From 5-pass $\mathcal{MQ}$-based identification to $\mathcal{MQ}$-based signatures

Andreas Hülsing, Joost Rijneveld, Simona Samardjiska, and Peter Schwabe

30 June 2016

Our take on PQ-Crypto

Prepare for actual use

- Reliable security arguments (Reductions, cryptanalysis)
- Reliable security estimates (cryptanalysis – conventional / quantum)
- Tolerable sizes and speed.

- 128 bit post-quantum security
- Tight security reduction in standard model or QROM
- Sizes / Time ? Let's get a baseline...

Our take on PQ-Crypto

Prepare for actual use

- Reliable security arguments (Reductions, cryptanalysis)
- Reliable security estimates (cryptanalysis – conventional / quantum)
- Tolerable sizes and speed.

- 128 bit post-quantum security
- Tight security reduction in standard model or QROM
- Sizes / Time ? Let's get a baseline...

Our take on PQ-Crypto

Prepare for actual use

- Reliable security arguments (Reductions, cryptanalysis)
- Reliable security estimates (cryptanalysis – conventional / quantum)
- Tolerable sizes and speed.

- 128 bit post-quantum security
- Tight security reduction in standard model or QROM
- Sizes / Time ? Let's get a baseline...

Our take on PQ-Crypto

Prepare for actual use

- Reliable security arguments (Reductions, cryptanalysis)
- Reliable security estimates (cryptanalysis – conventional / quantum)
- Tolerable sizes and speed.

- 128 bit post-quantum security
- Tight security reduction in standard model or QROM
- Sizes / Time ? Let's get a baseline...

Setting the landscape (Signatures)

- Lattices: (Ring-)TESLA [ABB+16,ABBD15]
- Hash-based: SPHINCS [BHH+15] / XMSS [BDH11, HRS16]
- $\mathcal{MQ}$: ?
- Codes: ???

$\mathcal{MQ}$ Crypto

- Post-quantum candidate.
- Mainly signatures (Encryption too recent)
- Fast, small signatures, large keys (100kb@100bit classical sec.)
- **Security?**

The history on security

Examples of broken schemes include

- **Oil-and-Vinegar** [Pat97] (**broken** in [KS98]),
- **SFLASH** [CGP] (**broken** in [DFSS07]),
- **MQQ-Sig** [GØJ+11] (**broken** in [FGP+15]),
- **(Enhanced) TTS** [YCC04,YC05] (**broken** in [TW12]), and
- **Enhanced STS** [TGTF10] (**broken** in [TW12]).

Essentially only two proposals still standing:

- **HFEv$^-$** variants [PCG01,PCY+15] and
- **Unbalanced Oil-and-Vinegar (UOV)** variants [KPG99,DS05].

Why?

Is $\mathcal{MQ}$-Problem easy?

No, NP-complete! [GJ79]

So, why then?

- Attacks do not solve $\mathcal{MQ}$,
- Ad-hoc designs
- Security actually based on $\mathcal{MQ}$ + IP [Pat96]
- IP often relies on (easy instance of) MinRank Problem [Cou01,FLP08]

Why?

Is $\mathcal{MQ}$-Problem easy?
No, NP-complete! [GJ79]
So, why then?

- Attacks do not solve $\mathcal{MQ}$,
- Ad-hoc designs
- Security actually based on $\mathcal{MQ}$ + IP [Pat96]
- IP often relies on (easy instance of) MinRank Problem [Cou01,FLP08]

Why?

Is $\mathcal{MQ}$-Problem easy?
No, NP-complete! [GJ79]
So, why then?

- Attacks do not solve $\mathcal{MQ}$,
- Ad-hoc designs
- Security actually based on $\mathcal{MQ}$ + IP [Pat96]
- IP often relies on (easy instance of) MinRank Problem [Cou01,FLP08]

So no reliable signatures from $\mathcal{MQ}$?

$\mathcal{MQ}$ Signatures with security reduction

Sakumoto, Shirai, and Hiwatari, Crypto 2011

- Identification schemes (IDS) with reduction from $\mathcal{MQ}$,
- 3- and 5-pass schemes
- 3-pass: Fiat-Shamir $\Rightarrow$ inefficient signatures
- 5-pass: No transform / security reduction

El Yousfi Alaoui, Dagdelen, Véron, Galindo, and Cayrel, Africacrypt 2012

- Fiat-Shamir transform for $2n + 1$ pass IDS
- Loose reduction
- Signature from [SSH11] 5-pass IDS.

