Multivariate signatures - a post quantum alternative

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]

Cyber Security Seminar, 29.10.2019, TU Delft

The post-quantum world is coming...

- We will have quantum computers soon...

The post-quantum world is coming...

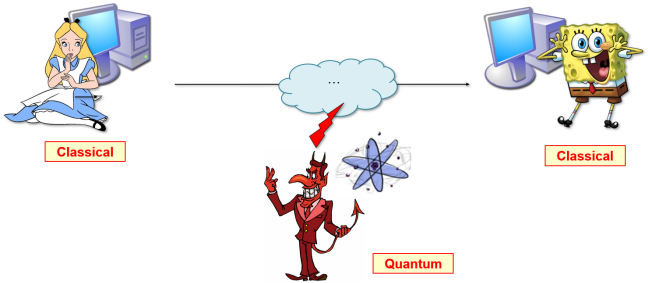
- We will have quantum computers soon...
- Are we ready?

The post-quantum world is coming...

- We will have quantum computers soon...
- Are we ready?
  - Shor's algorithm breaks all main-stream public key crypto today
  - RSA, DH, EC Cryptography

The post-quantum world is coming...

- We will have quantum computers soon...
- Are we ready?
  - Shor's algorithm breaks all main-stream public key crypto today
  - RSA, DH, EC Cryptography



NIST standardization process for Post-Quantum cryptography

- Standardize KEMs and digital signatures
- not a competition

NIST standardization process for Post-Quantum cryptography

- Standardize KEMs and digital signatures
- not a competition
- Timeline:
  - Fall 2016 - Formal call for proposals
  - Nov 2017 - Deadline for submissions
  - Jan 2019 - Round 2 candidates announced
  - 3-5 years analysis phase
  - +2 years draft standard preparation

NIST standardization process for Post-Quantum cryptography

- Standardize KEMs and digital signatures
- not a competition
- Timeline:
  - Fall 2016 - Formal call for proposals
  - Nov 2017 - Deadline for submissions
  - Jan 2019 - Round 2 candidates announced
  - 3-5 years analysis phase
  - +2 years draft standard preparation
- Round 1: 69 "complete and proper", 49 KEMs and 20 signatures
- Round 2: 26 candidates, 17 KEMs and 9 signatures

$\mathcal{MQ}$-based signatures

- Important candidate for post-quantum signatures
- Several submissions to NIST (Round 2 candidates in bold)
  - DualModeMS, **GeMSS**, Gui, HiMQ-3, **LUOV**, **MQDSS**, **Rainbow**
- Traditionally small signatures, larger keys
  - (except DualModeMS, LUOV, MQDSS)

$\mathcal{MQ}$-based signatures

- Important candidate for post-quantum signatures
- Several submissions to NIST (Round 2 candidates in bold)
  - DualModeMS, **GeMSS**, Gui, HiMQ-3, **LUOV**, **MQDSS**, **Rainbow**
- Traditionally small signatures, larger keys
  - (except DualModeMS, LUOV, MQDSS)

- Typically based on $\mathcal{MQ}$ but also related problems (e.g. IP)

$\mathcal{MQ}$-based signatures

- Important candidate for post-quantum signatures
- Several submissions to NIST (Round 2 candidates in bold)
  - DualModeMS, **GeMSS**, Gui, HiMQ-3, **LUOV**, **MQDSS**, **Rainbow**
- Traditionally small signatures, larger keys
  - (except DualModeMS, LUOV, MQDSS)

- Typically based on $\mathcal{MQ}$ but also related problems (e.g. IP)

- **MQDSS**: first signature with (lossy) ROM reduction to $\mathcal{MQ}$

$\mathcal{MQ}$-based signatures

- Important candidate for post-quantum signatures
- Several submissions to NIST (Round 2 candidates in bold)
  - DualModeMS, **GeMSS**, Gui, HiMQ-3, **LUOV**, **MQDSS**, **Rainbow**
- Traditionally small signatures, larger keys
  - (except DualModeMS, LUOV, MQDSS)

- Typically based on $\mathcal{MQ}$ but also related problems (e.g. IP)

