (res)

witness

verify: ✓

Identification scheme



Prover

Hash function

com

ch = H(com)

H

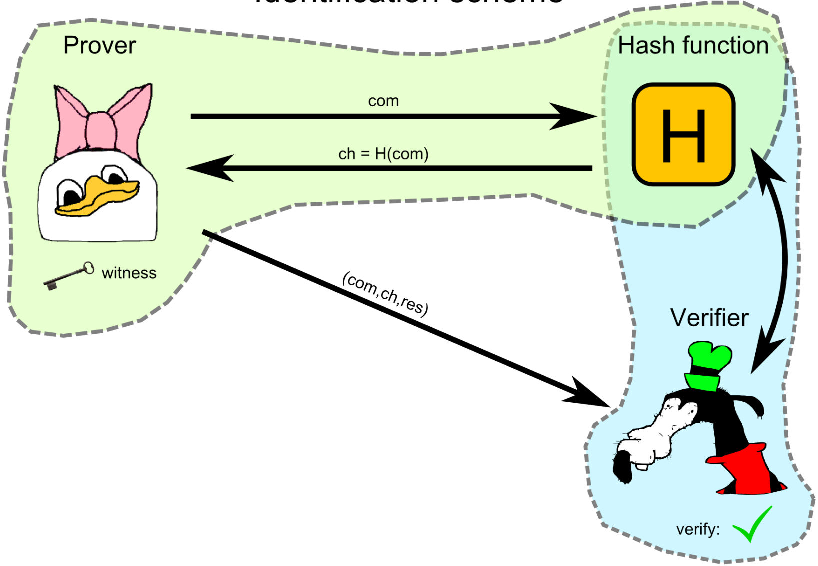
witness

(com,ch,res)

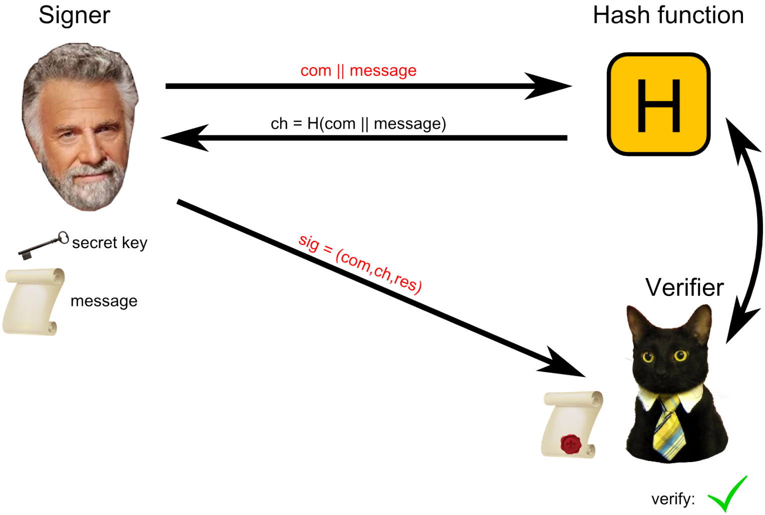
Verifier

verify: ✓

Identification scheme



Signature scheme



Signer

Hash function

com || message

ch = H(com || message)

H

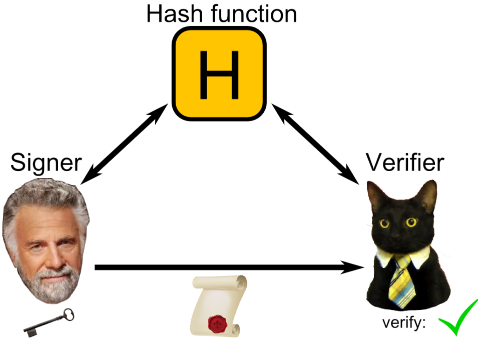
secret key

message

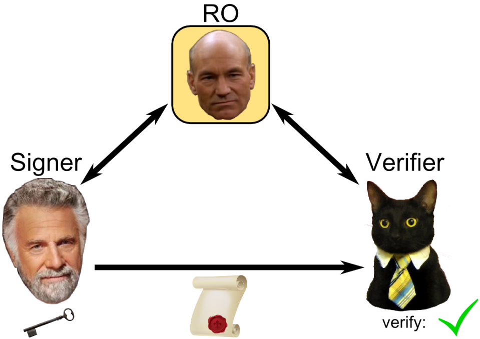
sig = (com,ch,res)