$\mathcal{MQ}$ Signatures with security reduction

Sakumoto, Shirai, and Hiwatari, Crypto 2011

- Identification schemes (IDS) with reduction from $\mathcal{MQ}$,
- 3- and 5-pass schemes
- 3-pass: Fiat-Shamir $\Rightarrow$ inefficient signatures
- 5-pass: No transform / security reduction

El Yousfi Alaoui, Dagdelen, Véron, Galindo, and Cayrel, Africacrypt 2012

- Fiat-Shamir transform for $2n + 1$ pass IDS
- Loose reduction
- Signature from [SSH11] 5-pass IDS.

So what's left to do?

We want:

- 128 bit post-quantum security
- Tight security reduction in standard model or QROM
- Sizes / Time ? Let's get a baseline...

TODO:

- Select parameters considering quantum attacks
- Tighten reduction / QROM
- (Optimized) Implementation

Easy, right? That's what we thought...

Project log

- (End 2015) Joost: "I can break this"
- (Still 2015) Easy fix (minor mistake in challenge generation)
- (JAN 2016) Marc Fischlin: "Strange that they only need two transcripts"
- (MAR 2016) Transform does not apply to [SSH11]
- ...

Project log

- (End 2015) Joost: "I can break this"
- (Still 2015) Easy fix (minor mistake in challenge generation)
- (JAN 2016) Marc Fischlin: "Strange that they only need two transcripts"
- (MAR 2016) Transform does not apply to [SSH11]
- ...

Project log

- (End 2015) Joost: "I can break this"
- (Still 2015) Easy fix (minor mistake in challenge generation)
- (JAN 2016) Marc Fischlin: "Strange that they only need two transcripts"
- (MAR 2016) Transform does not apply to [SSH11]
- ...

Project log

- (End 2015) Joost: "I can break this"
- (Still 2015) Easy fix (minor mistake in challenge generation)
- (JAN 2016) Marc Fischlin: "Strange that they only need two transcripts"
- (MAR 2016) Transform does not apply to [SSH11]
- ...

Project log

- (End 2015) Joost: "I can break this"
- (Still 2015) Easy fix (minor mistake in challenge generation)
- (JAN 2016) Marc Fischlin: "Strange that they only need two transcripts"
- (MAR 2016) Transform does not apply to [SSH11]
- ...

Our contribution

- ✓ Proof that every IDS where [ADV+12] applies can be turned to 3-pass IDS
- ✓ Proof that [ADV+12] does not apply to $\mathcal{MQ}$ (and to most other 5-pass IDS)
- ✓ New transform + reduction for (class of) 5-pass IDS to signature scheme
- ✓ New generic proposal MQDSS
- ✓ MQDSS-31-64: Instance with 128 bit security against quantum-computer-aided attacks
- ✓ Optimized implementation
- X No tight proof
- X Only ROM ($\rightarrow$ not QROM)

Our contribution

- ✓ Proof that every IDS where [ADV+12] applies can be turned to 3-pass IDS
- ✓ Proof that [ADV+12] does not apply to $\mathcal{MQ}$ (and to most other 5-pass IDS)
- ✓ New transform + reduction for (class of) 5-pass IDS to signature scheme
- ✓ New generic proposal MQDSS
- ✓ MQDSS-31-64: Instance with 128 bit security against quantum-computer-aided attacks
- ✓ Optimized implementation
- X No tight proof
- X Only ROM ($\rightarrow$ not QROM)

Our contribution

- ✓ **Proof that every IDS where [ADV+12] applies can be turned to 3-pass IDS**
- ✓ Proof that [ADV+12] does not apply to $\mathcal{MQ}$ (and to most other 5-pass IDS)
- ✓ New transform + reduction for (class of) 5-pass IDS to signature scheme
- ✓ New generic proposal MQDSS
- ✓ MQDSS-31-64: Instance with 128 bit security against quantum-computer-aided attacks
- ✓ Optimized implementation
- X No tight proof
- X Only ROM ($\rightarrow$ not QROM)

