MQDSS signatures - security

Ming-Shing Chen[1,2], Andreas Hülsing[3], Joost Rijneveld[4],
Simona Samardjiska[4], Peter Schwabe[4]

National Taiwan University[1] / Academia Sinica, Taipei, Taiwan[2]
Eindhoven University of Technology, The Netherlands[3]
Radboud University, Nijmegen, The Netherlands[4]

CWG-meeting, 24.03.2017, Utrecht

Earlier Joost presented MQDSS-31-64 ...

- Signature scheme
  - via Fiat-Shamir transform
  - from $\mathcal{MQ}$-based 5-pass IDS [Sakumoto et al. '11]
- Parameters for 128-bit Post-quantum security
- Optimized implementation

Motivation for this work

- Lack of provable $\mathcal{MQ}$ signature
- Inefficient signatures from 3-pass IDS [Sakumoto et al. '11]
  - big soundness error (2/3)

Motivation for this work

- Lack of provable $\mathcal{MQ}$ signature
- Inefficient signatures from 3-pass IDS [Sakumoto et al. '11]
  - big soundness error (2/3)
- Can we gain smth. if we consider signatures from 5-pass IDS?
  - smaller soundness error ($\frac{q+1}{2q}$ over $\mathbb{F}_q$) $\Rightarrow$ smaller signatures
  - FS transform for 5-pass already available [El Yousfi '12]
    - loose reduction in the ROM (as for 3-pass [Pointcheval & Stern '96])

Motivation for this work

- Lack of provable $\mathcal{MQ}$ signature
- Inefficient signatures from 3-pass IDS [Sakumoto et al. '11]
  - big soundness error (2/3)
- Can we gain smth. if we consider signatures from 5-pass IDS?
  - smaller soundness error ($\frac{q+1}{2q}$ over $\mathbb{F}_q$) $\Rightarrow$ smaller signatures
  - FS transform for 5-pass already available [El Yousfi '12]
    - loose reduction in the ROM (as for 3-pass [Pointcheval & Stern '96])
- It seems that what is left is ... (apart from what Joost presented)
  - tighter reduction
  - reduction in the QROM

Motivation for this work

- Lack of provable $\mathcal{MQ}$ signature
- Inefficient signatures from 3-pass IDS [Sakumoto et al. '11]
  - big soundness error (2/3)
- Can we gain smth. if we consider signatures from 5-pass IDS?
  - smaller soundness error ($\frac{q+1}{2q}$ over $\mathbb{F}_q$) $\Rightarrow$ smaller signatures
  - FS transform for 5-pass already available [El Yousfi '12]
    - loose reduction in the ROM (as for 3-pass [Pointcheval & Stern '96])
- It seems that what is left is ... (apart from what Joost presented)
  - tighter reduction
  - reduction in the QROM
- This is not what we did...

Motivation for this work

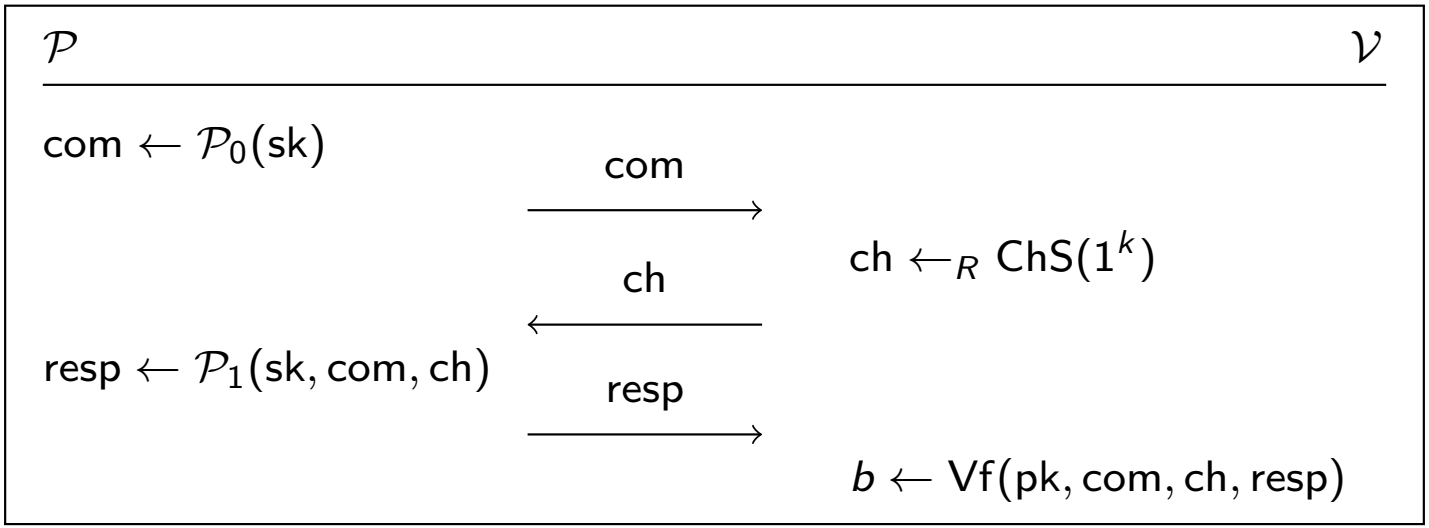
- Lack of provable $\mathcal{MQ}$ signature
- Inefficient signatures from 3-pass IDS [Sakumoto et al. '11]
  - big soundness error (2/3)
- Can we gain smth. if we consider signatures from 5-pass IDS?
  - smaller soundness error ($\frac{q+1}{2q}$ over $\mathbb{F}_q$) $\Rightarrow$ smaller signatures
  - FS transform for 5-pass already available [El Yousfi '12]
    - loose reduction in the ROM (as for 3-pass [Pointcheval & Stern '96])
- It seems that what is left is ... (apart from what Joost presented)
  - tighter reduction
  - reduction in the QROM
- This is not what we did...
- What we did - **Revisit Fiat-Shamir for 5-pass...**

Motivation for this work

- Lack of provable $\mathcal{MQ}$ signature
- Inefficient signatures from 3-pass IDS [Sakumoto et al. '11]
  - big soundness error (2/3)
- Can we gain smth. if we consider signatures from 5-pass IDS?
  - smaller soundness error ($\frac{q+1}{2q}$ over $\mathbb{F}_q$) $\Rightarrow$ smaller signatures
  - FS transform for 5-pass already available [El Yousfi '12]
    - loose reduction in the ROM (as for 3-pass [Pointcheval & Stern '96])
- It seems that what is left is ... (apart from what Joost presented)
  - tighter reduction
  - reduction in the QROM

  Still pending...
- This is not what we did...
- What we did - **Revisit Fiat-Shamir for 5-pass...**

Canonical 3-pass Identification Schemes



Properties of Canonical 3-pass IDS

Soundness (with soundness error κ)

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

- r rounds until $\kappa^r = negl(k)$
- guaranties negligible success of cheating Prover

Properties of Canonical 3-pass IDS

Soundness (with soundness error κ)

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

- r rounds until $\kappa^r = negl(k)$
- guaranties negligible success of cheating Prover

Special Soundness

There exists PPT algorithm $\mathcal{K}$ - knowledge extractor s.t. given two accepting transcripts $\mathsf{trans} = (\mathsf{com}, \mathsf{ch}, \mathsf{resp})$, $\mathsf{trans}' = (\mathsf{com}, \mathsf{ch}', \mathsf{resp}')$, where $\mathsf{ch} \neq ch'$

$$\Pr\left[\mathsf{sk} \leftarrow \mathcal{K}(1^k, \mathsf{pk}, \mathsf{trans}, \mathsf{trans}')\right] > 1/p(k).$$

- random challenges can be answered only if Prover knows a witness
- implies soundness and knowledge

Properties of Canonical 3-pass IDS

(statistical) Honest-Verifier Zero-Knowledge

Let $k \in \mathbb{N}$, $\mathrm{IDS} = (\mathrm{KGen}, \mathcal{P}, \mathcal{V})$ 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:

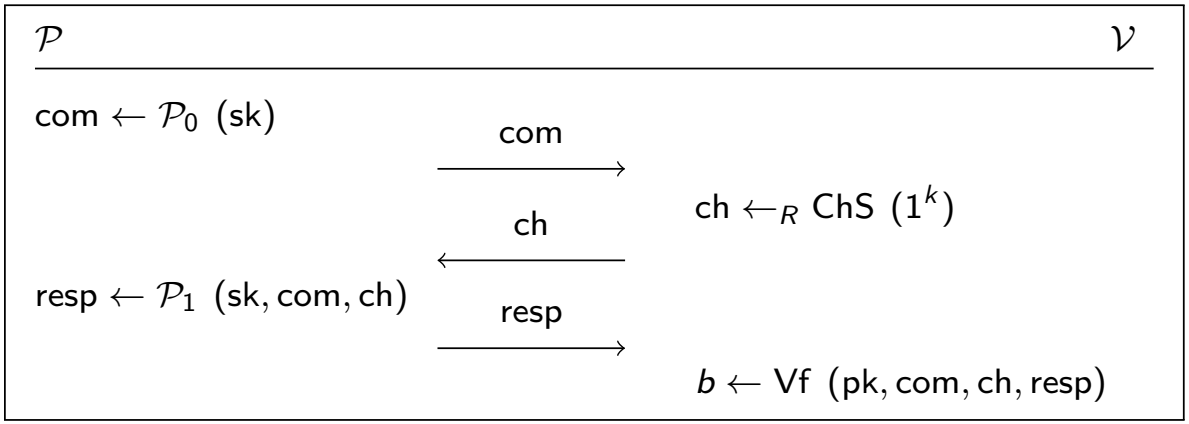
$$\left\{(\mathsf{pk}, \mathsf{sk}) \leftarrow \mathrm{KGen}(1^k) : (\mathsf{sk}, \mathsf{pk}, \mathrm{trans}(\langle \mathcal{P}(\mathsf{sk}), \mathcal{V}(\mathsf{pk}) \rangle))\right\}$$

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

- guaranties no leakage of secret

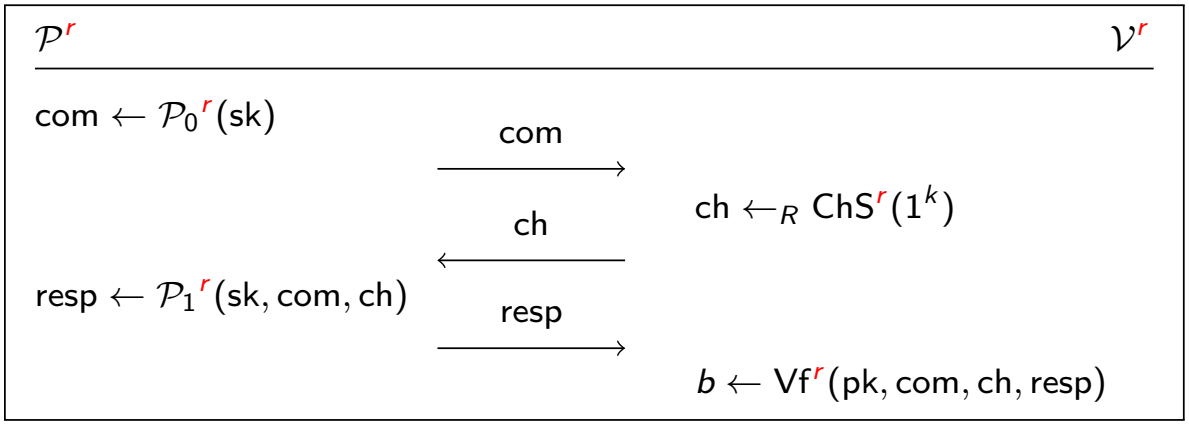
The Fiat-Shamir transform

IDS



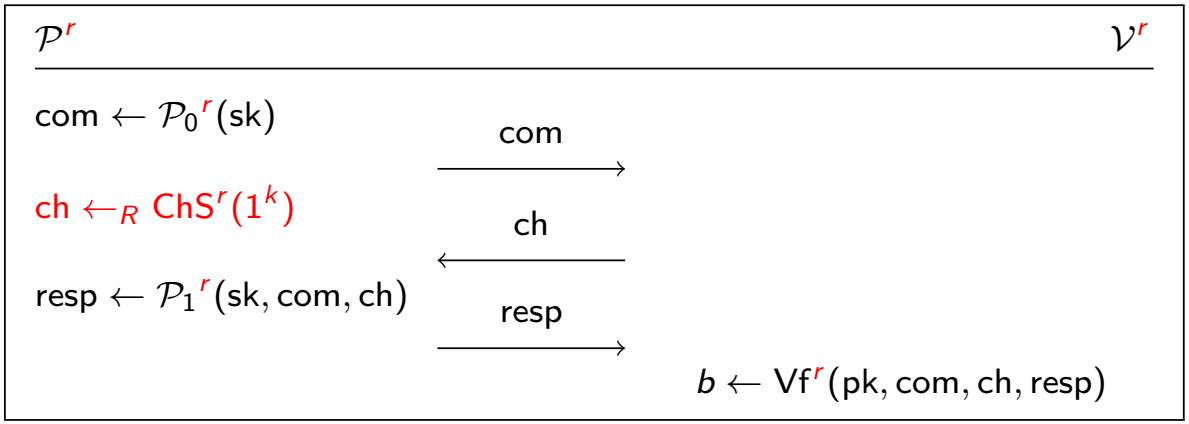
The Fiat-Shamir transform

IDS



The Fiat-Shamir transform

IDS



FS signature

Signer	**Verifier**
com $\leftarrow \mathcal{P}_0(\mathsf{sk})$	
ch $\leftarrow H(m, \mathsf{com})$	ch $\leftarrow H(m, \mathsf{com})$
resp $\leftarrow \mathcal{P}_1(\mathsf{sk}, \mathsf{com}, \mathsf{ch})$	$b \leftarrow \mathsf{Vf}(\mathsf{pk}, \mathsf{com}, \mathsf{ch}, \mathsf{resp})$
output : $\sigma = (\mathsf{com}, \mathsf{resp})$	**output** : b