- **MQDSS**: first signature with (lossy) ROM reduction to $\mathcal{MQ}$
- **SOFIA**: first signature with (lossy) QROM reduction to $\mathcal{MQ}$

$\mathcal{MQ}$-based signatures

- Important candidate for post-quantum signatures
- Several submissions to NIST (Round 2 candidates in bold)
  - DualModeMS, **GeMSS**, Gui, HiMQ-3, **LUOV**, **MQDSS**, **Rainbow**
- Traditionally small signatures, larger keys
  - (except DualModeMS, LUOV, MQDSS)

- Typically based on $\mathcal{MQ}$ but also related problems (e.g. IP)

- **MQDSS**: first signature with (lossy) ROM reduction to $\mathcal{MQ}$
- **SOFIA**: first signature with (lossy) QROM reduction to $\mathcal{MQ}$

  - Transform an $\mathcal{MQ}$-based IDS

$\mathcal{MQ}$ problem

The function family $\mathcal{MQ}(n, m, \mathbb{F}_q)$:

$$\mathbf{F}(\mathbf{x}) = (f_1(\mathbf{x}), \ldots, f_m(\mathbf{x})), \text{ where } f_s(\mathbf{x}) = \sum_{i,j} a_{i,j}^{(s)} x_i x_j + \sum_i b_i^{(s)} x_i$$
$$\text{for } a_{i,j}^{(s)},\ b_i^{(s)} \in \mathbb{F}_q, s \in \{1, \ldots, m\}$$

$\mathcal{MQ}$ problem

The function family $\mathcal{MQ}(n, m, \mathbb{F}_q)$:

$$\mathbf{F}(\mathbf{x}) = (f_1(\mathbf{x}), \ldots, f_m(\mathbf{x})), \text{ where } f_s(\mathbf{x}) = \sum_{i,j} a_{i,j}^{(s)} x_i x_j + \sum_i b_i^{(s)} x_i$$
$$\text{for } a_{i,j}^{(s)},\ b_i^{(s)} \in \mathbb{F}_q, s \in \{1, \ldots, m\}$$

Problem: For given $\mathbf{y} \in \mathbb{F}_q^m$, find $\mathbf{x} \in \mathbb{F}_q^n$ such that $\mathbf{F}(\mathbf{x}) = \mathbf{y}$.

$\mathcal{MQ}$ problem

The function family $\mathcal{MQ}(n, m, \mathbb{F}_q)$:

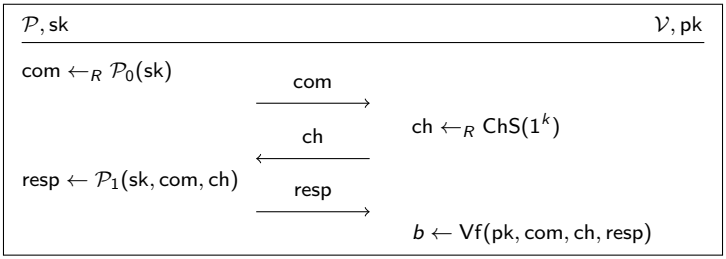
$$\mathbf{F}(\mathbf{x}) = (f_1(\mathbf{x}), \ldots, f_m(\mathbf{x})), \text{ where } f_s(\mathbf{x}) = \sum_{i,j} a_{i,j}^{(s)} x_i x_j + \sum_i b_i^{(s)} x_i$$
$$\text{for } a_{i,j}^{(s)},\ b_i^{(s)} \in \mathbb{F}_q, s \in \{1, \ldots, m\}$$

Problem: For given $\mathbf{y} \in \mathbb{F}_q^m$, find $\mathbf{x} \in \mathbb{F}_q^n$ such that $\mathbf{F}(\mathbf{x}) = \mathbf{y}$.