Fiat-Shamir – a primer

Canonical IDS

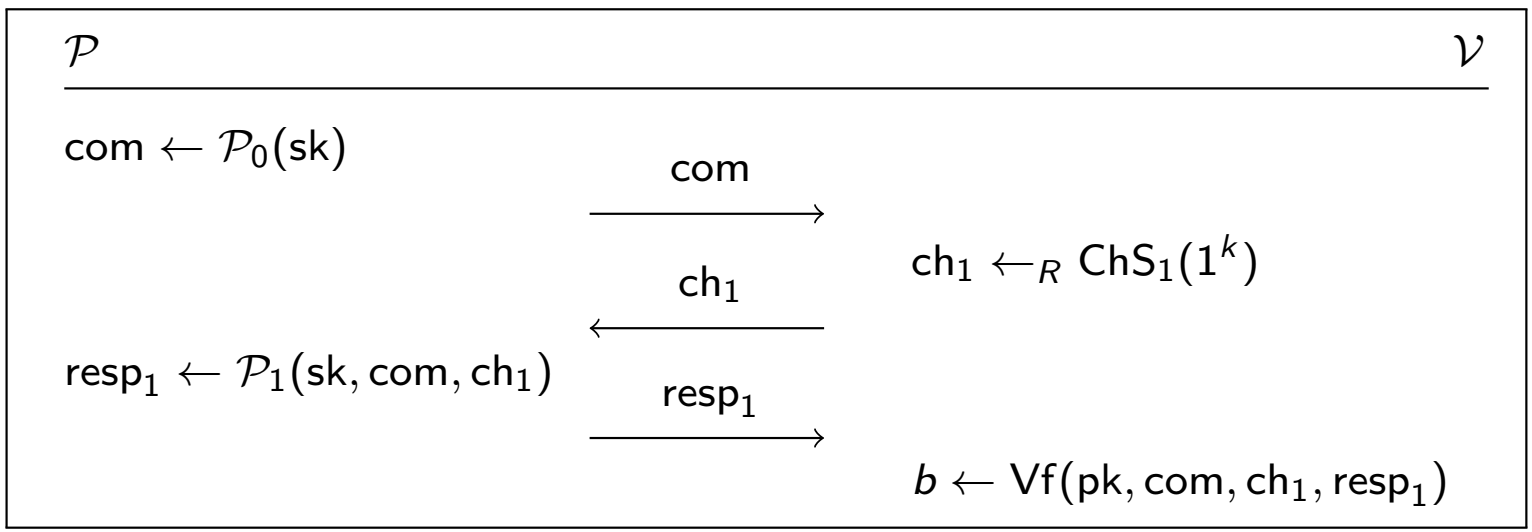

Figure : Canonical 3-pass IDS

Soundness

Definition (Soundness (with soundness error κ))

Let $k \in \mathbb{N}$, $\mathsf{IDS} = (\mathsf{KGen}, \mathcal{P}, \mathcal{V})$ an identification scheme. We say that IDS is sound with soundness error κ if for every PPT adversary $\mathcal{A}$

$$\left| \Pr \left[\begin{array}{l} (\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}(1^k) \\ \langle \mathcal{A}(1^k, \mathsf{pk}), \mathcal{V}(\mathsf{pk}) \rangle = 1 \end{array} \right] - \kappa \right| = \mathrm{negl}(k).$$

Definition (Special soundness)

A canonical IDS is said to fulfill special soundness if there exists a PPT algorithm $\mathcal{E}$, called the extractor, that given two accepting transcripts $\mathsf{trans} = (\mathsf{com}, \mathsf{ch}_1, \mathsf{resp}_1)$ and $\mathsf{trans}' = (\mathsf{com}, \mathsf{ch}_1', \mathsf{resp}_1')$ with $\mathsf{ch}_1 \neq \mathsf{ch}_1'$ as well as the corresponding public key pk, outputs a matching secret key sk for pk with non-negligible success probability.

Soundness

Definition (Soundness (with soundness error κ))

Let $k \in \mathbb{N}$, $\mathsf{IDS} = (\mathsf{KGen}, \mathcal{P}, \mathcal{V})$ an identification scheme. We say that IDS is sound with soundness error κ if for every PPT adversary $\mathcal{A}$

$$\left| \Pr \left[\begin{array}{l} (\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}(1^k) \\ \langle \mathcal{A}(1^k, \mathsf{pk}), \mathcal{V}(\mathsf{pk}) \rangle = 1 \end{array} \right] - \kappa \right| = \mathrm{negl}(k).$$

Definition (Special soundness)

A canonical IDS is said to fulfill special soundness if there exists a PPT algorithm $\mathcal{E}$, called the extractor, that given two accepting transcripts $\mathsf{trans} = (\mathsf{com}, \mathsf{ch}_1, \mathsf{resp}_1)$ and $\mathsf{trans}' = (\mathsf{com}, \mathsf{ch}_1', \mathsf{resp}_1')$ with $\mathsf{ch}_1 \neq \mathsf{ch}_1'$ as well as the corresponding public key pk, outputs a matching secret key sk for pk with non-negligible success probability.