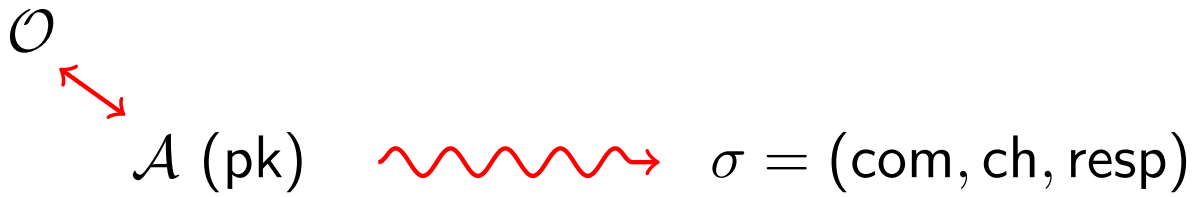
Security of FS signatures [Pointcheval & Stern '96]

IDS		**FS signature**
Special soundness	$\longrightarrow$	Secure under key-only attack

Security of FS signatures [Pointcheval & Stern '96]

IDS → **FS signature**

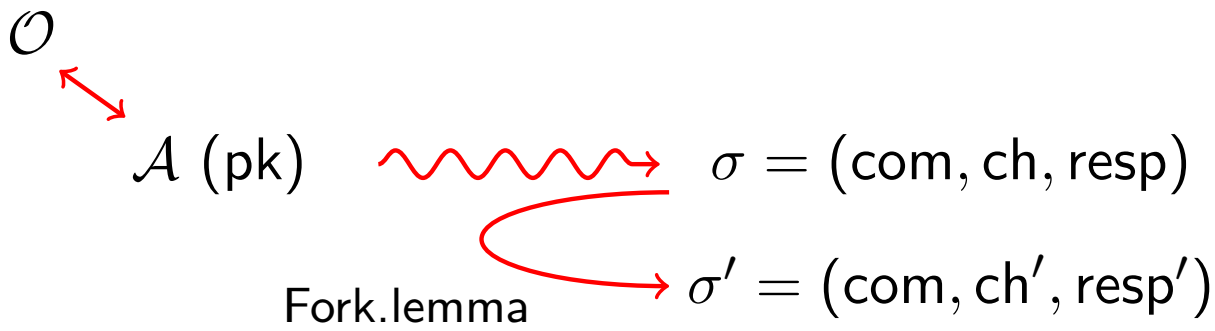
Special soundness ⟶ Secure under key-only attack



Security of FS signatures [Pointcheval & Stern '96]

IDS → **FS signature**

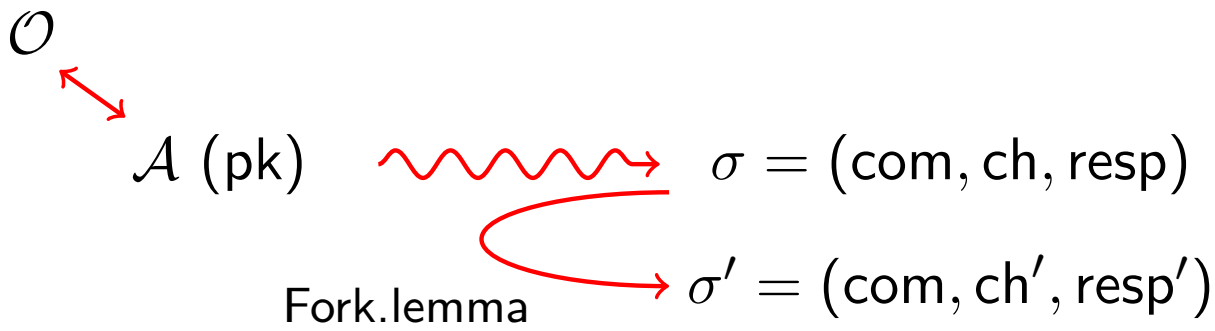
Special soundness ⟶ Secure under key-only attack



Security of FS signatures [Pointcheval & Stern '96]

IDS → **FS signature**

Special soundness ⟶ Secure under key-only attack

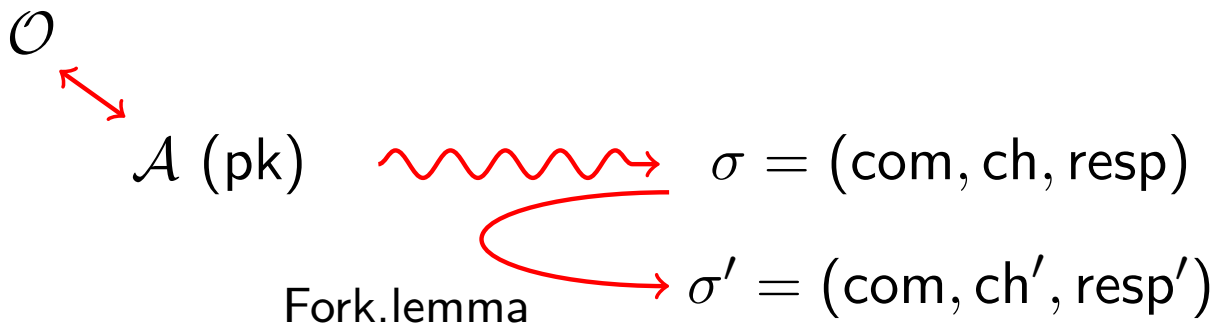


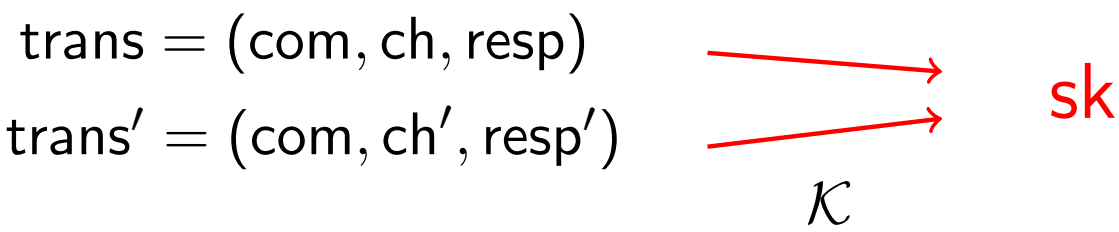
$$\text{trans} = (\text{com}, \text{ch}, \text{resp})$$
$$\text{trans}' = (\text{com}, \text{ch}', \text{resp}')$$

Security of FS signatures [Pointcheval & Stern '96]