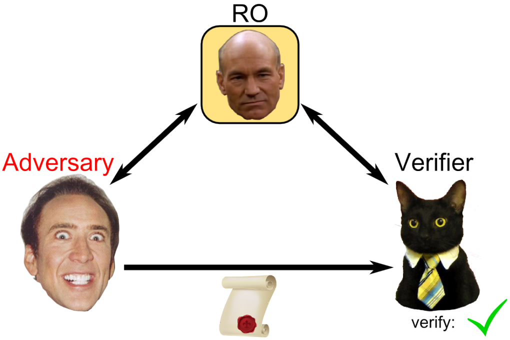
Verifier

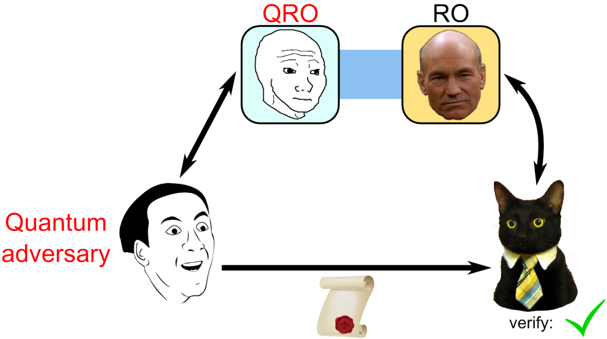
verify: ✓



Hash function
H
Signer
Verifier
verify: ✓


RO
Signer
Verifier
verify: ✓


RO
Adversary
Verifier
verify: ✓

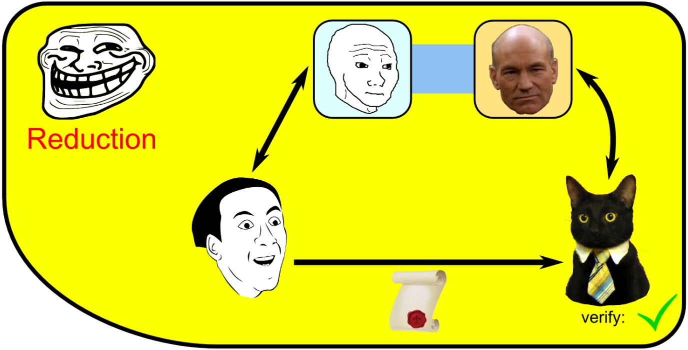


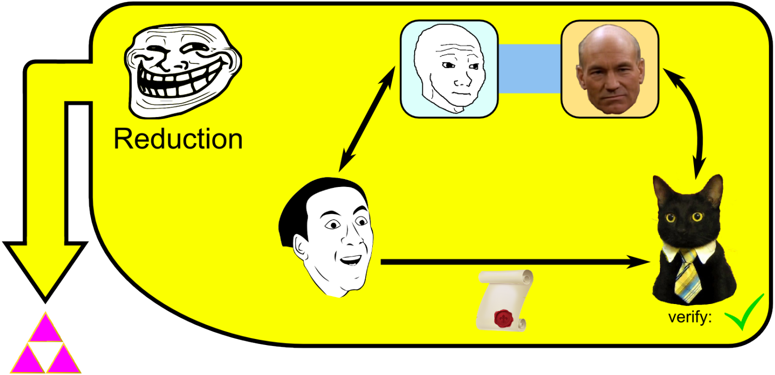
QRO

RO

Quantum adversary

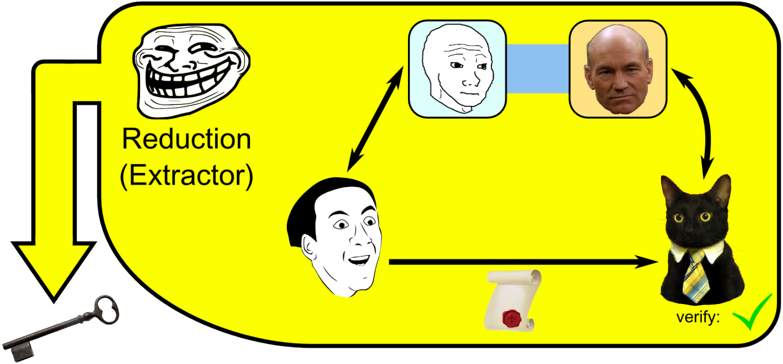
verify: ✓

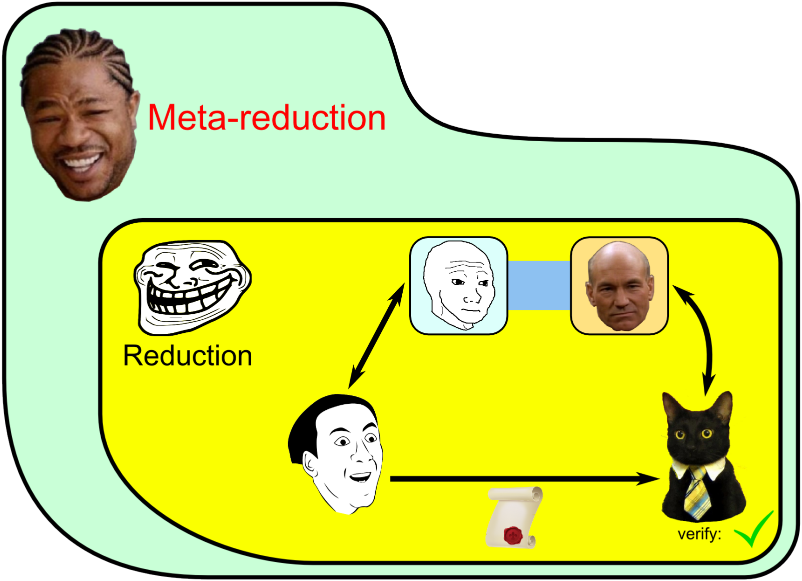

Reduction
verify: ✓



Reduction

verify: ✓

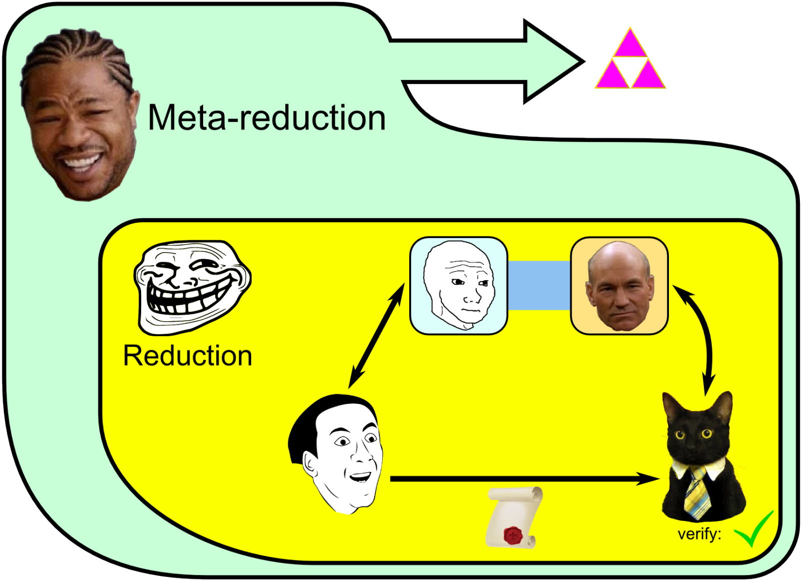

Reduction
(Extractor)
verify: ✓

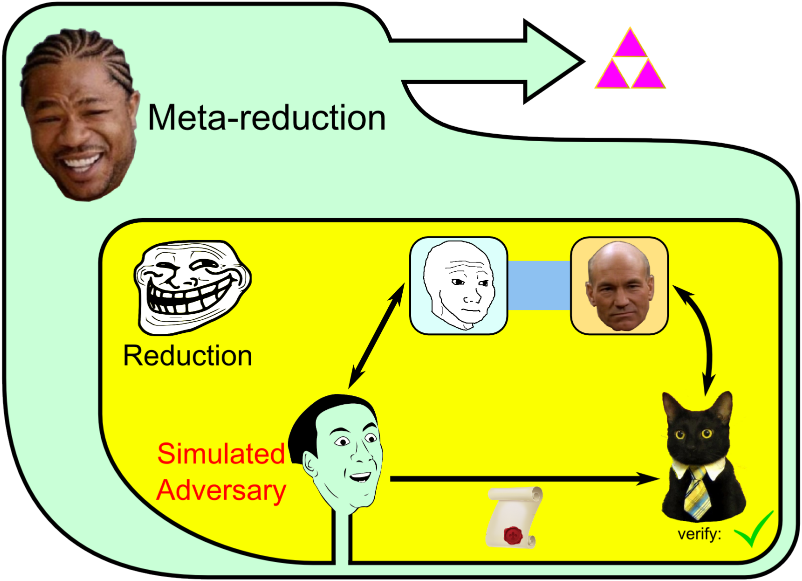


Meta-reduction

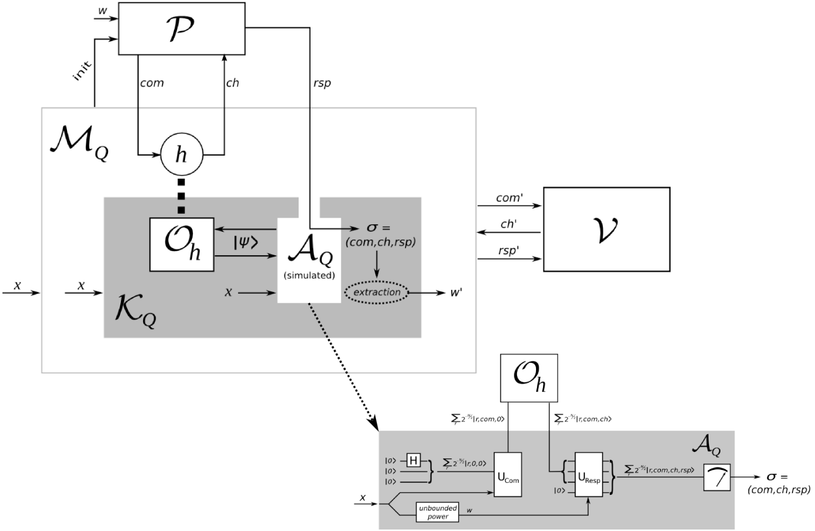
Reduction

verify: ✓


Meta-reduction
Reduction
verify: ✓


Meta-reduction
Reduction
Simulated Adversary
verify: ✓

Our Meta-Reduction



Impossibility result

Theorem:

No Fiat–Shamir signature scheme admits efficient black-box extractors, provided underlying identification scheme has:

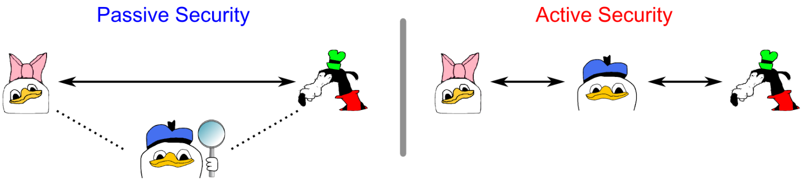
- **witness-independent commitments**
- **active security**

Impossibility result

Theorem:

No Fiat–Shamir signature scheme admits efficient black-box extractors, provided underlying identification scheme has:

- **witness-independent commitments**
- **active security**

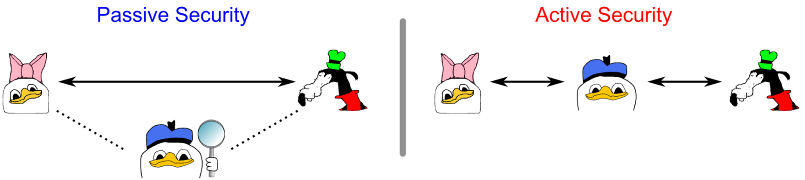


Impossibility result

Theorem:

No Fiat–Shamir signature scheme admits efficient black-box extractors, provided underlying identification scheme has:

- **witness-independent commitments**
- **active security**



Notice: **passive security** is enough to obtain secure signature schemes via the Fiat–Shamir transform.

Positive result

Idea

Remove active security from underlying identification scheme

Positive result

Idea