i.e., solve the system of equations:

$$\begin{aligned} y_1 =& a_{1,1}^{(1)} x_1 x_1 + a_{1,2}^{(1)} x_1 x_2 + \ldots + a_{n,n}^{(1)} x_n x_n + b_1^{(1)} x_1 + \ldots + b_n^{(1)} x_n \\ &\vdots \\ y_m =& a_{1,1}^{(m)} x_1 x_1 + a_{1,2}^{(m)} x_1 x_2 + \ldots + a_{n,n}^{(m)} x_n x_n + b_1^{(m)} x_1 + \ldots + b_n^{(m)} x_n \end{aligned}$$

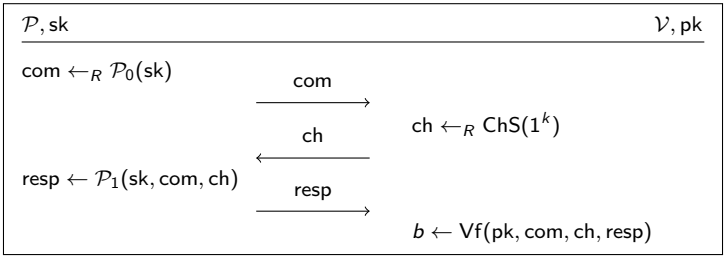
Canonical Identification Schemes



Informally:

1. Prover commits to some (randomized) value derived from sk
2. Verifier picks a challenge 'ch'
3. Prover computes response 'resp'
4. Verifier checks if response matches challenge

Properties of Canonical 3-pass IDS

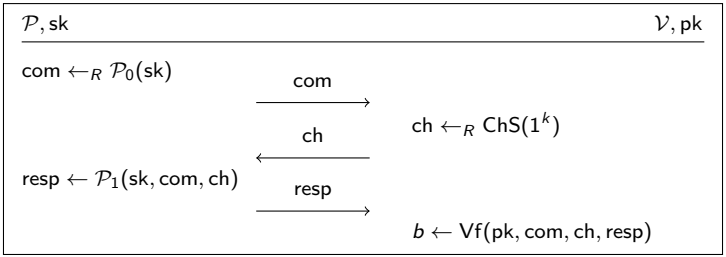


Soundness (with soundness error κ)

Probability that a PPT adversary $\mathcal{A}$ gets verified is $\kappa + \mathrm{negl}(k)$

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

Properties of Canonical 3-pass IDS



Special Soundness

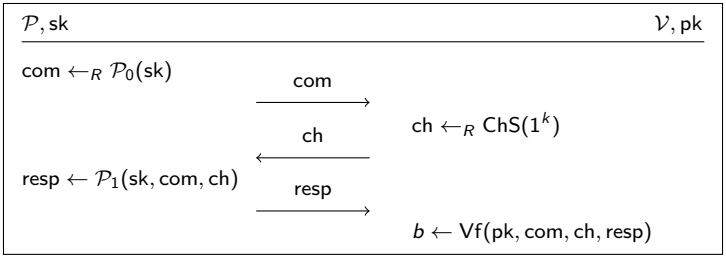
There exists PPT algorithm $\mathcal{K}$ - knowledge extractor s.t. given two accepting transcripts:

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

extracts the secret sk with non-negligible probability

- random challenges can be answered only if Prover knows a witness

Properties of Canonical 3-pass IDS



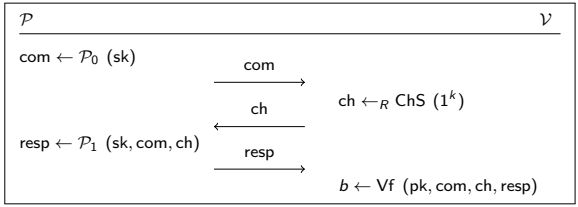
(statistical) Honest-Verifier Zero-Knowledge

There exists a PPT algorithm $\mathcal{S}$, called the simulator, such that the statistical distance between the real transcript and the simulated transcript is negligible in k.