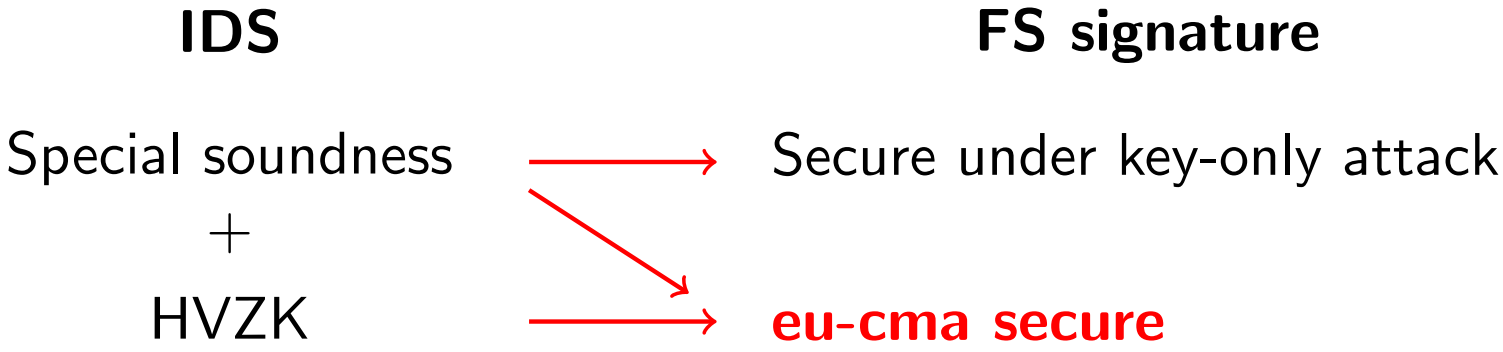
IDS → **FS signature**

Special soundness ⟶ Secure under key-only attack

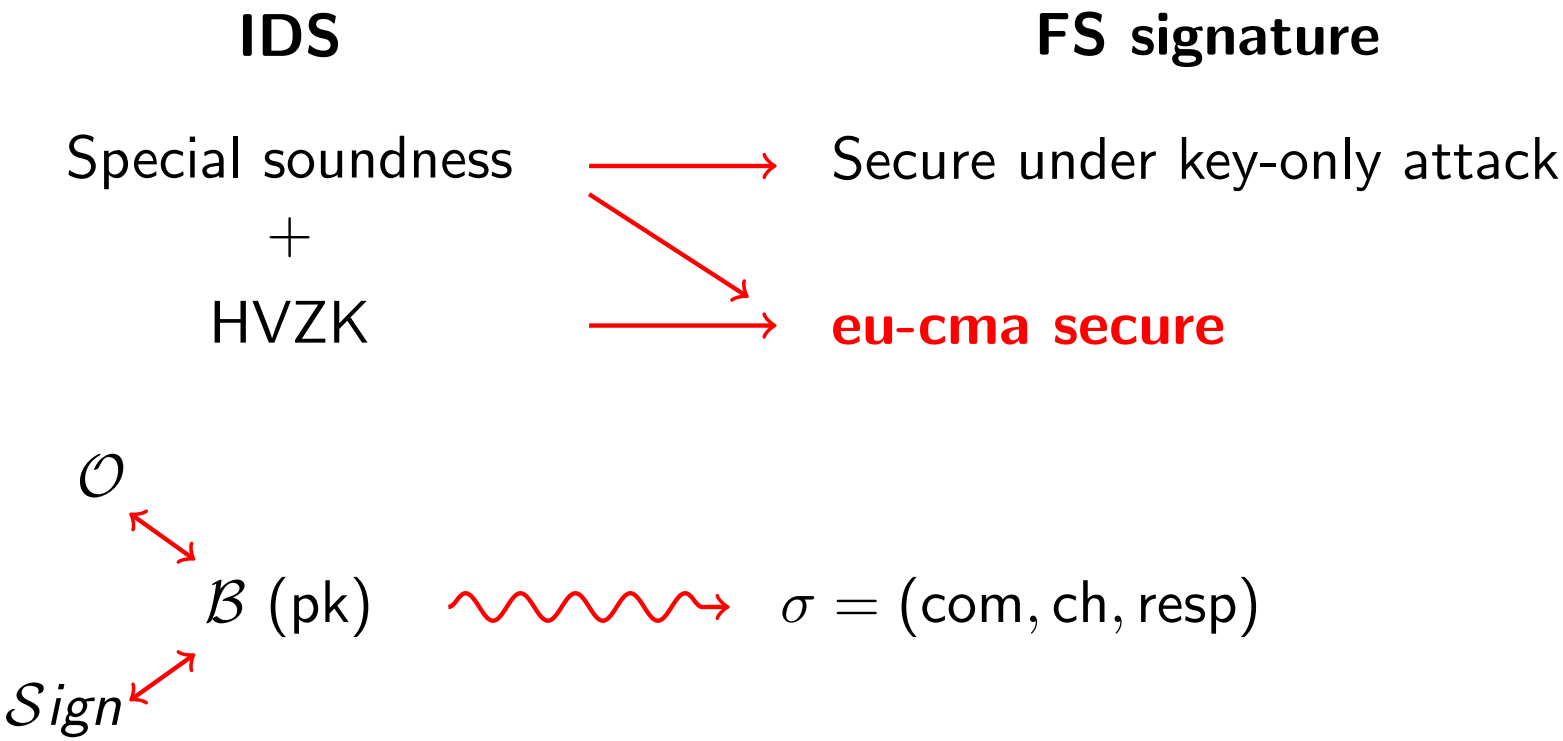




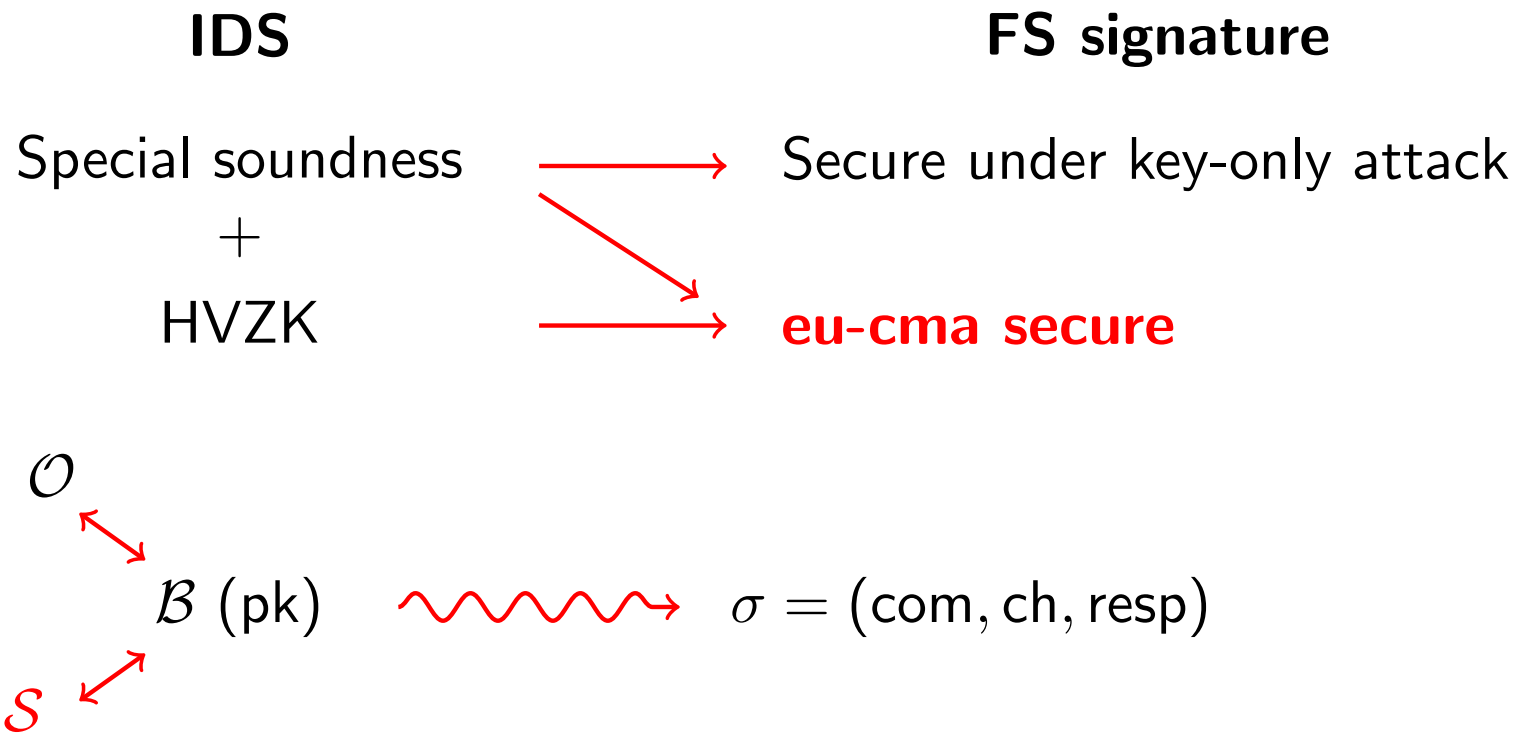
Security of FS signatures [Pointcheval & Stern '96]



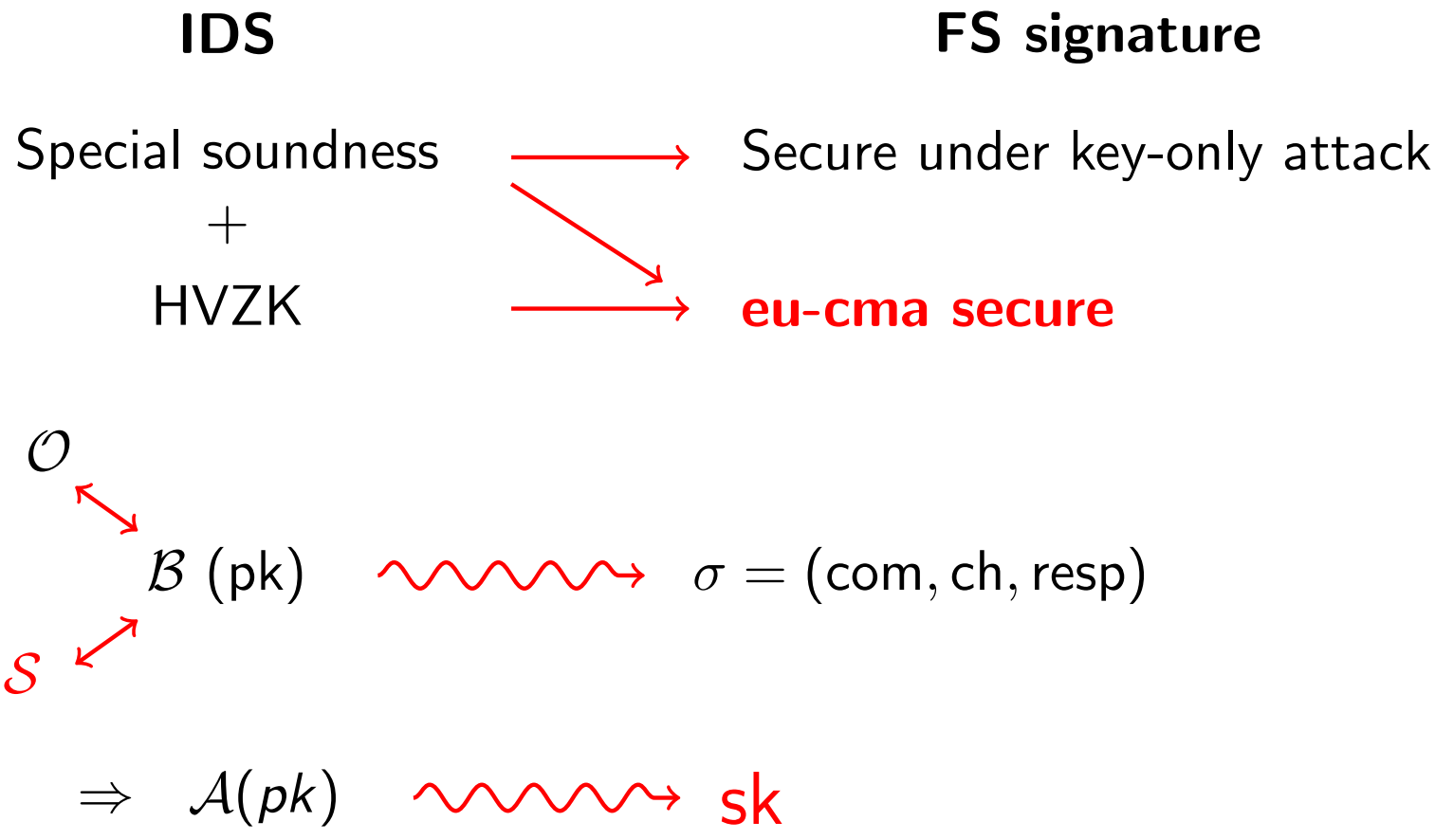
Security of FS signatures [Pointcheval & Stern '96]



Security of FS signatures [Pointcheval & Stern '96]



Security of FS signatures [Pointcheval & Stern '96]



Canonical 5-pass IDS

$\mathcal{P}$		$\mathcal{V}$
$\mathsf{com} \leftarrow \mathcal{P}_0(\mathsf{sk})$	$\xrightarrow{\mathsf{com}}$	
	$\xleftarrow{\mathsf{ch}_1}$	$\mathsf{ch}_1 \leftarrow_R \mathsf{ChS}_1(1^k)$
$\mathsf{resp}_1 \leftarrow \mathcal{P}_1(\mathsf{sk}, \mathsf{com}, \mathsf{ch}_1)$	$\xrightarrow{\mathsf{resp}_1}$	
	$\xleftarrow{\mathsf{ch}_2}$	$\mathsf{ch}_2 \leftarrow_R \mathsf{ChS}_2(1^k)$
$\mathsf{resp}_2 \leftarrow \mathcal{P}_2(\mathsf{sk}, \mathsf{com}, \mathsf{ch}_1, \mathsf{resp}_1, \mathsf{ch}_2)$	$\xrightarrow{\mathsf{resp}_2}$	
		$b \leftarrow \mathsf{Vf}(\mathsf{pk}, \mathsf{com}, \mathsf{ch}_1, \mathsf{resp}_1, \mathsf{ch}_2, \mathsf{resp}_2)$

The Fiat-Shamir transform on 5-pass IDS

IDS

$\mathcal{P}$		$\mathcal{V}$
$\mathsf{com} \leftarrow \mathcal{P}_0(\mathsf{sk})$	$\xrightarrow{\mathsf{com}}$	
	$\xleftarrow{\mathsf{ch}_1}$	$\mathsf{ch}_1 \leftarrow_R \mathsf{ChS}_1(1^k)$
$\mathsf{resp}_1 \leftarrow \mathcal{P}_1(\mathsf{sk}, \mathsf{com}, \mathsf{ch}_1)$	$\xrightarrow{\mathsf{resp}_1}$	
	$\xleftarrow{\mathsf{ch}_2}$	$\mathsf{ch}_2 \leftarrow_R \mathsf{ChS}_2(1^k)$
$\mathsf{resp}_2 \leftarrow \mathcal{P}_2(\mathsf{sk}, \mathsf{com}, \mathsf{ch}_1, \mathsf{resp}_1, \mathsf{ch}_2)$	$\xrightarrow{\mathsf{resp}_2}$	
		$b \leftarrow \mathsf{Vf}(\mathsf{pk}, \mathsf{com}, \mathsf{ch}_1, \mathsf{resp}_1, \mathsf{ch}_2, \mathsf{resp}_2)$

The Fiat-Shamir transform on 5-pass IDS

IDS

$\mathcal{P}$		$\mathcal{V}$
$\mathsf{com} \leftarrow \mathcal{P}_0(\mathsf{sk})$	$\xrightarrow{\mathsf{com}}$	
	$\xleftarrow{\mathsf{ch}_1}$	$\mathsf{ch}_1 \leftarrow_R \mathsf{ChS}_1(1^k)$
$\mathsf{resp}_1 \leftarrow \mathcal{P}_1(\mathsf{sk}, \mathsf{com}, \mathsf{ch}_1)$	$\xrightarrow{\mathsf{resp}_1}$	
	$\xleftarrow{\mathsf{ch}_2}$	$\mathsf{ch}_2 \leftarrow_R \mathsf{ChS}_2(1^k)$
$\mathsf{resp}_2 \leftarrow \mathcal{P}_2(\mathsf{sk}, \mathsf{com}, \mathsf{ch}_1, \mathsf{resp}_1, \mathsf{ch}_2)$	$\xrightarrow{\mathsf{resp}_2}$	
		$b \leftarrow \mathsf{Vf}(\mathsf{pk}, \mathsf{com}, \mathsf{ch}_1, \mathsf{resp}_1, \mathsf{ch}_2, \mathsf{resp}_2)$

FS signature

Signer

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

$\mathsf{ch}_1 \leftarrow H_1(m, \mathsf{com})$

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

$\mathsf{ch}_2 \leftarrow H_2(m, \mathsf{com}, \mathsf{ch}_1, \mathsf{resp}_1)$

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

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

Verifier

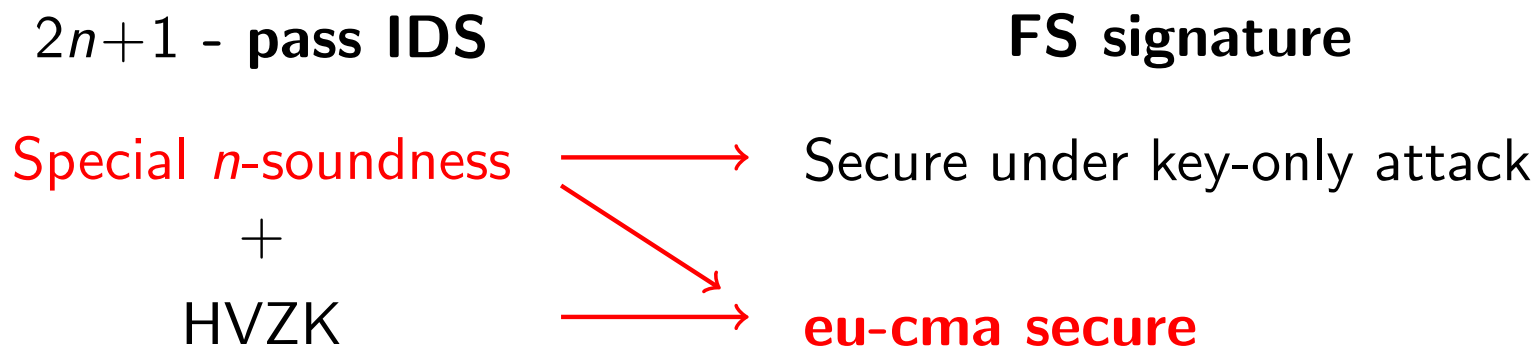
$\mathsf{ch}_1 \leftarrow H_1(m, \mathsf{com})$

$\mathsf{ch}_2 \leftarrow H_2(m, \mathsf{com}, \mathsf{ch}_1, \mathsf{resp}_1)$

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

output : b

El Yousfi et al. '12 proof of security



Special n-Soundness

There exists PPT algorithm $\mathcal{E}$- knowledge extractor s.t. given two accepting transcripts $\text{trans} = (\text{com}, \text{ch}_1, \text{resp}_1, \ldots, \text{ch}_n, \text{resp}_n)$,
$\text{trans}' = (\text{com}, \text{ch}_1, \text{resp}_1, \ldots, \text{ch}'_n, \text{resp}'_n)$, where $\text{ch}_n \neq ch'_n$,

$$\Pr\left[\text{sk} \leftarrow \mathcal{E}(1^k, \text{pk}, \text{trans}, \text{trans}')\right] > 1/p(k).$$

- Proof very similar to Pointcheval & Stern

A problem...