Remove active security from underlying identification scheme

Identification schemese with **Oblivious Commitments**

Positive result

Idea

Remove active security from underlying identification scheme

Identification schemese with **Oblivious Commitments**

with normal commitment:

Positive result

Idea

Remove active security from underlying identification scheme

Identification schemese with **Oblivious Commitments**

with normal commitment:

w,x

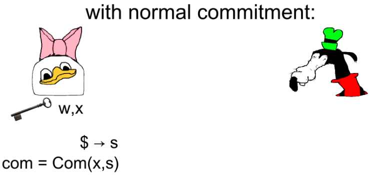
$ → s

Positive result

Idea

Remove active security from underlying identification scheme

Identification schemese with **Oblivious Commitments**



with normal commitment:

w,x

$ → s

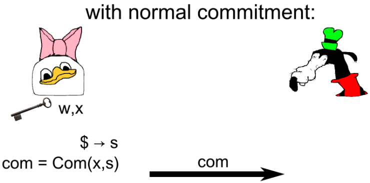
com = Com(x,s)

Positive result

Idea

Remove active security from underlying identification scheme

Identification schemese with **Oblivious Commitments**



with normal commitment:

w,x

$ → s

com = Com(x,s)

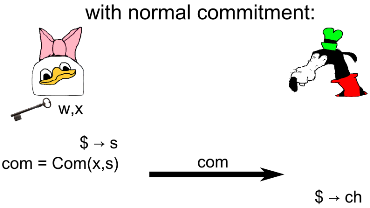
com

Positive result

Idea

Remove active security from underlying identification scheme

Identification schemese with Oblivious Commitments



with normal commitment:

w,x

$ → s

com = Com(x,s)

com

$ → ch

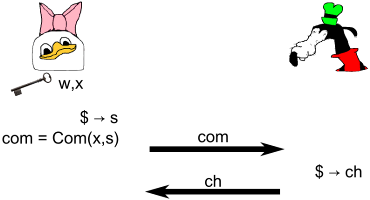
Positive result

Idea

Remove active security from underlying identification scheme

Identification schemese with **Oblivious Commitments**

with normal commitment:



w,x

$ → s
com = Com(x,s)

com →

← ch

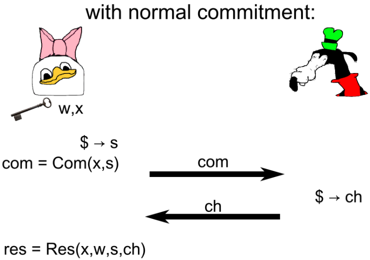
$ → ch

Positive result

Idea

Remove active security from underlying identification scheme

Identification schemese with Oblivious Commitments



with normal commitment:

w,x

$ → s

com = Com(x,s)

com →

$ → ch

← ch

res = Res(x,w,s,ch)