Canonical IDS

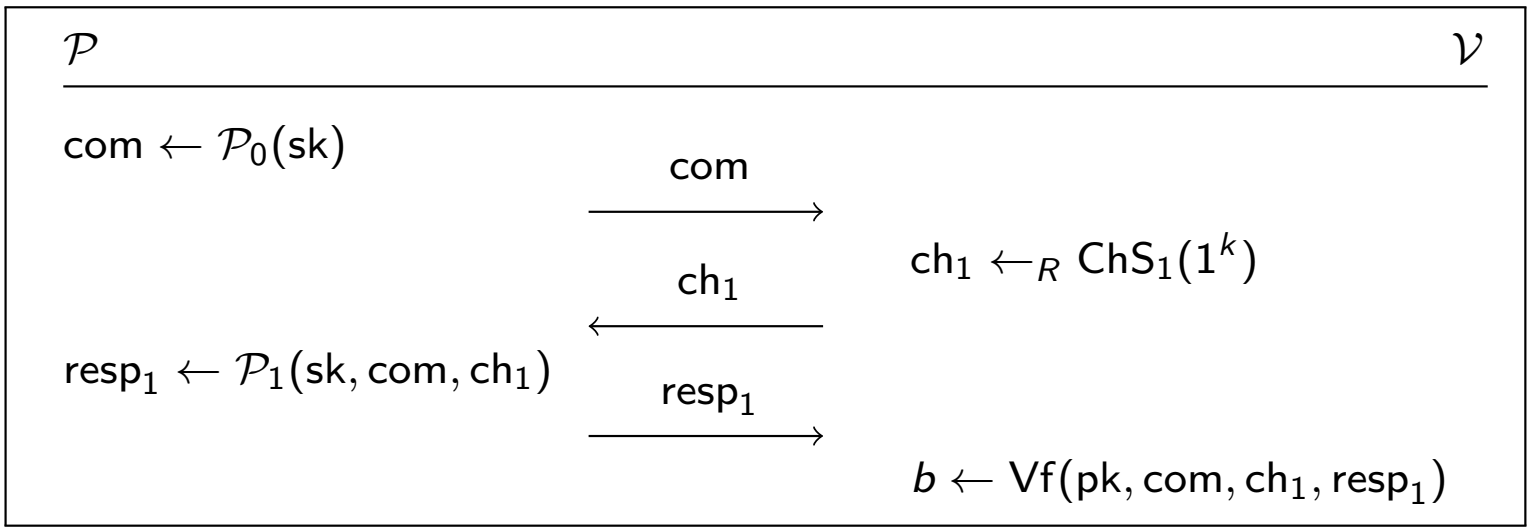

Figure : Canonical 3-pass IDS

Honest-Verifier Zero-Knowledge (HVZK)

Definition ((statistical) Honest-verifier zero-knowledge)

Let $k \in \mathbb{N}$, $\mathsf{IDS} = (\mathsf{KGen}, \mathcal{P}, \mathcal{V})$ an identification scheme. We say that IDS is statistical honest-verifier zero-knowledge if there exists a probabilistic polynomial time algorithm $\mathcal{S}$, called the simulator, such that the statistical distance between the following two distribution ensembles is negligible in k:

$$\left\{(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}(1^k) : (\mathsf{sk}, \mathsf{pk}, \mathsf{trans}(\langle \mathcal{P}(\mathsf{sk}), \mathcal{V}(\mathsf{pk}) \rangle))\right\}$$

$$\left\{(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathsf{KGen}(1^k) : (\mathsf{sk}, \mathsf{pk}, \mathcal{S}(\mathsf{pk}))\right\}$$