$\mathcal{P}$		$\mathcal{V}$
$\mathsf{com} \leftarrow \mathcal{P}_0(\mathsf{sk})$	$\xrightarrow{\mathsf{com}}$	
	$\xleftarrow{\mathsf{ch}_1}$	$\mathsf{ch}_1 \leftarrow_R \mathsf{ChS}_1(1^k)$
$\mathsf{resp}_1 \leftarrow \mathcal{P}_1(\mathsf{sk}, \mathsf{com}, \mathsf{ch}_1)$		
	$\xrightarrow{\mathsf{resp}_1}$	
	$\xleftarrow{\mathsf{ch}_2}$	$\mathsf{ch}_2 \leftarrow_R \mathsf{ChS}_2(1^k)$
$\mathsf{resp}_2 \leftarrow \mathcal{P}_2(\mathsf{sk}, \mathsf{com}, \mathsf{ch}_1, \mathsf{resp}_1, \mathsf{ch}_2)$	$\xrightarrow{\mathsf{resp}_2}$	
		$b \leftarrow \mathsf{Vf}(\mathsf{pk}, \mathsf{com}, \mathsf{ch}_1, \mathsf{resp}_1, \mathsf{ch}_2, \mathsf{resp}_2)$

A problem...

$\mathcal{P}$		$\mathcal{V}$
$\mathsf{com} \leftarrow \mathcal{P}_0(\mathsf{sk})$	$\xrightarrow{\mathsf{com}}$	
$\mathsf{ch}_1 \leftarrow_R \mathsf{ChS}_1(1^k)$	$\xleftarrow{\mathsf{ch}_1}$	
$\mathsf{resp}_1 \leftarrow \mathcal{P}_1(\mathsf{sk}, \mathsf{com}, \mathsf{ch}_1)$		
	$\xrightarrow{\mathsf{resp}_1}$	
	$\xleftarrow{\mathsf{ch}_2}$	$\mathsf{ch}_2 \leftarrow_R \mathsf{ChS}_2(1^k)$
$\mathsf{resp}_2 \leftarrow \mathcal{P}_2(\mathsf{sk}, \mathsf{com}, \mathsf{ch}_1, \mathsf{resp}_1, \mathsf{ch}_2)$	$\xrightarrow{\mathsf{resp}_2}$	
		$b \leftarrow \mathsf{Vf}(\mathsf{pk}, \mathsf{com}, \mathsf{ch}_1, \mathsf{resp}_1, \mathsf{ch}_2, \mathsf{resp}_2)$

A problem...

$\mathcal{P}$		$\mathcal{V}$
$\mathsf{com} \leftarrow \mathcal{P}_0(\mathsf{sk})$	$\xrightarrow{\mathsf{com}}$	
$\mathsf{ch}_1 \leftarrow_R \mathsf{ChS}_1(1^k)$	$\xleftarrow{\mathsf{ch}_1}$	
$\mathsf{resp}_1 \leftarrow \mathcal{P}_1(\mathsf{sk}, \mathsf{com}, \mathsf{ch}_1)$		
$\mathsf{com}' = (\mathsf{com}, \mathsf{ch}_1, \mathsf{resp}_1)$	$\xrightarrow{\mathsf{resp}_1}$	
	$\xleftarrow{\mathsf{ch}_2}$	$\mathsf{ch}_2 \leftarrow_R \mathsf{ChS}_2(1^k)$
$\mathsf{resp}_2 \leftarrow \mathcal{P}_2(\mathsf{sk}, \mathsf{com}, \mathsf{ch}_1, \mathsf{resp}_1, \mathsf{ch}_2)$	$\xrightarrow{\mathsf{resp}_2}$	
		$b \leftarrow \mathsf{Vf}(\mathsf{pk}, \mathsf{com}, \mathsf{ch}_1, \mathsf{resp}_1, \mathsf{ch}_2, \mathsf{resp}_2)$

A problem...

$\mathcal{P}$		$\mathcal{V}$
$\mathsf{com} \leftarrow \mathcal{P}_0(\mathsf{sk})$		
$\mathsf{ch}_1 \leftarrow_R \mathsf{ChS}_1(1^k)$		
$\mathsf{resp}_1 \leftarrow \mathcal{P}_1(\mathsf{sk}, \mathsf{com}, \mathsf{ch}_1)$		
$\mathsf{com}' = (\mathsf{com}, \mathsf{ch}_1, \mathsf{resp}_1)$	$\xrightarrow{\mathsf{com}'}$	
	$\xleftarrow{\mathsf{ch}_2}$	$\mathsf{ch}_2 \leftarrow_R \mathsf{ChS}_2(1^k)$
$\mathsf{resp}_2 \leftarrow \mathcal{P}_2(\mathsf{sk}, \mathsf{com}, \mathsf{ch}_1, \mathsf{resp}_1, \mathsf{ch}_2)$	$\xrightarrow{\mathsf{resp}_2}$	
		$b \leftarrow \mathsf{Vf}(\mathsf{pk}, \mathsf{com}, \mathsf{ch}_1, \mathsf{resp}_1, \mathsf{ch}_2, \mathsf{resp}_2)$

A problem...

$\mathcal{P}$		$\mathcal{V}$
$\mathsf{com} \leftarrow \mathcal{P}_0(\mathsf{sk})$		
$\mathsf{ch}_1 \leftarrow_R \mathsf{ChS}_1(1^k)$		
$\mathsf{resp}_1 \leftarrow \mathcal{P}_1(\mathsf{sk}, \mathsf{com}, \mathsf{ch}_1)$		
$\mathsf{com}' = (\mathsf{com}, \mathsf{ch}_1, \mathsf{resp}_1)$	$\xrightarrow{\mathsf{com}'}$	
	$\xleftarrow{\mathsf{ch}_2}$	$\mathsf{ch}_2 \leftarrow_R \mathsf{ChS}_2(1^k)$
$\mathsf{resp}_2 \leftarrow \mathcal{P}_2(\mathsf{sk}, \mathsf{com}, \mathsf{ch}_1, \mathsf{resp}_1, \mathsf{ch}_2)$	$\xrightarrow{\mathsf{resp}_2}$	
		$b \leftarrow \mathsf{Vf}(\mathsf{pk}, \mathsf{com}, \mathsf{ch}_1, \mathsf{resp}_1, \mathsf{ch}_2, \mathsf{resp}_2)$

- Every $2n+1$ - pass can be turned into 3-pass!
  - HVZK preserved - Same simulator $\mathcal{S}$
  - Special n-soundness $\rightarrow$ special soundness - Same extractor $\mathcal{K}$
- How come nobody noticed?

Recall Sakumoto et al. 5-pass IDS

$\mathcal{P}(\mathbf{F}, \mathbf{v}, \mathbf{s})$		$\mathcal{V}(\mathbf{F}, \mathbf{v})$
$\mathbf{r}_0, \mathbf{t}_0 \leftarrow_R \mathbb{F}_q^n, \mathbf{e}_0 \leftarrow_R \mathbb{F}_q^m$		
$\mathbf{r}_1 \leftarrow \mathbf{s} - \mathbf{r}_0$		
$c_0 \leftarrow Com(\mathbf{r}_0, \mathbf{t}_0, \mathbf{e}_0)$		
$c_1 \leftarrow Com(\mathbf{r}_1, \mathbf{G}(\mathbf{t}_0, \mathbf{r}_1) + \mathbf{e}_0)$	$\xrightarrow{(c_0, c_1)}$	
		$\alpha \leftarrow_R \mathbb{F}_q$
	$\xleftarrow{\alpha}$	
$\mathbf{t}_1 \leftarrow \alpha\mathbf{r}_0 - \mathbf{t}_0$		
$\mathbf{e}_1 \leftarrow \alpha\mathbf{F}(\mathbf{r}_0) - \mathbf{e}_0$	$\xrightarrow{\text{resp}_1 = (\mathbf{t}_1, \mathbf{e}_1)}$	
		$\text{ch}_2 \leftarrow_R \{0, 1\}$
	$\xleftarrow{\text{ch}_2}$	
If $\text{ch}_2 = 0$, $\text{resp}_2 \leftarrow \mathbf{r}_0$		
Else $\text{resp}_2 \leftarrow \mathbf{r}_1$	$\xrightarrow{\text{resp}_2}$	
		If $\text{ch}_2 = 0$, Parse $\text{resp}_2 = \mathbf{r}_0$, check
		$c_0 \stackrel{?}{=} Com(\mathbf{r}_0, \alpha\mathbf{r}_0 - \mathbf{t}_1, \alpha\mathbf{F}(\mathbf{r}_0) - \mathbf{e}_1)$
		Else Parse $\text{resp}_2 = \mathbf{r}_1$, check
		$c_1 \stackrel{?}{=} Com(\mathbf{r}_1, \alpha(\mathbf{v} - \mathbf{F}(\mathbf{r}_1)) - \mathbf{G}(\mathbf{t}_1, \mathbf{r}_1) - \mathbf{e}_1)$

Sakumoto et al. 5-pass IDS does not fulfill special 2-soundness!

$\mathcal{A}(\mathbf{F}, \mathbf{v})$	$\mathcal{V}(\mathbf{F}, \mathbf{v})$

$\mathbf{s}, \mathbf{r}_0, \mathbf{t}_0 \leftarrow_R \mathbb{F}_q^n, \mathbf{e}_0 \leftarrow_R \mathbb{F}_q^m$