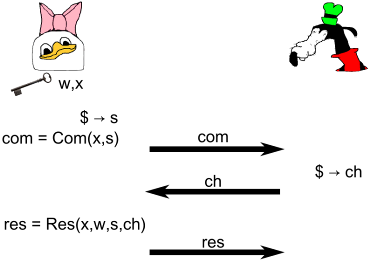
Positive result

Idea

Remove active security from underlying identification scheme

Identification schemese with **Oblivious Commitments**

with normal commitment:



w,x

$\$ \to s$

com = Com(x,s)

com

$\$ \to ch$

ch

res = Res(x,w,s,ch)

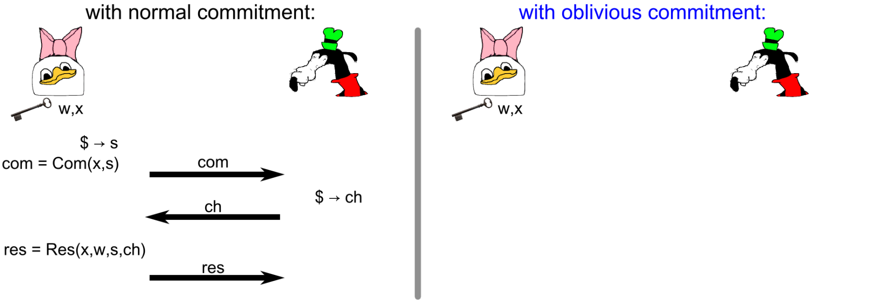
res

Positive result

Idea

Remove active security from underlying identification scheme

Identification schemese with **Oblivious Commitments**



with normal commitment:

w,x

$ → s

com = Com(x,s)

com

$ → ch

ch

res = Res(x,w,s,ch)

res

with oblivious commitment:

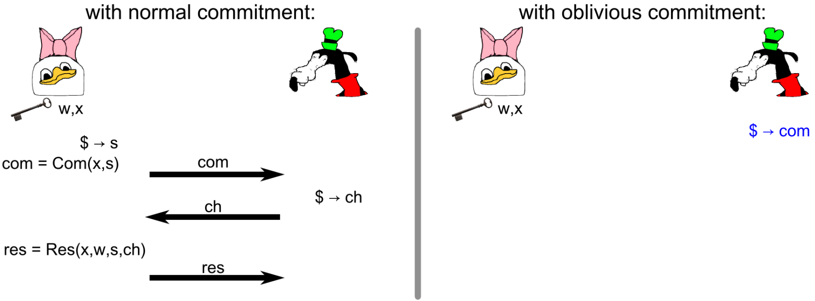
w,x

Positive result

Idea

Remove active security from underlying identification scheme

Identification schemese with **Oblivious Commitments**



with normal commitment:

w,x

$ → s

com = Com(x,s)

com →

$ → ch

← ch

res = Res(x,w,s,ch)

res →

with oblivious commitment:

w,x

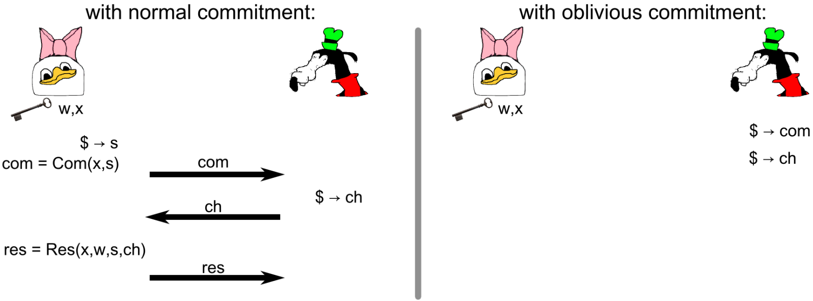
$ → com

Positive result

Idea

Remove active security from underlying identification scheme

Identification schemese with **Oblivious Commitments**



with normal commitment:

w,x

$ → s

com = Com(x,s)

com

$ → ch

ch

res = Res(x,w,s,ch)

res

with oblivious commitment:

w,x

$ → com

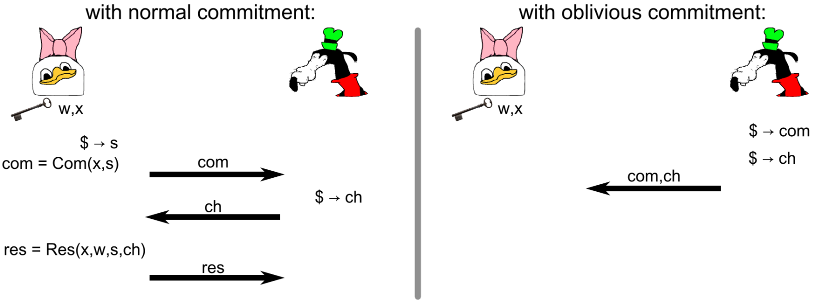
$ → ch

Positive result

Idea

Remove active security from underlying identification scheme

Identification schemese with Oblivious Commitments



with normal commitment:

w,x

$ → s

com = Com(x,s)

com

$ → ch

ch

res = Res(x,w,s,ch)

res

with oblivious commitment:

w,x

$ → com

$ → ch

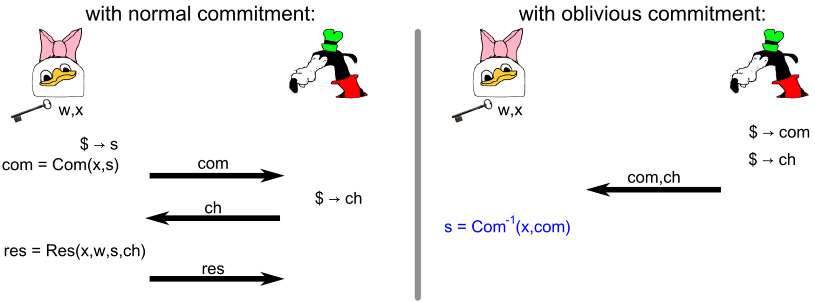
com,ch

Positive result

Idea

Remove active security from underlying identification scheme

Identification schemese with Oblivious Commitments



with normal commitment:

w,x

$\$ \rightarrow s$

com = Com(x,s)

com

ch

$\$ \rightarrow ch$

res = Res(x,w,s,ch)