Canonical IDS

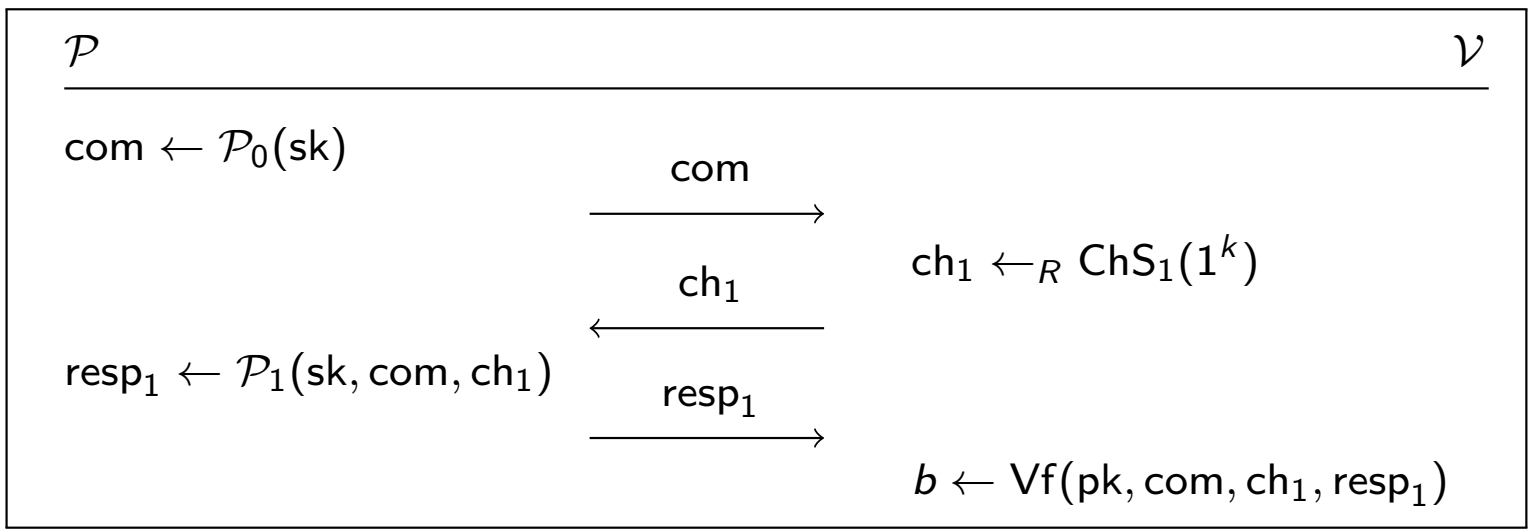

Figure : Canonical 3-pass IDS

Fiat-Shamir Transform

$\mathsf{SIGN}(\mathsf{sk}, M)$	$\mathsf{VF}(\mathsf{pk}, M, \sigma)$
$\mathsf{com} \leftarrow \mathcal{P}_0(\mathsf{sk})$	$ch_1 \leftarrow \mathcal{H}(\mathsf{com} \Vert M)$
$\mathsf{ch}_1 \leftarrow \mathcal{H}(\mathsf{com} \Vert M) \in \mathsf{ChS}_1(1^k)$	**return** $b \leftarrow \mathsf{Vf}(\mathsf{pk}, \mathsf{com}, \mathsf{ch}_1, \mathsf{resp}_1)$
$\mathsf{resp}_1 \leftarrow \mathcal{P}_1(\mathsf{sk}, \mathsf{com}, \mathsf{ch}_1)$	
return $\sigma = (\mathsf{com}, \mathsf{resp}_1)$	

Figure : Generic Fiat-Shamir Signatures

Security

- Pointcheval & Stern (JoC 2000): Secure if IDS
  - HVZK, and
  - achieves special soundness.
- Proof in ROM
- Idea: Rewind $\mathcal{A}$ and change RO answers to obtain two transcripts with different ch_1 (Forking Lemma).
- HVZK allows to simulate Sign-oracle without sk.