- guaranties no leakage of secret

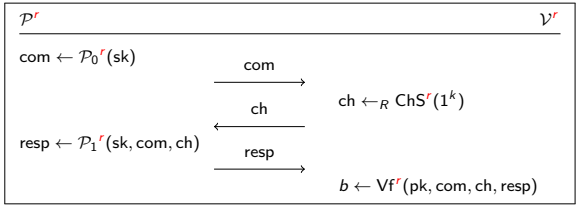
The Fiat-Shamir transform

IDS



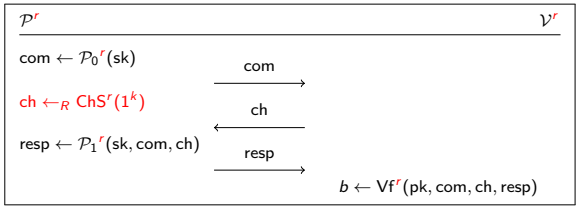
The Fiat-Shamir transform

IDS

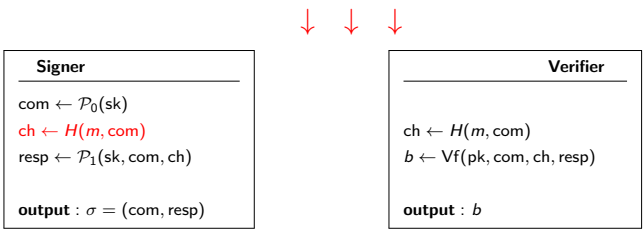


The Fiat-Shamir transform

IDS



FS signature



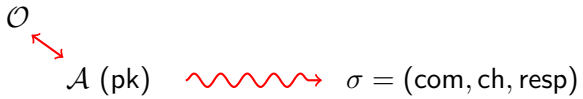
Security of FS signatures [Pointcheval & Stern '96]

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

Security of FS signatures [Pointcheval & Stern '96]

IDS → **FS signature**

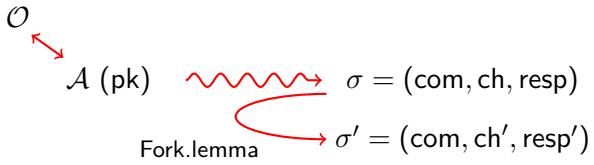
Special soundness → Secure under key-only attack



Security of FS signatures [Pointcheval & Stern '96]

IDS → **FS signature**

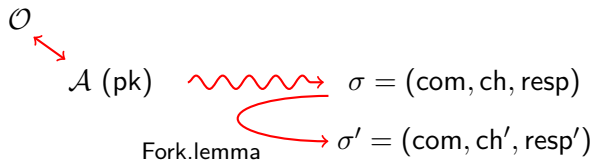
Special soundness → Secure under key-only attack



Security of FS signatures [Pointcheval & Stern '96]

IDS → **FS signature**

Special soundness → Secure under key-only attack



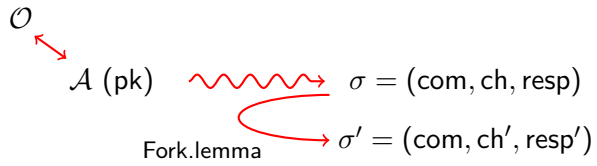
$\mathsf{trans} = (\mathsf{com}, \mathsf{ch}, \mathsf{resp})$

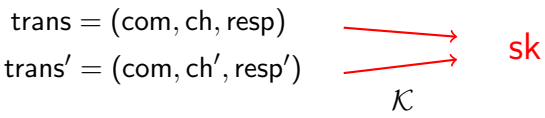
$\mathsf{trans}' = (\mathsf{com}, \mathsf{ch}', \mathsf{resp}')$

Security of FS signatures [Pointcheval & Stern '96]

IDS → **FS signature**

Special soundness → Secure under key-only attack





Security of FS signatures [Pointcheval & Stern '96]