res

with oblivious commitment:

w,x

$\$ \rightarrow com$

$\$ \rightarrow ch$

com,ch

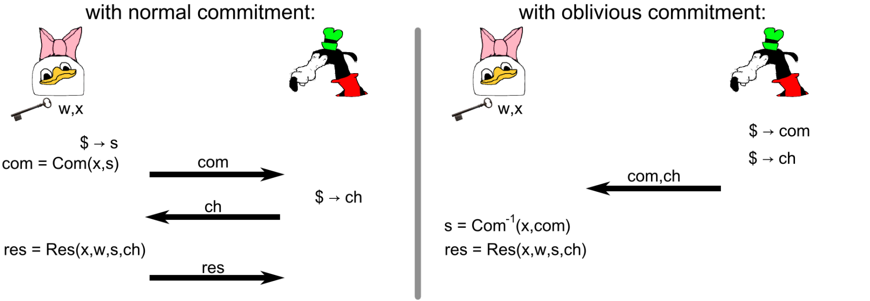
$s = Com^{-1}(x,com)$

Positive result

Idea

Remove active security from underlying identification scheme

Identification schemese with **Oblivious Commitments**



with normal commitment:

w,x

$ → s

com = Com(x,s)

com

ch

$ → ch

res = Res(x,w,s,ch)

res

with oblivious commitment:

w,x

$ → com

$ → ch

com,ch

s = Com^{-1}(x,com)

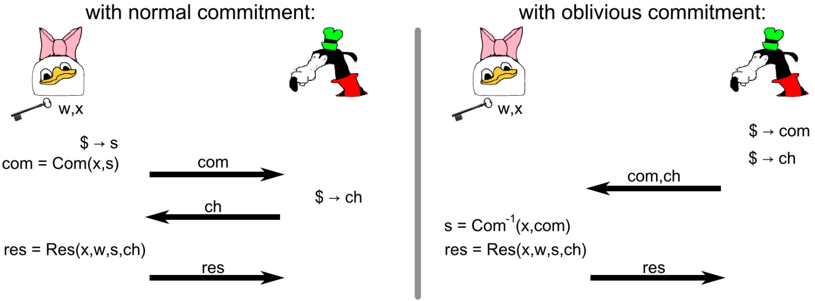
res = Res(x,w,s,ch)

Positive result

Idea

Remove active security from underlying identification scheme

Identification schemese with **Oblivious Commitments**



with normal commitment:

w,x

$ → s

com = Com(x,s)

com

$ → ch

ch

res = Res(x,w,s,ch)

res

with oblivious commitment:

w,x

$ → com

$ → ch

com,ch

s = Com^{-1}(x,com)

res = Res(x,w,s,ch)

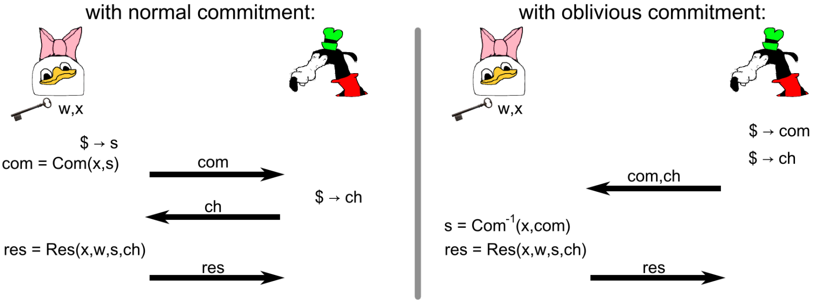
res

Positive result

Idea

Remove active security from underlying identification scheme

Identification schemese with **Oblivious Commitments**



with normal commitment:

w,x

$ → s

com = Com(x,s)

com

$ → ch

ch

res = Res(x,w,s,ch)

res

with oblivious commitment:

w,x

$ → com

$ → ch

com,ch

s = Com^{-1}(x,com)

res = Res(x,w,s,ch)

res

Oblivious commitments remove active security!

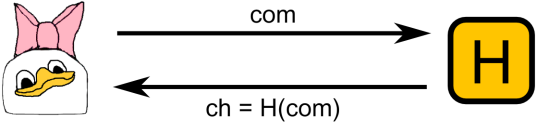
Positive result

How to apply Fiat–Shamir with oblivious commitment schemes?

Positive result

How to apply Fiat–Shamir with oblivious commitment schemes?

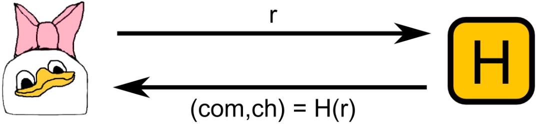
Our patch:



Positive result

How to apply Fiat–Shamir with oblivious commitment schemes?

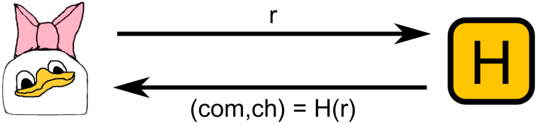
Our patch:



Positive result

How to apply Fiat–Shamir with oblivious commitment schemes?

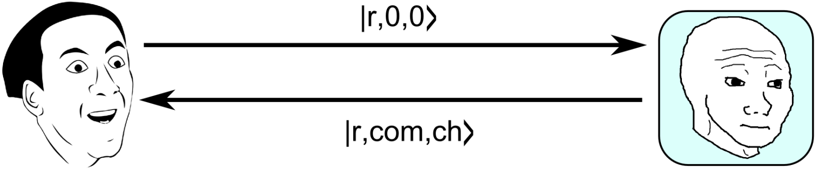
Our patch:



Theorem:

The Fiat–Shamir transformation of an oblivious commitment identification scheme yields an existentially unforgeable secure signature scheme in the QROM.