$\alpha \leftarrow_R \mathbb{F}_q$

$\mathbf{r}_1 \leftarrow \mathbf{s} - \mathbf{r}_0$

$\mathbf{t}_1 \leftarrow \alpha \mathbf{r}_0 - \mathbf{t}_0$

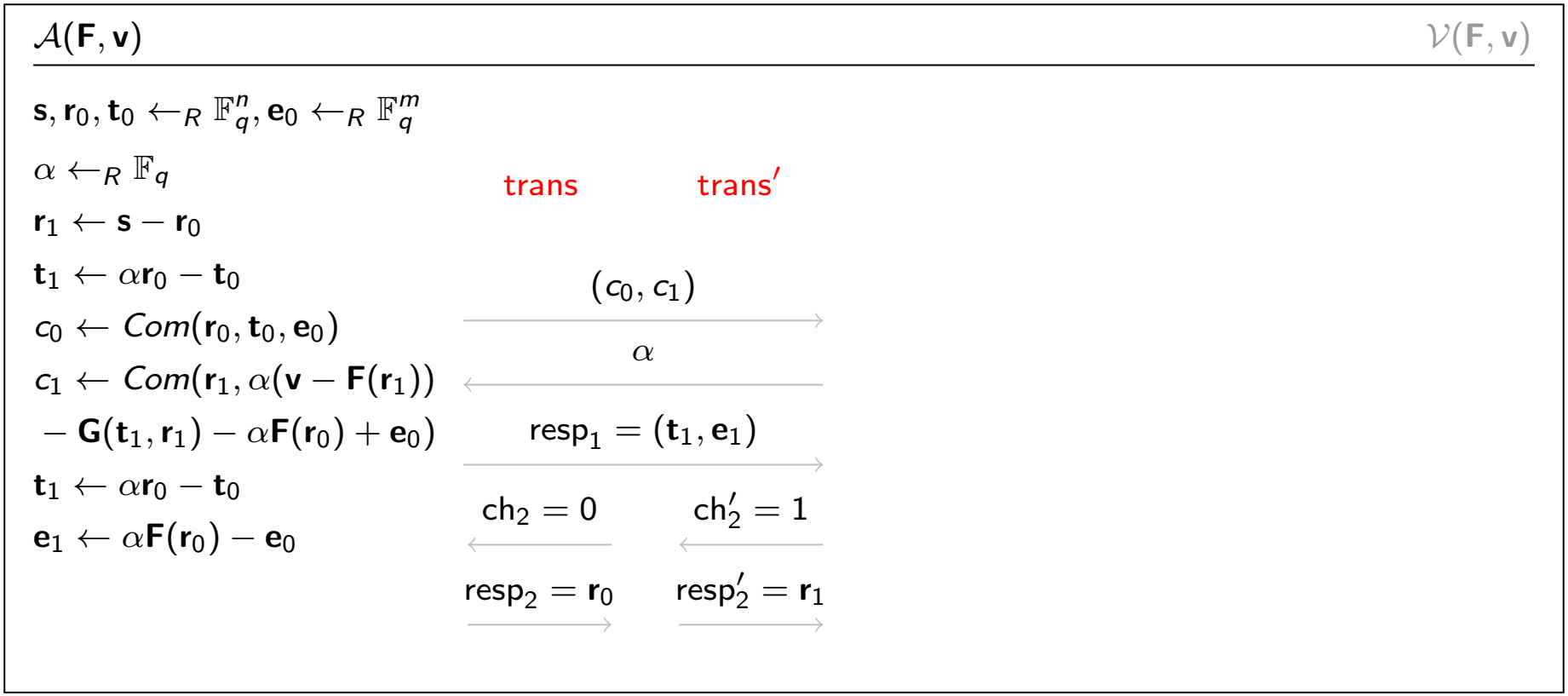
$c_0 \leftarrow Com(\mathbf{r}_0, \mathbf{t}_0, \mathbf{e}_0)$

$c_1 \leftarrow Com(\mathbf{r}_1, \alpha(\mathbf{v} - \mathbf{F}(\mathbf{r}_1))$
$- \mathbf{G}(\mathbf{t}_1, \mathbf{r}_1) - \alpha \mathbf{F}(\mathbf{r}_0) + \mathbf{e}_0)$

$\mathbf{t}_1 \leftarrow \alpha \mathbf{r}_0 - \mathbf{t}_0$

$\mathbf{e}_1 \leftarrow \alpha \mathbf{F}(\mathbf{r}_0) - \mathbf{e}_0$

Sakumoto et al. 5-pass IDS does not fulfill special 2-soundness!



Sakumoto et al. 5-pass IDS does not fulfill special 2-soundness!

$\mathcal{A}(\mathbf{F}, \mathbf{v})$		$\mathcal{V}(\mathbf{F}, \mathbf{v})$
$\mathbf{s}, \mathbf{r}_0, \mathbf{t}_0 \leftarrow_R \mathbb{F}_q^n, \mathbf{e}_0 \leftarrow_R \mathbb{F}_q^m$		
$\alpha \leftarrow_R \mathbb{F}_q$	trans trans$'$	
$\mathbf{r}_1 \leftarrow \mathbf{s} - \mathbf{r}_0$		
$\mathbf{t}_1 \leftarrow \alpha\mathbf{r}_0 - \mathbf{t}_0$	(c_0, c_1) $\longrightarrow$	
$c_0 \leftarrow Com(\mathbf{r}_0, \mathbf{t}_0, \mathbf{e}_0)$	α $\longleftarrow$	
$c_1 \leftarrow Com(\mathbf{r}_1, \alpha(\mathbf{v} - \mathbf{F}(\mathbf{r}_1)) - \mathbf{G}(\mathbf{t}_1, \mathbf{r}_1) - \alpha\mathbf{F}(\mathbf{r}_0) + \mathbf{e}_0)$	$\text{resp}_1 = (\mathbf{t}_1, \mathbf{e}_1)$ $\longrightarrow$	
$\mathbf{t}_1 \leftarrow \alpha\mathbf{r}_0 - \mathbf{t}_0$	$\text{ch}_2 = 0$ $\longleftarrow$ $\quad$ $\text{ch}_2' = 1$ $\longleftarrow$	trans valid!
$\mathbf{e}_1 \leftarrow \alpha\mathbf{F}(\mathbf{r}_0) - \mathbf{e}_0$		$\mathbf{t}_0 = \alpha\mathbf{r}_0 - \mathbf{t}_1, \mathbf{e}_0 = \alpha\mathbf{F}(\mathbf{r}_0) - \mathbf{e}_1$
	$\text{resp}_2 = \mathbf{r}_0$ $\longrightarrow$ $\quad$ $\text{resp}_2' = \mathbf{r}_1$ $\longrightarrow$	trans$'$ valid!
		$\alpha(\mathbf{v} - \mathbf{F}(\mathbf{r}_1)) - \mathbf{G}(\mathbf{t}_1, \mathbf{r}_1) - \mathbf{e}_1 =$
		$\alpha(\mathbf{v} - \mathbf{F}(\mathbf{r}_1)) - -\mathbf{G}(\mathbf{t}_1, \mathbf{r}_1) - \alpha\mathbf{F}(\mathbf{r}_0) + \mathbf{e}_0$

Sakumoto et al. 5-pass IDS does not fulfill special 2-soundness!

$\mathcal{A}(\mathbf{F}, \mathbf{v})$		$\mathcal{V}(\mathbf{F}, \mathbf{v})$
$\mathbf{s}, \mathbf{r}_0, \mathbf{t}_0 \leftarrow_R \mathbb{F}_q^n, \mathbf{e}_0 \leftarrow_R \mathbb{F}_q^m$		
$\alpha \leftarrow_R \mathbb{F}_q$	trans trans′	
$\mathbf{r}_1 \leftarrow \mathbf{s} - \mathbf{r}_0$		
$\mathbf{t}_1 \leftarrow \alpha\mathbf{r}_0 - \mathbf{t}_0$	(c_0, c_1) →	
$c_0 \leftarrow Com(\mathbf{r}_0, \mathbf{t}_0, \mathbf{e}_0)$		
$c_1 \leftarrow Com(\mathbf{r}_1, \alpha(\mathbf{v} - \mathbf{F}(\mathbf{r}_1)) - \mathbf{G}(\mathbf{t}_1, \mathbf{r}_1) - \alpha\mathbf{F}(\mathbf{r}_0) + \mathbf{e}_0)$	← α	
	$\text{resp}_1 = (\mathbf{t}_1, \mathbf{e}_1)$ →	
$\mathbf{t}_1 \leftarrow \alpha\mathbf{r}_0 - \mathbf{t}_0$		trans valid!
$\mathbf{e}_1 \leftarrow \alpha\mathbf{F}(\mathbf{r}_0) - \mathbf{e}_0$	$\text{ch}_2 = 0$ ← $\quad$ $\text{ch}_2' = 1$ ←	$\mathbf{t}_0 = \alpha\mathbf{r}_0 - \mathbf{t}_1, \mathbf{e}_0 = \alpha\mathbf{F}(\mathbf{r}_0) - \mathbf{e}_1$
	$\text{resp}_2 = \mathbf{r}_0$ → $\quad$ $\text{resp}_2' = \mathbf{r}_1$ →	trans′ valid!
		$\alpha(\mathbf{v} - \mathbf{F}(\mathbf{r}_1)) - \mathbf{G}(\mathbf{t}_1, \mathbf{r}_1) - \mathbf{e}_1 =$
		$\alpha(\mathbf{v} - \mathbf{F}(\mathbf{r}_1)) - -\mathbf{G}(\mathbf{t}_1, \mathbf{r}_1) - \alpha\mathbf{F}(\mathbf{r}_0) + \mathbf{e}_0$

$$\mathcal{K}(\text{trans}, \text{trans}') \longrightarrow \text{sk} = \mathbf{s}' \quad \text{s.t. } \mathbf{F}(\mathbf{s}') = \mathbf{v}$$

Sakumoto et al. 5-pass IDS does not fulfill special 2-soundness!

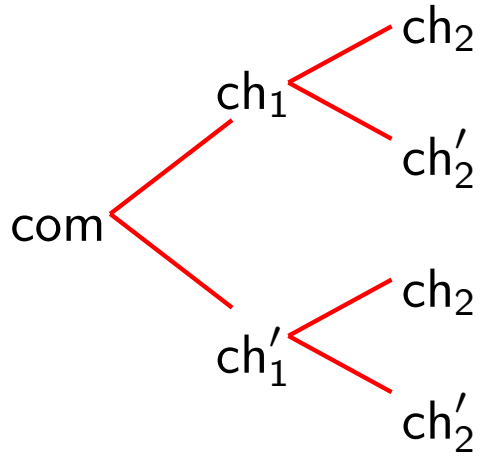
$\mathcal{A}(\mathbf{F}, \mathbf{v})$		$\mathcal{V}(\mathbf{F}, \mathbf{v})$
$\mathbf{s}, \mathbf{r}_0, \mathbf{t}_0 \leftarrow_R \mathbb{F}_q^n, \mathbf{e}_0 \leftarrow_R \mathbb{F}_q^m$		
$\alpha \leftarrow_R \mathbb{F}_q$	trans trans′	
$\mathbf{r}_1 \leftarrow \mathbf{s} - \mathbf{r}_0$		
$\mathbf{t}_1 \leftarrow \alpha\mathbf{r}_0 - \mathbf{t}_0$	$(c_0, c_1) \longrightarrow$	
$c_0 \leftarrow Com(\mathbf{r}_0, \mathbf{t}_0, \mathbf{e}_0)$	$\longleftarrow \alpha$	
$c_1 \leftarrow Com(\mathbf{r}_1, \alpha(\mathbf{v} - \mathbf{F}(\mathbf{r}_1))$		
$- \mathbf{G}(\mathbf{t}_1, \mathbf{r}_1) - \alpha\mathbf{F}(\mathbf{r}_0) + \mathbf{e}_0)$	$\text{resp}_1 = (\mathbf{t}_1, \mathbf{e}_1) \longrightarrow$	
$\mathbf{t}_1 \leftarrow \alpha\mathbf{r}_0 - \mathbf{t}_0$		trans valid!
$\mathbf{e}_1 \leftarrow \alpha\mathbf{F}(\mathbf{r}_0) - \mathbf{e}_0$	$\text{ch}_2 = 0 \longleftarrow$ $\text{ch}_2' = 1 \longleftarrow$	$\mathbf{t}_0 = \alpha\mathbf{r}_0 - \mathbf{t}_1, \mathbf{e}_0 = \alpha\mathbf{F}(\mathbf{r}_0) - \mathbf{e}_1$
	$\text{resp}_2 = \mathbf{r}_0 \longrightarrow$ $\text{resp}_2' = \mathbf{r}_1 \longrightarrow$	trans′ valid!
		$\alpha(\mathbf{v} - \mathbf{F}(\mathbf{r}_1)) - \mathbf{G}(\mathbf{t}_1, \mathbf{r}_1) - \mathbf{e}_1 =$
		$\alpha(\mathbf{v} - \mathbf{F}(\mathbf{r}_1)) - -\mathbf{G}(\mathbf{t}_1, \mathbf{r}_1) - \alpha\mathbf{F}(\mathbf{r}_0) + \mathbf{e}_0$

$$\mathcal{K}(\text{trans}, \text{trans}') \longrightarrow \text{sk} = \mathbf{s}'$$
$$\text{s.t. } \mathbf{F}(\mathbf{s}') = \mathbf{v} \Rightarrow \mathcal{MQ} \textbf{ problem solved!}$$

Sakumoto et al. 5-pass IDS

The extractor $\mathcal{K}$ **needs 4 valid transcripts!**

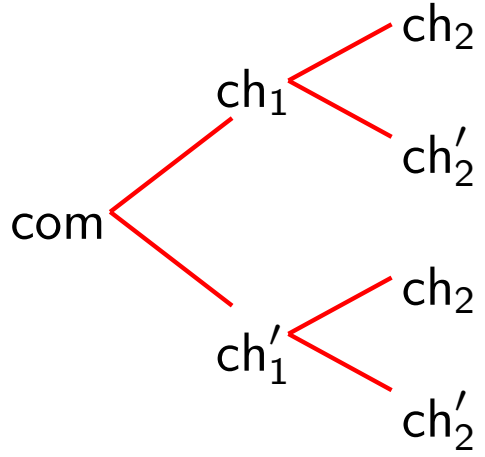
$(\mathsf{com}, \mathsf{ch}_1, \mathsf{resp}_1, \mathsf{ch}_2, \mathsf{resp}_2)$
$(\mathsf{com}, \mathsf{ch}_1, \mathsf{resp}_1, \mathsf{ch}_2', \mathsf{resp}_2')$
$(\mathsf{com}, \mathsf{ch}_1', \mathsf{resp}_1', \mathsf{ch}_2, \mathsf{resp}_2'')$
$(\mathsf{com}, \mathsf{ch}_1', \mathsf{resp}_1', \mathsf{ch}_2', \mathsf{resp}_2''')$