IDS

Special soundness

+

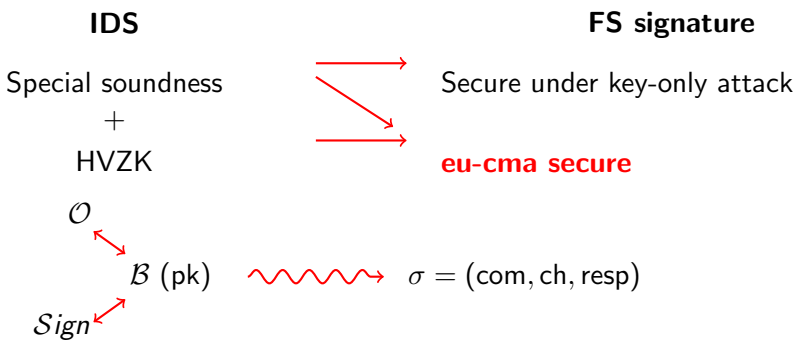
HVZK

FS signature

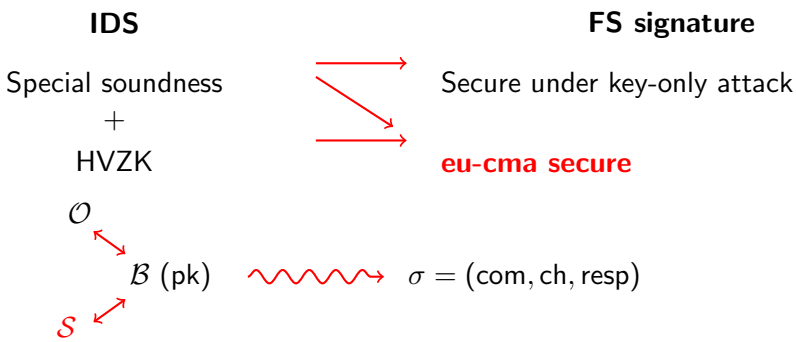
Secure under key-only attack

eu-cma secure

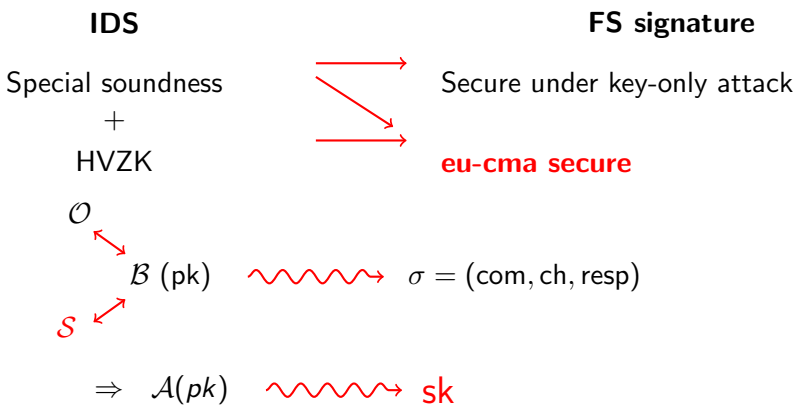
Security of FS signatures [Pointcheval & Stern '96]



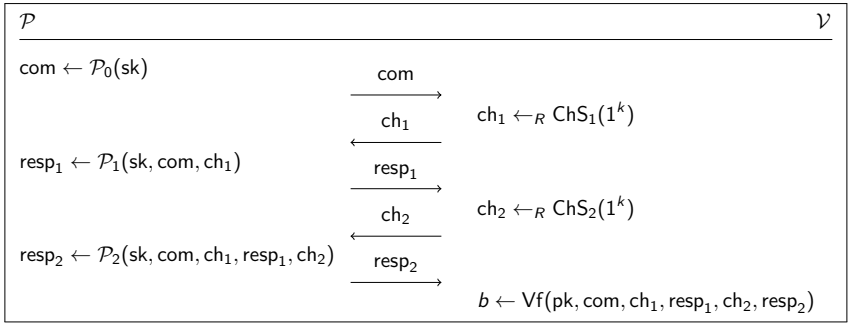
Security of FS signatures [Pointcheval & Stern '96]



Security of FS signatures [Pointcheval & Stern '96]