El Yousfi Alaoui et al. idea (for 5-pass)

Canonical 5-pass IDS

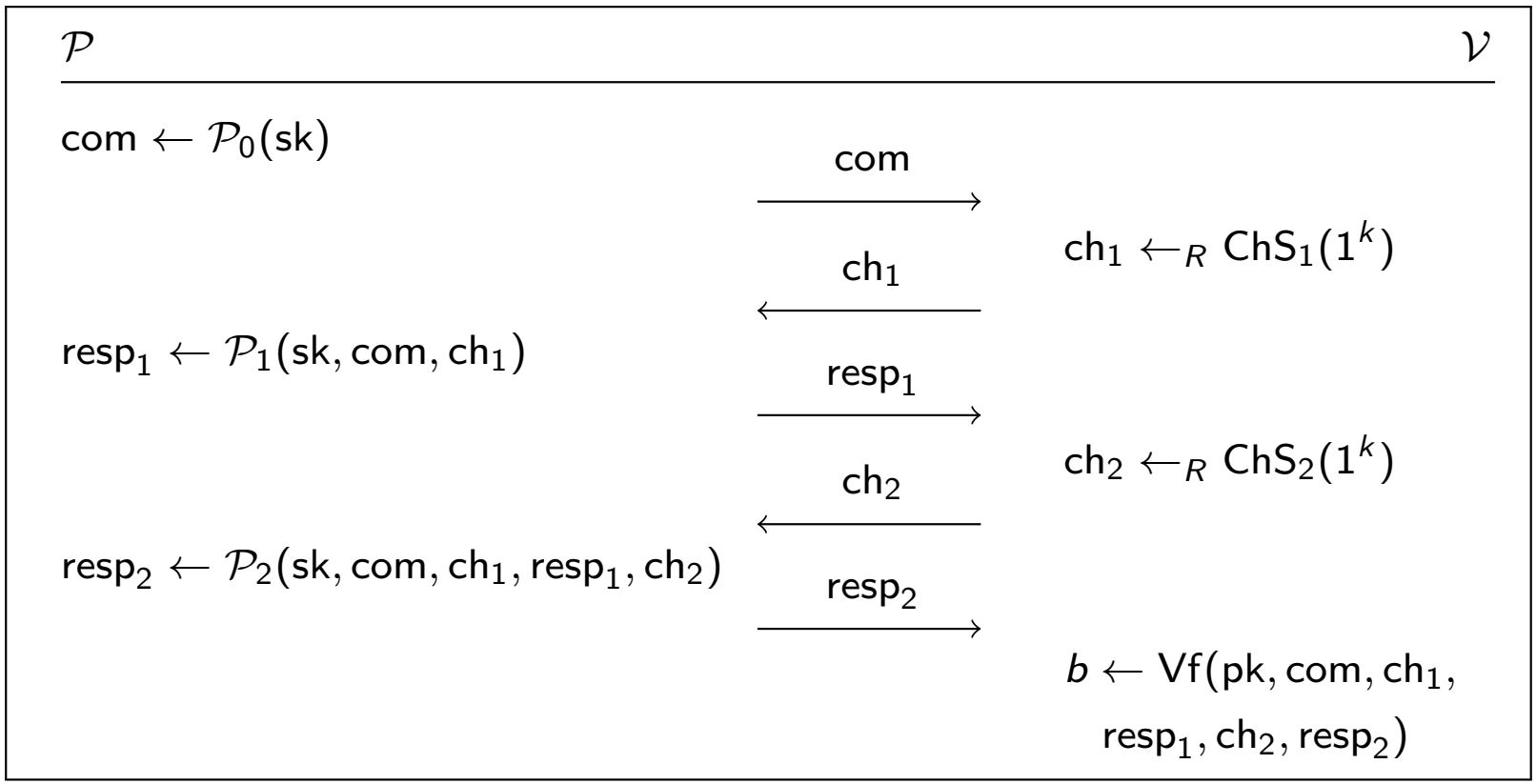

Figure : Canonical 5-pass IDS

Fiat-Shamir Transform

SIGN(sk, M)

$\mathsf{com} \leftarrow \mathcal{P}_0(\mathsf{sk})$

$\mathsf{ch}_1 \leftarrow \mathcal{H}(\mathsf{com} \| M) \in \mathsf{ChS}_1(1^k)$

$\mathsf{resp}_1 \leftarrow \mathcal{P}_1(\mathsf{sk}, \mathsf{com}, \mathsf{ch}_1)$

$\mathsf{ch}_2 \leftarrow \mathcal{H}(\mathsf{com} \| \mathsf{ch}_1 \| \mathsf{resp}_1 \| M) \in \mathsf{ChS}_2(1^k)$

$\mathsf{resp}_2 \leftarrow \mathcal{P}_2(\mathsf{sk}, \mathsf{com}, \mathsf{ch}_1, \mathsf{resp}_1, \mathsf{ch}_2)$

return $\sigma = (\mathsf{com}, \mathsf{resp}_1, \mathsf{resp}_2)$

VF(pk, M, σ)