Sakumoto et al. 5-pass IDS

The extractor $\mathcal{K}$ **needs 4 valid transcripts!**

$(\text{com}, \text{ch}_1, \text{resp}_1, \text{ch}_2, \text{resp}_2)$
$(\text{com}, \text{ch}_1, \text{resp}_1, \text{ch}_2', \text{resp}_2')$
$(\text{com}, \text{ch}_1', \text{resp}_1', \text{ch}_2, \text{resp}_2'')$
$(\text{com}, \text{ch}_1', \text{resp}_1', \text{ch}_2', \text{resp}_2''')$



- Focus attention on 5-pass IDS with second challenge space $|\text{ChS}_2| = 2$
  - Sakumoto et al. 5-pass IDS is such
  - Most in the literature are such

Note: El Yousfi et al. amended their error in [Dagdelen et al. '16]

$q2$ - IDS

$\mathcal{P}$		$\mathcal{V}$
$\mathsf{com} \leftarrow \mathcal{P}_0(\mathsf{sk})$	$\xrightarrow{\mathsf{com}}$	
	$\xleftarrow{\mathsf{ch}_1}$	$\mathsf{ch}_1 \leftarrow_R \mathsf{ChS}_1(1^k) \quad \lvert\mathsf{ChS}_1(1^k)\rvert = q$
$\mathsf{resp}_1 \leftarrow \mathcal{P}_1(\mathsf{sk}, \mathsf{com}, \mathsf{ch}_1)$	$\xrightarrow{\mathsf{resp}_1}$	
	$\xleftarrow{\mathsf{ch}_2}$	$\mathsf{ch}_2 \leftarrow_R \mathsf{ChS}_2(1^k) \quad \lvert\mathsf{ChS}_2(1^k)\rvert = 2$
$\mathsf{resp}_2 \leftarrow \mathcal{P}_2(\mathsf{sk}, \mathsf{com}, \mathsf{ch}_1, \mathsf{resp}_1, \mathsf{ch}_2)$	$\xrightarrow{\mathsf{resp}_2}$	
		$b \leftarrow \mathsf{Vf}(\mathsf{pk}, \mathsf{com}, \mathsf{ch}_1, \mathsf{resp}_1, \mathsf{ch}_2, \mathsf{resp}_2)$

$q2$-Extractor

Given pk of a $q2$-IDS, and four accepting transcripts $(\mathsf{com}, \mathsf{ch}_1, \mathsf{resp}_1, \mathsf{ch}_2, \mathsf{resp}_2)$, $(\mathsf{com}, \mathsf{ch}_1, \mathsf{resp}_1, \mathsf{ch}_2', \mathsf{resp}_2')$, $(\mathsf{com}, \mathsf{ch}_1', \mathsf{resp}_1', \mathsf{ch}_2, \mathsf{resp}_2'')$, $(\mathsf{com}, \mathsf{ch}_1', \mathsf{resp}_1', \mathsf{ch}_2', \mathsf{resp}_2''')$, with $\mathsf{ch}_1 \neq \mathsf{ch}_1'$, $\mathsf{ch}_2 \neq \mathsf{ch}_2'$,
a $q2$-Extractor $\mathcal{K}$ outputs a matching secret key sk with non-negligible probability.

The Fiat-Shamir transform on 5-pass IDS

IDS

$\mathcal{P}$		$\mathcal{V}$
$\mathsf{com} \leftarrow \mathcal{P}_0(\mathsf{sk})$	$\xrightarrow{\mathsf{com}}$	
	$\xleftarrow{\mathsf{ch}_1}$	$\mathsf{ch}_1 \leftarrow_R \mathsf{ChS}_1(1^k)$
$\mathsf{resp}_1 \leftarrow \mathcal{P}_1(\mathsf{sk}, \mathsf{com}, \mathsf{ch}_1)$	$\xrightarrow{\mathsf{resp}_1}$	
	$\xleftarrow{\mathsf{ch}_2}$	$\mathsf{ch}_2 \leftarrow_R \mathsf{ChS}_2(1^k)$
$\mathsf{resp}_2 \leftarrow \mathcal{P}_2(\mathsf{sk}, \mathsf{com}, \mathsf{ch}_1, \mathsf{resp}_1, \mathsf{ch}_2)$	$\xrightarrow{\mathsf{resp}_2}$	
		$b \leftarrow \mathsf{Vf}(\mathsf{pk}, \mathsf{com}, \mathsf{ch}_1, \mathsf{resp}_1, \mathsf{ch}_2, \mathsf{resp}_2)$

FS signature

Signer

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

$\mathsf{ch}_1 \leftarrow H_1(m, \mathsf{com})$

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

$\mathsf{ch}_2 \leftarrow H_2(m, \mathsf{com}, \mathsf{ch}_1, \mathsf{resp}_1)$

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

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

Verifier

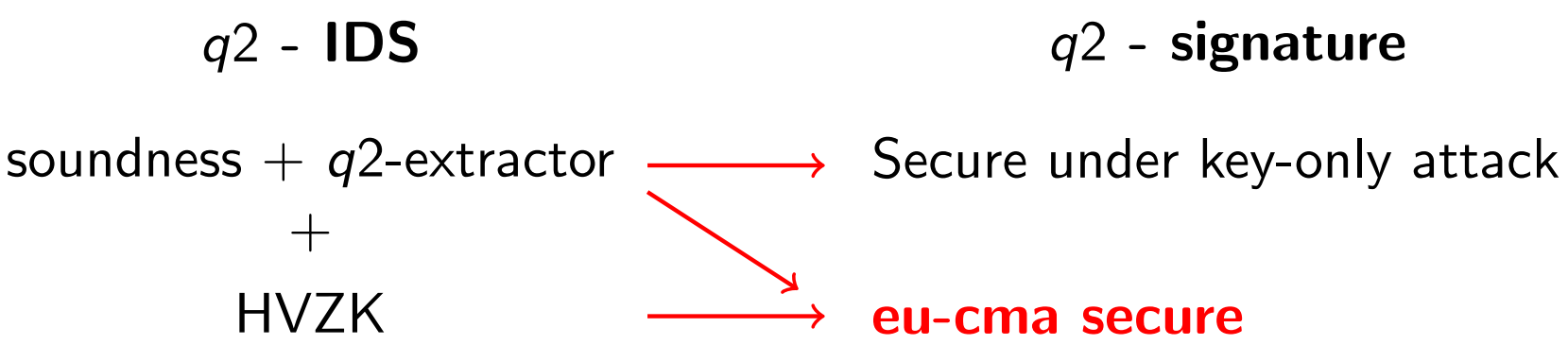
$\mathsf{ch}_1 \leftarrow H_1(m, \mathsf{com})$

$\mathsf{ch}_2 \leftarrow H_2(m, \mathsf{com}, \mathsf{ch}_1, \mathsf{resp}_1)$

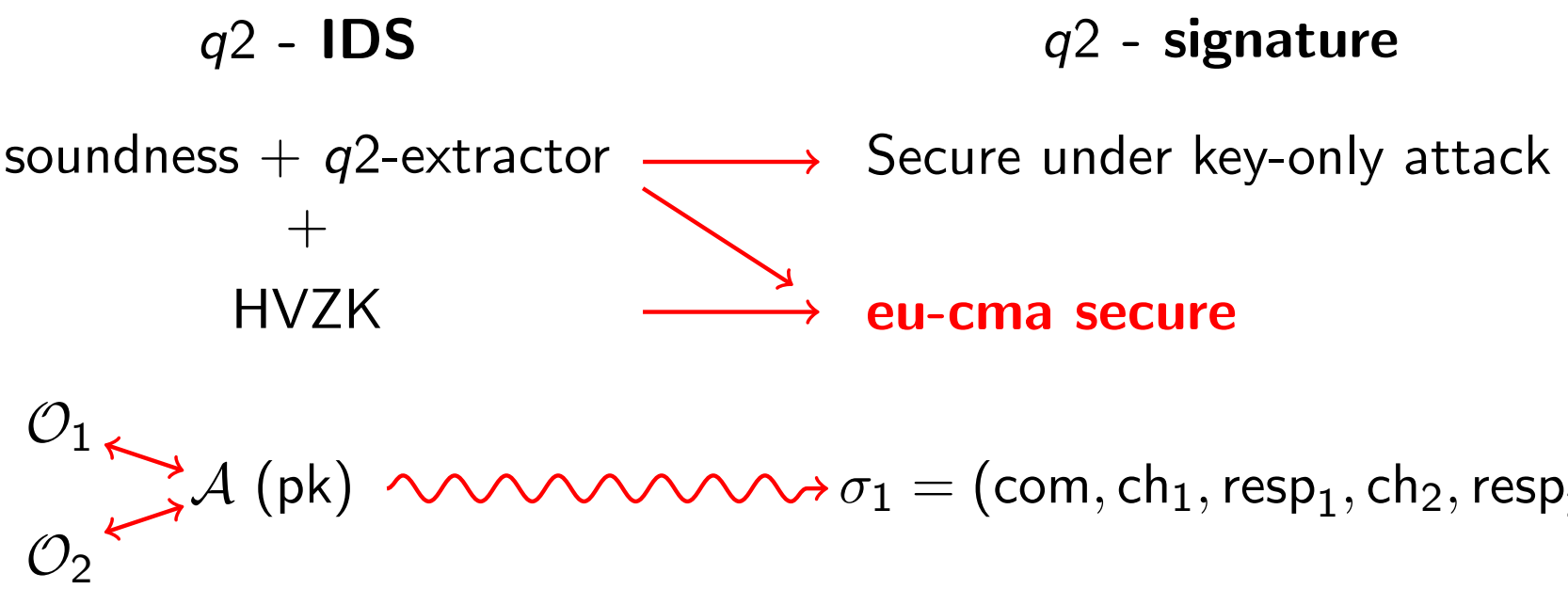
$b \leftarrow \mathsf{Vf}(\mathsf{pk}, \mathsf{com}, \mathsf{ch}_1, \mathsf{resp}_1, \mathsf{ch}_2, \mathsf{resp}_2)$