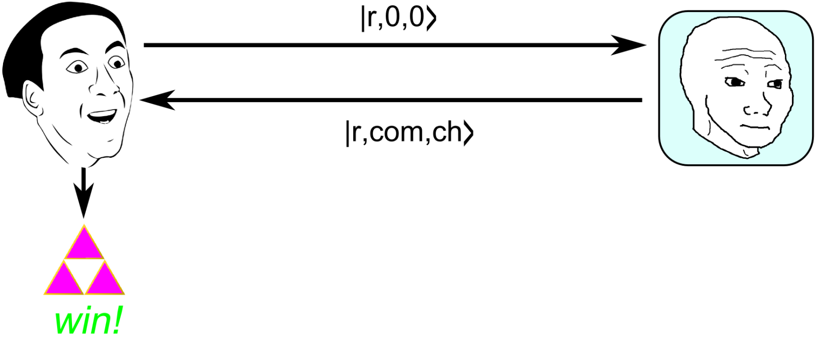
How our positive result works



$|r,0,0\rangle$

$|r,\mathrm{com},\mathrm{ch}\rangle$

How our positive result works

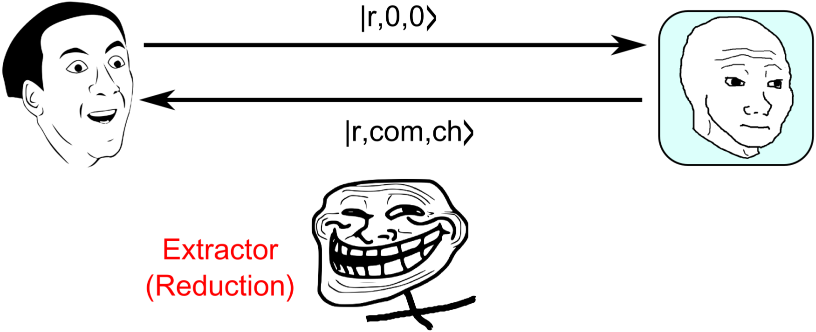


$|r,0,0\rangle$

$|r,\mathrm{com},\mathrm{ch}\rangle$

win!

How our positive result works

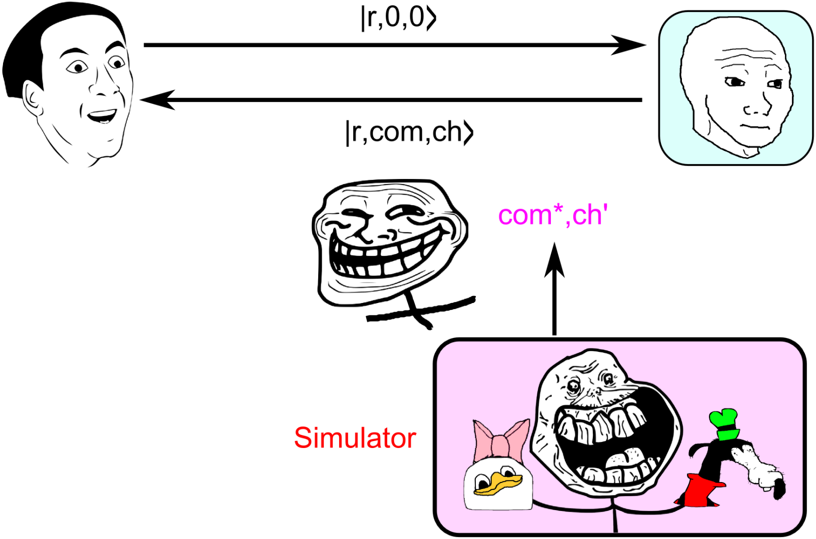


$|r,0,0\rangle$

$|r,com,ch\rangle$

Extractor
(Reduction)

How our positive result works



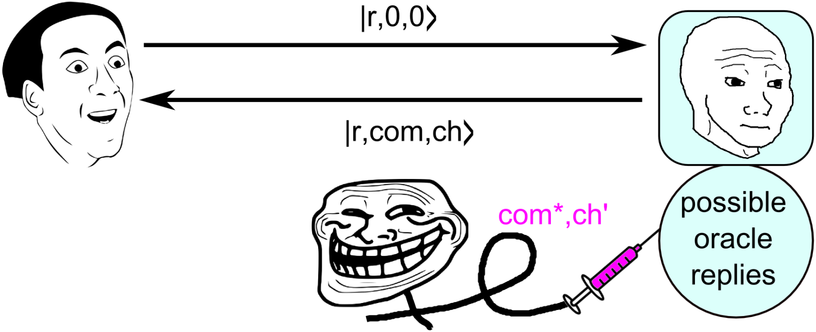
$|r,0,0\rangle$

$|r,com,ch\rangle$

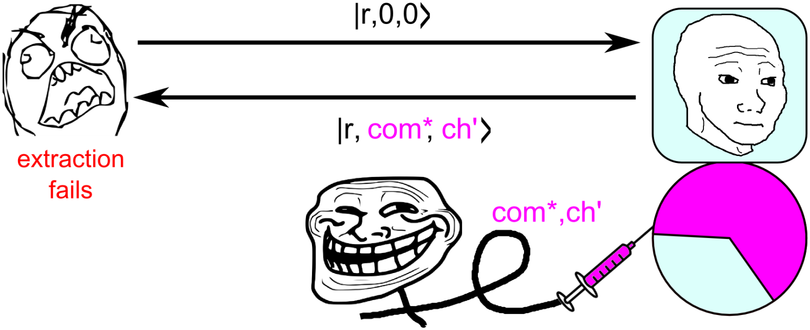
com*,ch'