$\mathsf{ch}_1 \leftarrow \mathcal{H}(\mathsf{com} \| M)$

$\mathsf{ch}_2 \leftarrow \mathcal{H}(\mathsf{com} \| \mathsf{ch}_1 \| \mathsf{resp}_1 \| M)$

return $b \leftarrow \mathsf{Vf}(\mathsf{pk}, \mathsf{com}, \mathsf{ch}_1, \mathsf{resp}_1, \mathsf{ch}_2, \mathsf{resp}_2)$

Figure : Generic Fiat-Shamir Signatures from 5-pass IDS

Security

- El Yousfi Alaoui et al. (Africacrypt 2012): Secure if IDS
  - HVZK, and
  - achieves n-**special soundness**.
- Proof almost identical to Pointcheval & Stern

Definition (Special n-soundness (informal))

There exists a PPT extractor $\mathcal{E}$ that extracts a secret key given pk and two accepting transcripts that differ in last challenge.

Security

- El Yousfi Alaoui et al. (Africacrypt 2012): Secure if IDS
  - HVZK, and
  - achieves n-**special soundness**.
- Proof almost identical to Pointcheval & Stern

Definition (Special n-soundness (informal))

There exists a PPT extractor $\mathcal{E}$ that extracts a secret key given pk and two accepting transcripts that differ in last challenge.

Result 1

Theorem

Let $\mathsf{IDS} = (\mathsf{KGen}, \mathcal{P}, \mathcal{V})$ *be a canonical* 5*-pass IDS that fulfills special n-soundness. Then* IDS *can be transformed into a canonical 3-pass IDS* $\mathsf{IDS}' = (\mathsf{KGen}, \mathcal{P}', \mathcal{V}')$ *that fulfills special soundness and HVZK. Moreover,* IDS' *is at least as efficient as* IDS*.*