output : b

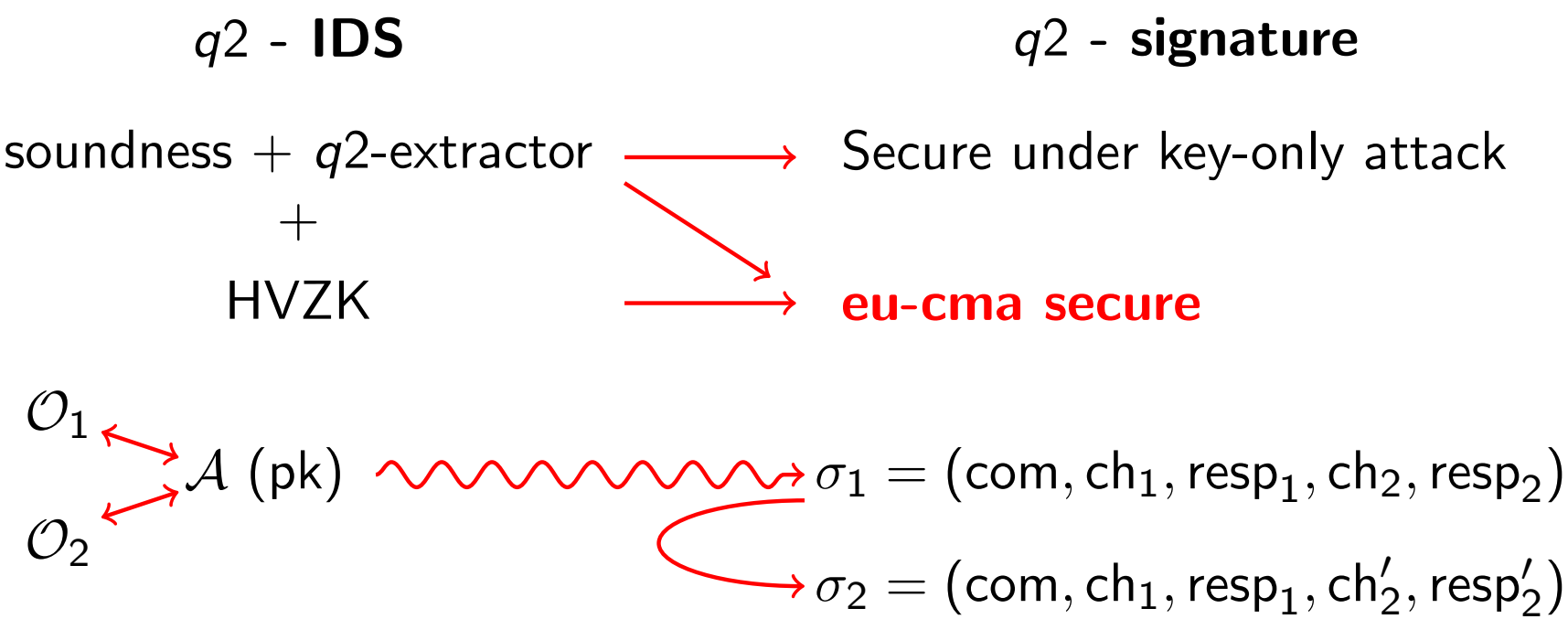
Security of $q2$ - signatures



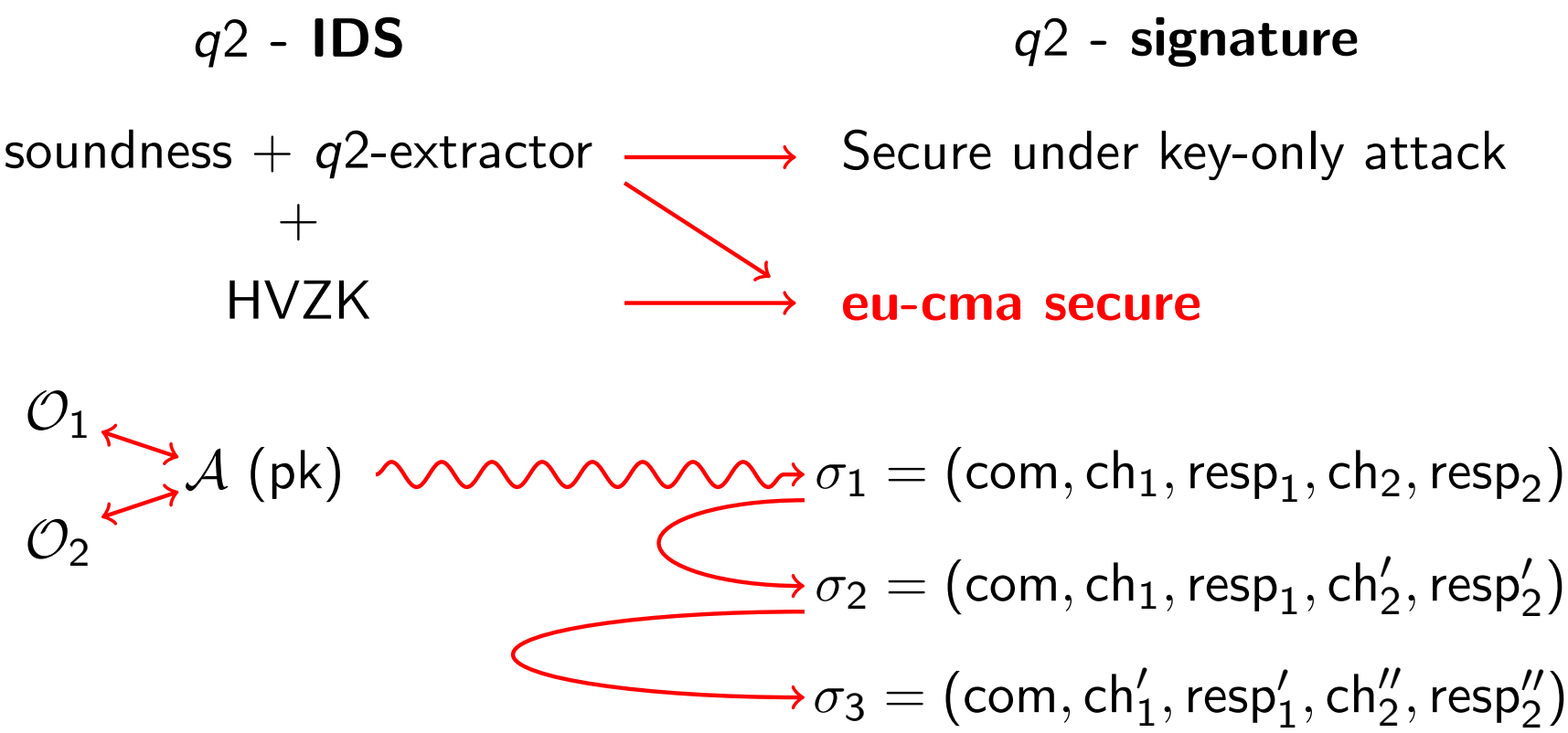
Security of $q2$ - signatures



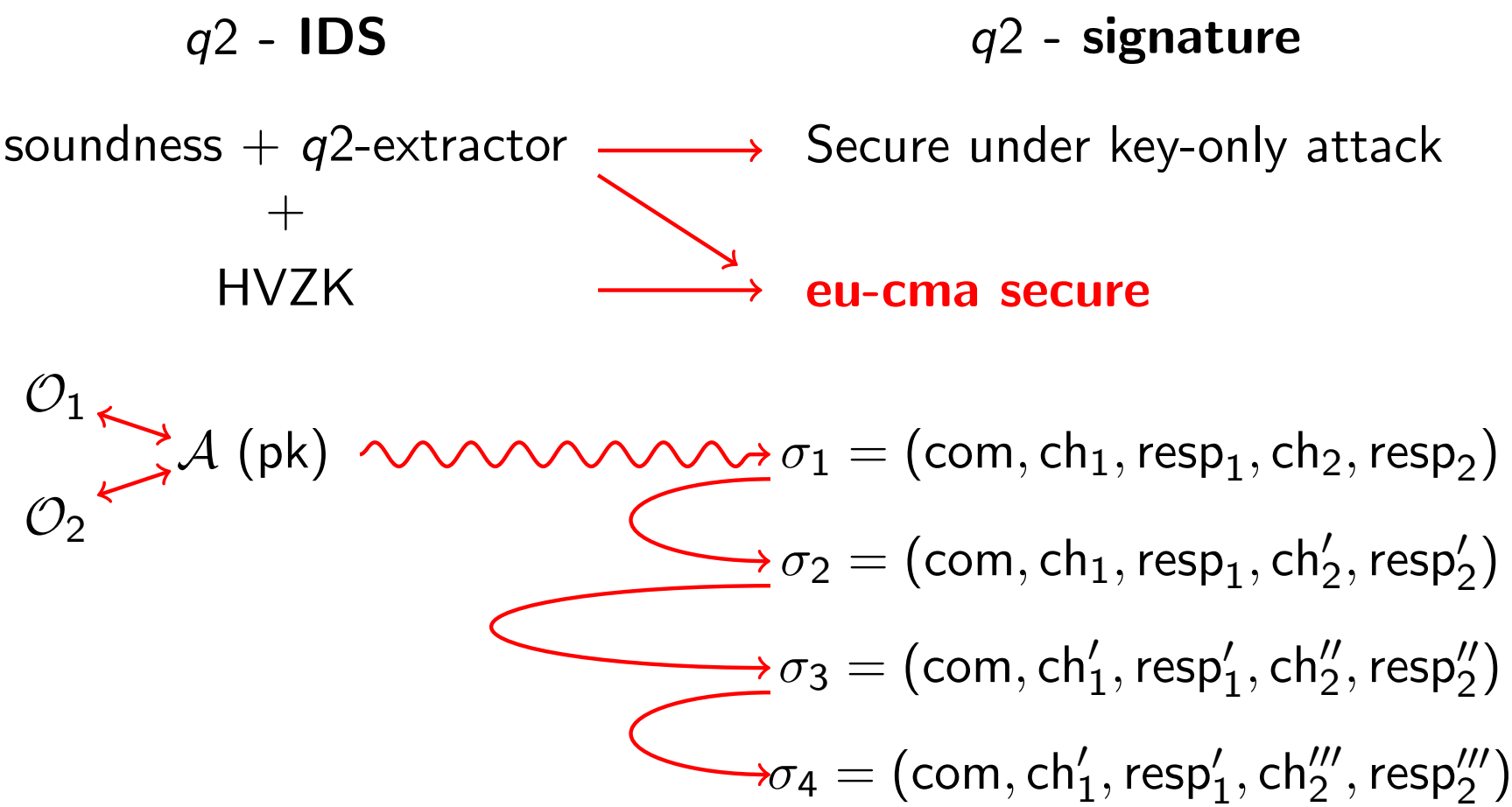
Security of $q2$ - signatures



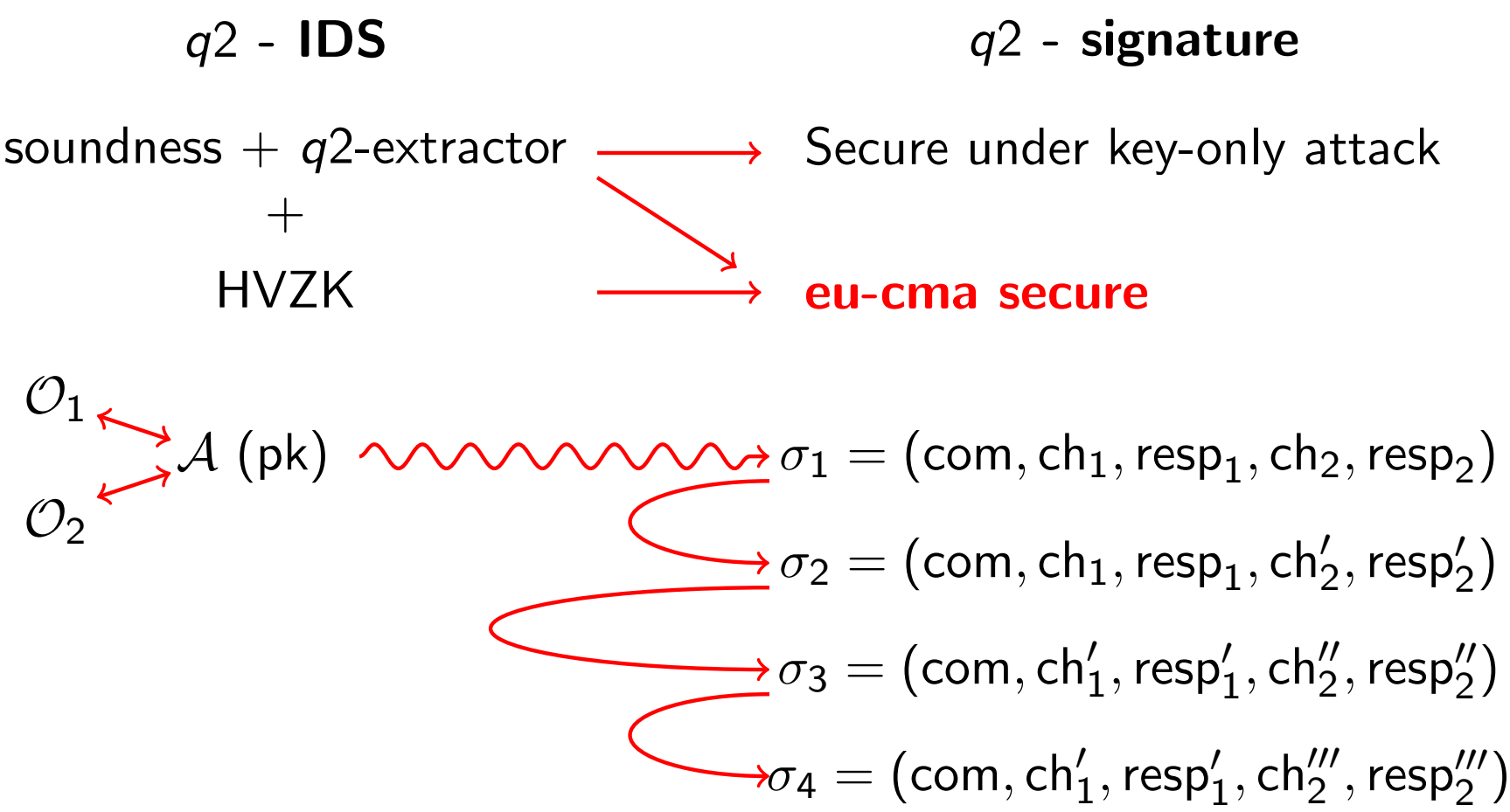
Security of $q2$ - signatures



Security of $q2$ - signatures

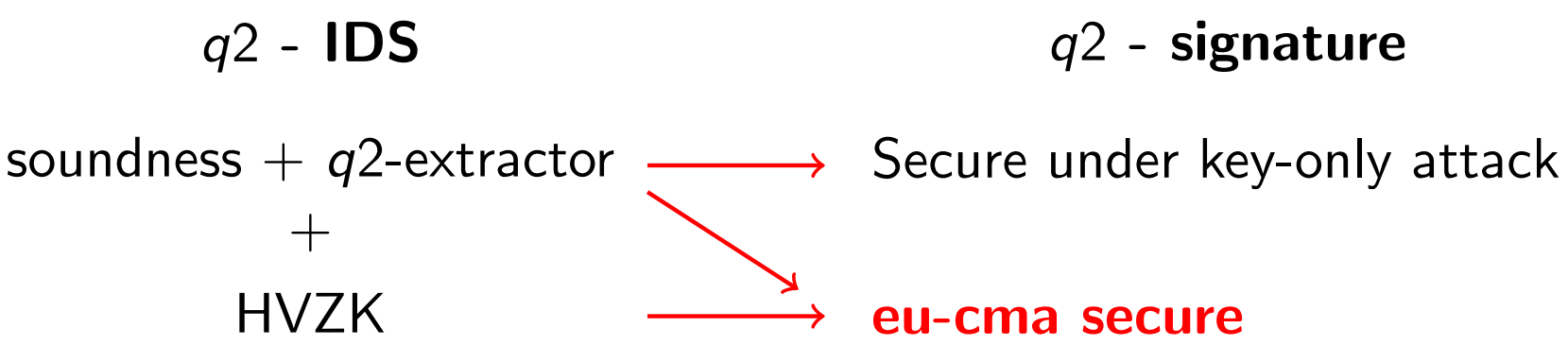


Security of $q2$ - signatures

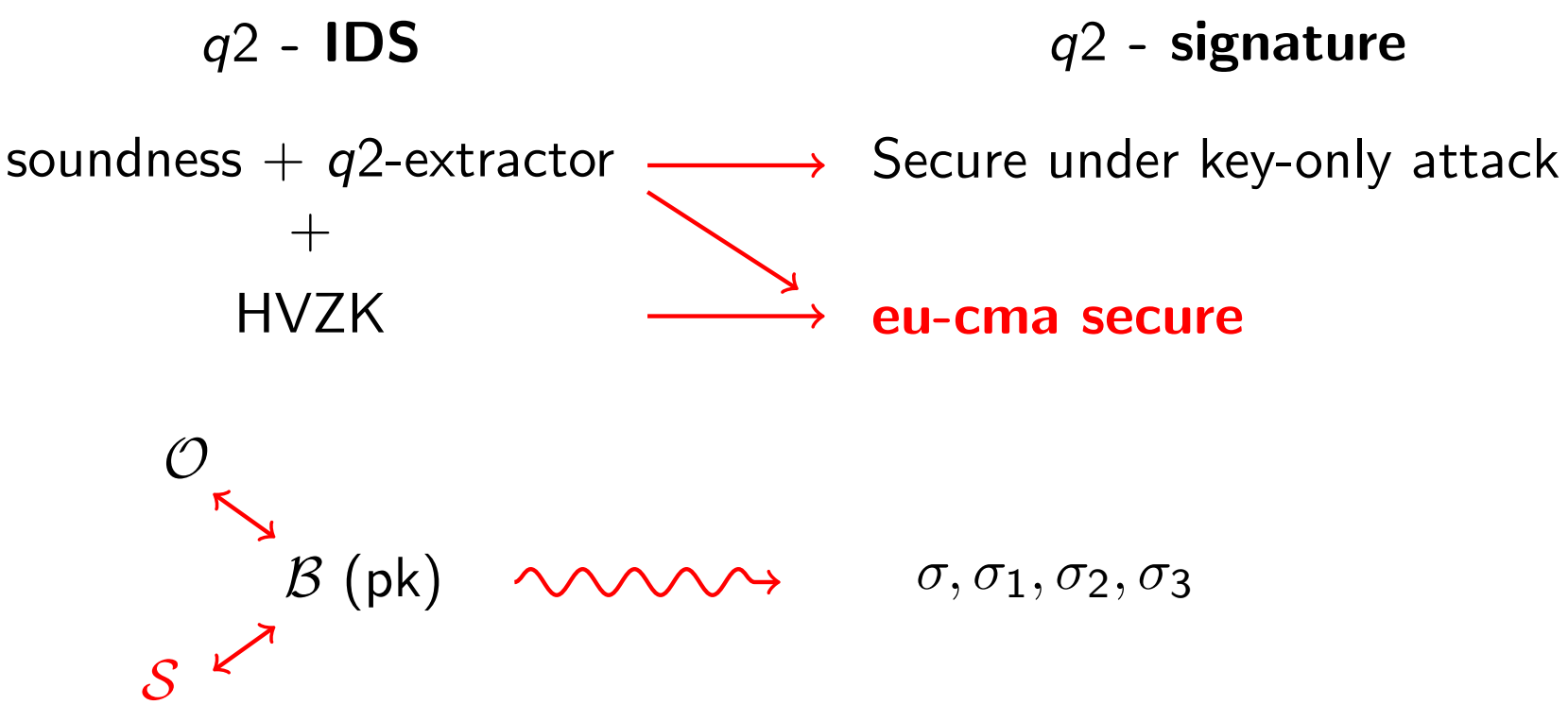


Generalized Forking lemma - ensures existence of the 4 transcripts

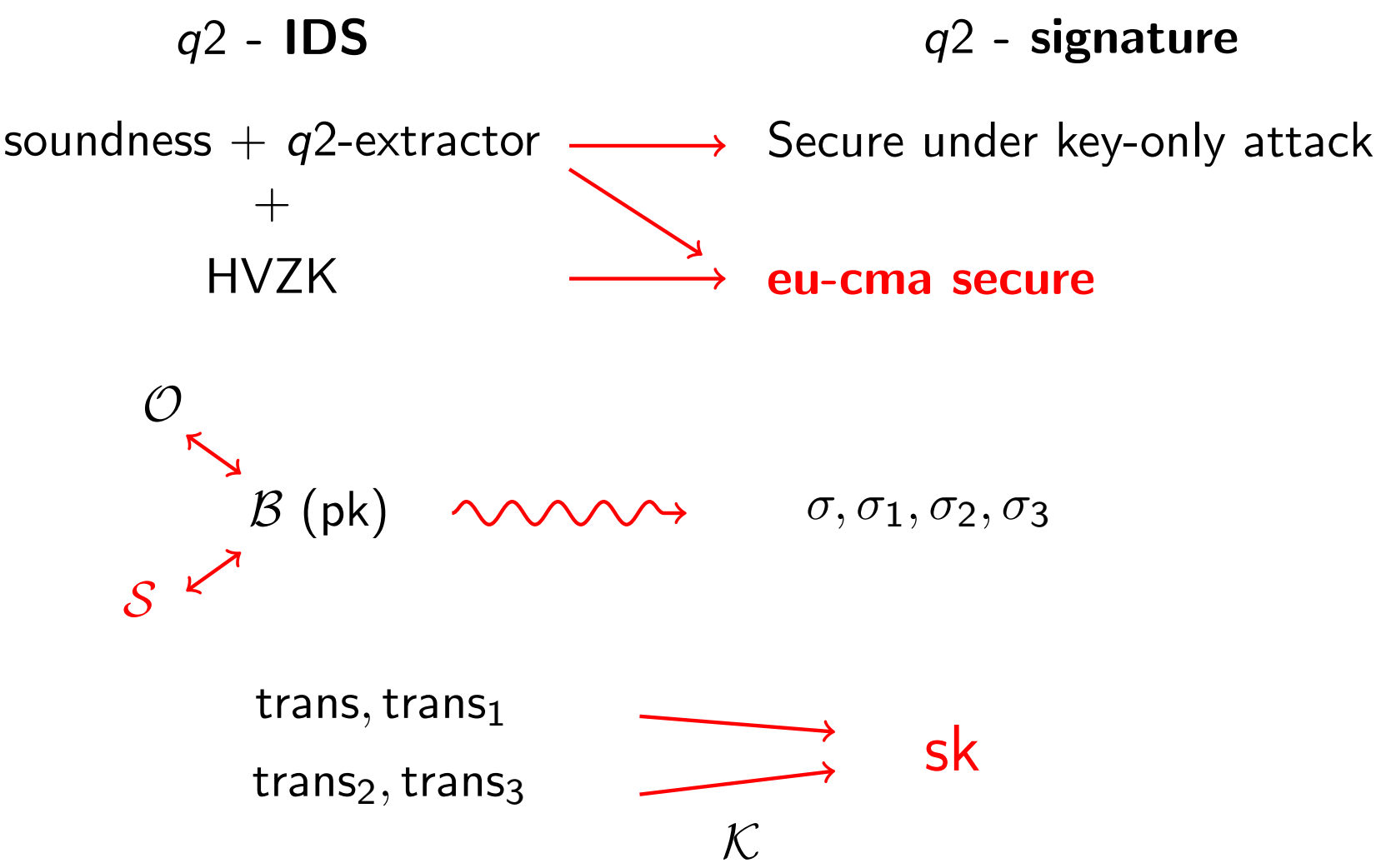
Security of $q2$ - signatures



Security of $q2$ - signatures



Security of $q2$ - signatures



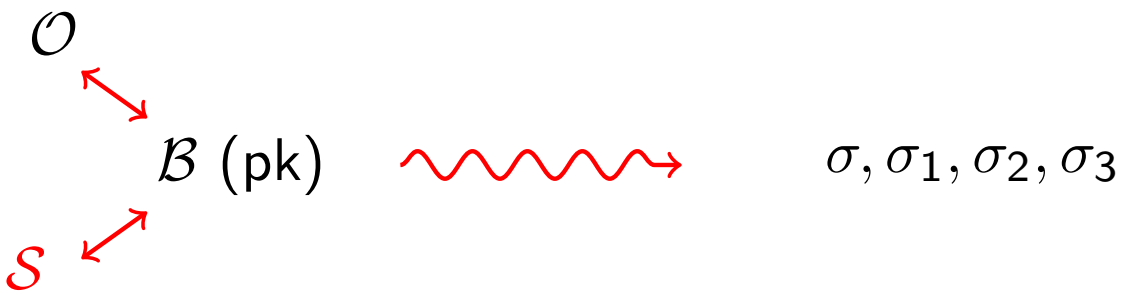
Security of $q2$ - signatures

$q2$ - **IDS** $\qquad$ $q2$ - **signature**

soundness + $q2$-extractor $\longrightarrow$ Secure under key-only attack

+

HVZK $\longrightarrow$ **eu-cma secure**



$\text{trans}, \text{trans}_1$

$\text{trans}_2, \text{trans}_3$

Next step ...

- tighter reduction in ROM
- reduction in QROM

Next step ...(Work in progress)

- tighter reduction in ROM
- reduction in QROM

What is the problem with FS proof in the QROM?

- We need **to see** the signature σ before rewinding
- We need **to see** the oracle inputs
- Seeing (measuring) destroys the quantum state
- The proof fails terribly

Next step ...(Work in progress)

- tighter reduction in ROM
- reduction in QROM

What is the problem with FS proof in the QROM?