Simulator

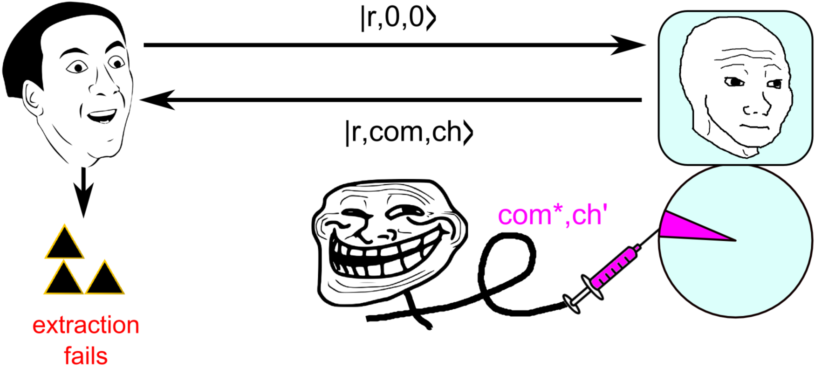
How our positive result works



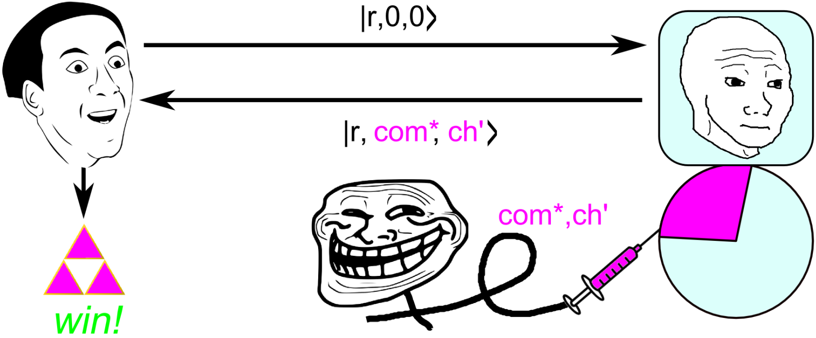
How our positive result works



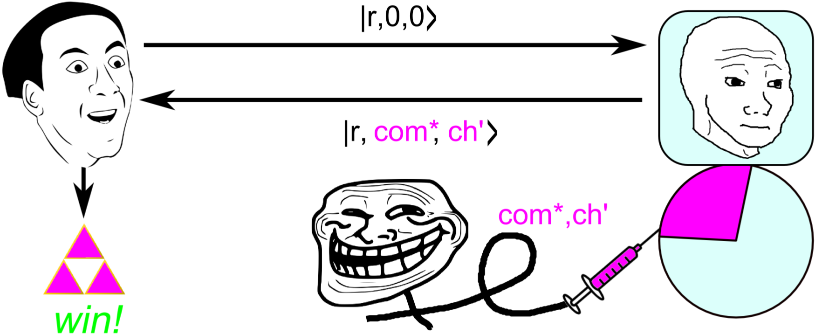
How our positive result works



How our positive result works



How our positive result works



$|r,0,0\rangle$

$|r, \text{com*}, \text{ch'}\rangle$

com*,ch'

win!

$$\Pr\left[\mathit{success}\right] \geq \delta\epsilon - \frac{8}{3}q_H^4\delta^2 - q_S \cdot 4\sqrt{(q_H + q_S)\cdot 2^{-\frac{n}{2}}}$$
$$- \left(q_S q_H + \frac{(q_S - 1)^2}{2}\right)\cdot 2^{-n} - negl(\epsilon)$$

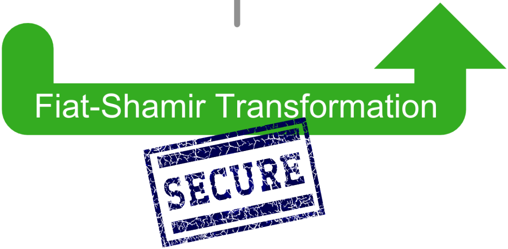
A surprising result

Weaker
Identification scheme

(no active security)

Stronger
Signature scheme

(provably secure
in the QROM)



Fiat-Shamir Transformation

SECURE

An example instantiation

1. Start with a witness-independent, oblivious commitment identification scheme based on post-quantum primitives

An example instantiation

1. Start with a witness-independent, oblivious commitment identification scheme based on post-quantum primitives

   Our choice: [Lyu12]

[Lyu12]: V. Lyubashevsky, *'Lattice signatures without trapdoors'*, 2012

An example instantiation

1. Start with a witness-independent, oblivious commitment identification scheme based on post-quantum primitives

   Our choice: [Lyu12]

2. Let the prover sample and send a random value r which is ignored by the verifier

[Lyu12]: V. Lyubashevsky, *'Lattice signatures without trapdoors'*, 2012

An example instantiation

1. Start with a witness-independent, oblivious commitment identification scheme based on post-quantum primitives

   Our choice: [Lyu12]

2. Let the prover sample and send a random value r which is ignored by the verifier
3. Let the verifier choose and send both *com* and *ch*

[Lyu12]: V. Lyubashevsky, *'Lattice signatures without trapdoors'*, 2012

An example instantiation

1. Start with a witness-independent, oblivious commitment identification scheme based on post-quantum primitives

   Our choice: [Lyu12]

2. Let the prover sample and send a random value r which is ignored by the verifier
3. Let the verifier choose and send both *com* and *ch*
4. Prover uses a trapdoor to find preimage for the obtained oblivious commitment and completes protocol

[Lyu12]: V. Lyubashevsky, *'Lattice signatures without trapdoors'*, 2012

An example instantiation

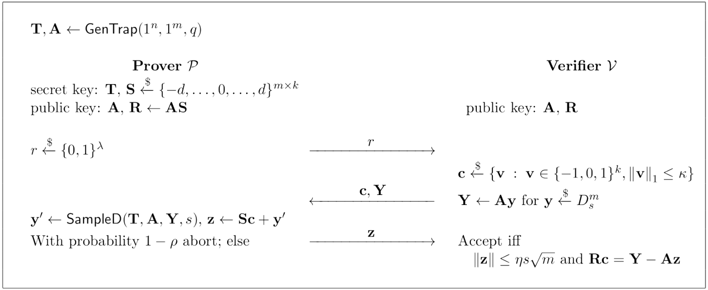
1. Start with a witness-independent, oblivious commitment identification scheme based on post-quantum primitives

   Our choice: [Lyu12]

2. Let the prover sample and send a random value r which is ignored by the verifier
3. Let the verifier choose and send both *com* and *ch*
4. Prover uses a trapdoor to find preimage for the obtained oblivious commitment and completes protocol
5. Apply our 'patched' Fiat–Shamir transformation to resulting scheme.

[Lyu12]: V. Lyubashevsky, *'Lattice signatures without trapdoors'*, 2012

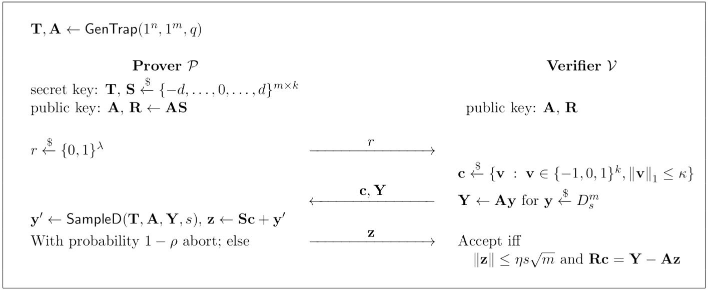
Our patched version of the Lyubashevsky scheme