IDS′

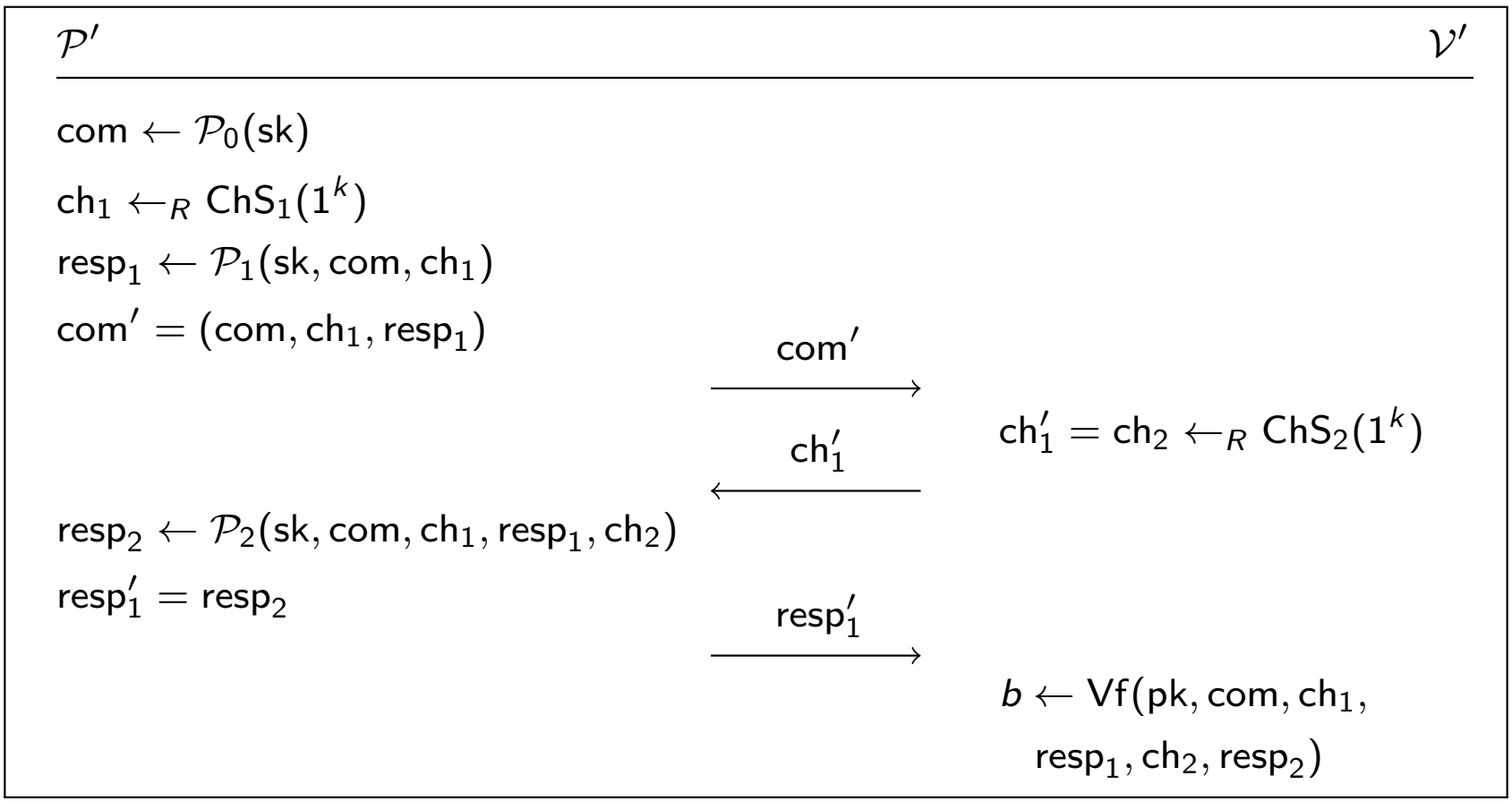

Figure : From 5-pass to 3-pass

Security

HVZK

- Use simulator for IDS and just reorder first three messages into a single one.

Special soundness

- Reduction: If there exists an extractor for IDS' we can use it for IDS too.
- Again, just transform transcripts.

So does this work for all 5-pass IDS?

So does this work for all 5-pass IDS?
No!

Most 5-pass IDS do not fulfill special n-soundness

Result 2

The 5-pass $\mathcal{MQ}$-IDS from Sakumoto et al. does not fulfill special n-soundness

- It is trivial to generate two accepting transcripts that disagree in last challenge. (Soundness error $= \frac{1}{2} + \frac{1}{2q}$)
- There only exists an extractor for **four** transcripts with

$$\mathsf{ch}_1^1 = \mathsf{ch}_1^2 \neq \mathsf{ch}_1^3 = \mathsf{ch}_1^4$$

$$\mathsf{ch}_2^1 \neq \mathsf{ch}_2^2 \wedge \mathsf{ch}_2^3 \neq \mathsf{ch}_2^4$$

$$(\mathsf{ChS}_1 = [0, q],\ \mathsf{ChS}_2 = \{0, 1\})$$

Most 5-pass IDS do not fulfill special n-soundness

Result 2

The 5-pass $\mathcal{MQ}$-IDS from Sakumoto et al. does not fulfill special n-soundness

- It is trivial to generate two accepting transcripts that disagree in last challenge. (Soundness error $= \frac{1}{2} + \frac{1}{2q}$)
- There only exists an extractor for **four** transcripts with

$$\mathsf{ch}_1^1 = \mathsf{ch}_1^2 \neq \mathsf{ch}_1^3 = \mathsf{ch}_1^4$$

$$\mathsf{ch}_2^1 \neq \mathsf{ch}_2^2 \wedge \mathsf{ch}_2^3 \neq \mathsf{ch}_2^4$$

$(\mathsf{ChS}_1 = [0, q],\ \mathsf{ChS}_2 = \{0, 1\})$

More results in paper

- ✓ Fixed transform & reductions for "q2-IDS".
- ✓ Specified a full construction using 5-pass $\mathcal{MQ}$-IDS + security reduction.
- ✓ Selected parameters with 128bits security against quantum-computer-aided attacks.
- ✓ Optimized implementation of Signatures from 3- and 5-pass $\mathcal{MQ}$-IDS.

Paper will be on eprint soon...

Some concluding thoughts

- Dear reviewers, ... **please check the proofs** (at least for accepted papers).
- There were two clear mistakes in two places in El Yousfi et al. (parallel composition, 5-pass $\mathcal{MQ}$-IDS fulfills special n-soundness).
- Dear authors,... **please publish your full proofs!**.
- Sakumoto et al. only published incredibly hard to read proof sketches.

This was not a single persons fault many people contributed to this.