- We need **to see** the signature σ before rewinding
- We need **to see** the oracle inputs
- Seeing (measuring) destroys the quantum state
- The proof fails terribly

A solution: Unruh transform [Unruh '14] adapted for $q2$ IDS

- Online extractability
- We can extract the witness without rewinding
- Enough transcripts available directly in ROM

Next step ...(Work in progress)

$\mathcal{P}$		$\mathcal{V}$
$\mathsf{com} \leftarrow \mathcal{P}_0(\mathsf{sk})$		
For $i \in \{1, \ldots, m\}$ **do**		
$\mathsf{ch}_1^{(i)} \leftarrow_R \mathsf{ChS}_1 \setminus \{\mathsf{ch}_1^{(1)}, \ldots, \mathsf{ch}_1^{(i-1)}\}$		
$\mathsf{resp}_1^{(i)} \leftarrow \mathcal{P}_1(\mathsf{sk}, \mathsf{com}, \mathsf{ch}_1^{(i)})$		
$h_1^{(i)} \leftarrow G(\mathsf{resp}_1^{(i)})$		
$h_2^{(1)} \leftarrow G(\mathsf{resp}_2^{(1)}), h_2^{(2)} \leftarrow G(\mathsf{resp}_2^{(2)})$		
$\mathbf{com} \leftarrow (\mathsf{com}, h_1^{(1)}, \ldots, h_1^{(m)}, h_2^{(1)}, h_2^{(2)})$	$\xrightarrow{\mathbf{com}}$	
	$\xleftarrow{(I, J)}$	$I \leftarrow_R \{1, \ldots, m\}, J \leftarrow_R \{0, 1\}$
	$\xrightarrow{\mathsf{resp}_1^{(I)}, \mathsf{resp}_2^{(J)}}$	
		$b \leftarrow \mathsf{Vf}(\mathsf{pk}, \mathsf{com}, I, \mathsf{resp}_1^{(I)}, J, \mathsf{resp}_2^{(J)})$

Next step ...(Work in progress)

Unruh transform adapted for $q2$ IDS

- tighter reduction in ROM
- reduction in QROM
- ... signature size $\approx$ 1.5 of MQDSS-31-64

Thank you for listening!