$\mathbf{T}, \mathbf{A} \leftarrow \mathsf{GenTrap}(1^n, 1^m, q)$

Prover $\mathcal{P}$		**Verifier** $\mathcal{V}$
secret key: $\mathbf{T}$, $\mathbf{S} \overset{\$}{\leftarrow} \{-d, \ldots, 0, \ldots, d\}^{m \times k}$		
public key: $\mathbf{A}$, $\mathbf{R} \leftarrow \mathbf{AS}$		public key: $\mathbf{A}$, $\mathbf{R}$
$r \overset{\$}{\leftarrow} \{0,1\}^\lambda$	$\xrightarrow{r}$	
		$\mathbf{c} \overset{\$}{\leftarrow} \{\mathbf{v} \ : \ \mathbf{v} \in \{-1,0,1\}^k, \Vert\mathbf{v}\Vert_1 \leq \kappa\}$
	$\xleftarrow{\mathbf{c}, \mathbf{Y}}$	$\mathbf{Y} \leftarrow \mathbf{Ay}$ for $\mathbf{y} \overset{\$}{\leftarrow} D_s^m$
$\mathbf{y}' \leftarrow \mathsf{SampleD}(\mathbf{T}, \mathbf{A}, \mathbf{Y}, s)$, $\mathbf{z} \leftarrow \mathbf{Sc} + \mathbf{y}'$		
With probability $1 - \rho$ abort; else	$\xrightarrow{\mathbf{z}}$	Accept iff
		$\Vert\mathbf{z}\Vert \leq \eta s \sqrt{m}$ and $\mathbf{Rc} = \mathbf{Y} - \mathbf{Az}$

Our patched version of the Lyubashevsky scheme



$\mathbf{T}, \mathbf{A} \leftarrow \mathsf{GenTrap}(1^n, 1^m, q)$

Prover $\mathcal{P}$

secret key: $\mathbf{T}$, $\mathbf{S} \xleftarrow{\$} \{-d, \ldots, 0, \ldots, d\}^{m \times k}$

public key: $\mathbf{A}$, $\mathbf{R} \leftarrow \mathbf{AS}$

Verifier $\mathcal{V}$

public key: $\mathbf{A}$, $\mathbf{R}$

$r \xleftarrow{\$} \{0,1\}^\lambda$ $\xrightarrow{\quad r \quad}$

$\mathbf{c} \xleftarrow{\$} \{\mathbf{v} \ : \ \mathbf{v} \in \{-1,0,1\}^k, \|\mathbf{v}\|_1 \leq \kappa\}$

$\xleftarrow{\quad \mathbf{c}, \mathbf{Y} \quad}$ $\mathbf{Y} \leftarrow \mathbf{Ay}$ for $\mathbf{y} \xleftarrow{\$} D_s^m$

$\mathbf{y}' \leftarrow \mathsf{SampleD}(\mathbf{T}, \mathbf{A}, \mathbf{Y}, s)$, $\mathbf{z} \leftarrow \mathbf{Sc} + \mathbf{y}'$

With probability $1 - \rho$ abort; else $\xrightarrow{\quad \mathbf{z} \quad}$

Accept iff

$\|\mathbf{z}\| \leq \eta s \sqrt{m}$ and $\mathbf{Rc} = \mathbf{Y} - \mathbf{Az}$

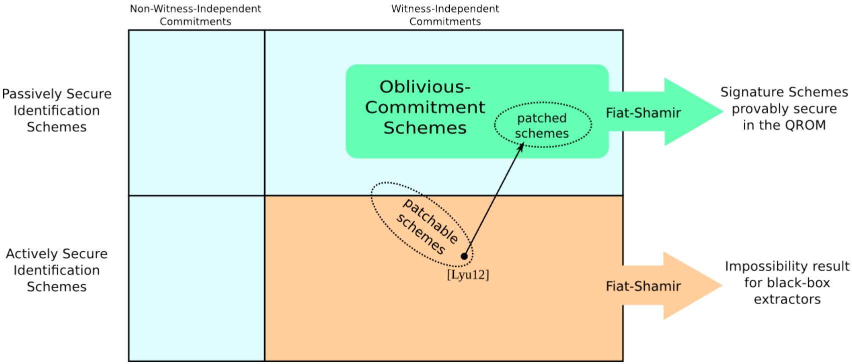
Similar to [GPV08] with hash-and-sign, also proven secure in [BZ13]

[GPV08]:Gentry,Peikert,Vaikuntanathan,*'Trapdoors for hard lattices and new cryptographic constructions'*,2008

[BZ13]:Boneh,Zhandry,*'Secure signatures and chosen ciphertext security in a post-quantum world'*,2013

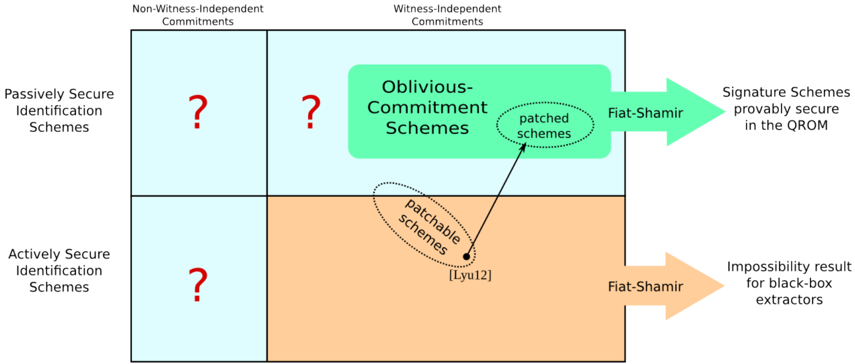
Conclusions

The Fiat–Shamir Transformation in the QROM


Non-Witness-Independent Commitments
Witness-Independent Commitments
Passively Secure Identification Schemes
Actively Secure Identification Schemes
Oblivious-Commitment Schemes
patched schemes
patchable schemes
[Lyu12]
Fiat-Shamir
Signature Schemes provably secure in the QROM
Fiat-Shamir
Impossibility result for black-box extractors

Conclusions

The Fiat–Shamir Transformation in the QROM


Non-Witness-Independent Commitments
Witness-Independent Commitments
Passively Secure Identification Schemes
Actively Secure Identification Schemes
?
?
?
Oblivious-Commitment Schemes
patched schemes
patchable schemes
[Lyu12]
Fiat-Shamir
Signature Schemes provably secure in the QROM
Fiat-Shamir
Impossibility result for black-box extractors

Open questions

End of this talk

Thanks for your attention!

tommaso@gagliardoni.net

TECHNISCHE
UNIVERSITÄT
DARMSTADT

CASED

EC SPRIDE
EUROPEAN CENTER FOR
SECURITY AND PRIVACY BY DESIGN