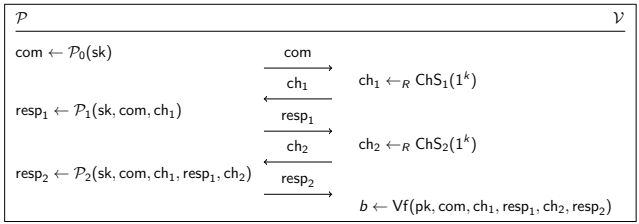


Canonical 5-pass IDS



The Fiat-Shamir transform on 5-pass IDS

IDS



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	**Verifier**
$\mathsf{com} \leftarrow \mathcal{P}_0(\mathsf{sk})$	
$\mathsf{ch}_1 \leftarrow H_1(m, \mathsf{com})$	$\mathsf{ch}_1 \leftarrow H_1(m, \mathsf{com})$
$\mathsf{resp}_1 \leftarrow \mathcal{P}_1(\mathsf{sk}, \mathsf{com}, \mathsf{ch}_1)$	
$\mathsf{ch}_2 \leftarrow H_2(m, \mathsf{com}, \mathsf{ch}_1, \mathsf{resp}_1)$	$\mathsf{ch}_2 \leftarrow H_2(m, \mathsf{com}, \mathsf{ch}_1, \mathsf{resp}_1)$
$\mathsf{resp}_2 \leftarrow \mathcal{P}_2(\mathsf{sk}, \mathsf{com}, \mathsf{ch}_1, \mathsf{resp}_1, \mathsf{ch}_2)$	$b \leftarrow \mathsf{Vf}(\mathsf{pk}, \mathsf{com}, \mathsf{ch}_1, \mathsf{resp}_1, \mathsf{ch}_2, \mathsf{resp}_2)$
output : $\sigma = (\mathsf{com}, \mathsf{resp}_1, \mathsf{resp}_2)$	**output** : b

Sakumoto-Shirai-Hiwatari 5-pass IDS

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

- Smaller soundness error ($\frac{q+1}{2q}$ over $\mathbb{F}_q$) $\Rightarrow$ **smaller signatures**
- Key technique: **cut-and-choose for** $\mathcal{MQ}$

Sakumoto-Shirai-Hiwatari IDS

- Smaller soundness error ($\frac{q+1}{2q}$ over $\mathbb{F}_q$) $\Rightarrow$ **smaller signatures**
- Key technique: **cut-and-choose for** $\mathcal{MQ}$

- Bilinear map $\mathbf{G}(\mathbf{x},\mathbf{y}) = \mathbf{F}(\mathbf{x}+\mathbf{y}) - \mathbf{F}(\mathbf{x}) - \mathbf{F}(\mathbf{y})$
  - Split $\mathbf{s}$ and $\mathbf{F}(\mathbf{s})$ into $\mathbf{r}_0, \mathbf{r}_1$ and $\mathbf{F}(\mathbf{r}_0), \mathbf{F}(\mathbf{r}_1)$
    - Since then $\mathbf{s} = \mathbf{r}_0 + \mathbf{r}_1 \Rightarrow \mathbf{F}(\mathbf{s}) = \mathbf{G}(\mathbf{r}_0, \mathbf{r}_1) + \mathbf{F}(\mathbf{r}_0) + \mathbf{F}(\mathbf{r}_1)$
  - Split $\mathbf{r}_0$ and $\mathbf{F}(\mathbf{r}_0)$ further into $\mathbf{t}_0, \mathbf{t}_1$ resp. $\mathbf{e}_0, \mathbf{e}_1$

Sakumoto-Shirai-Hiwatari IDS

- Smaller soundness error ($\frac{q+1}{2q}$ over $\mathbb{F}_q$) $\Rightarrow$ **smaller signatures**
- Key technique: **cut-and-choose for** $\mathcal{MQ}$

- Bilinear map $\mathbf{G}(\mathbf{x},\mathbf{y}) = \mathbf{F}(\mathbf{x}+\mathbf{y}) - \mathbf{F}(\mathbf{x}) - \mathbf{F}(\mathbf{y})$
  - Split $\mathbf{s}$ and $\mathbf{F}(\mathbf{s})$ into $\mathbf{r}_0, \mathbf{r}_1$ and $\mathbf{F}(\mathbf{r}_0), \mathbf{F}(\mathbf{r}_1)$
    - Since then $\mathbf{s} = \mathbf{r}_0 + \mathbf{r}_1 \Rightarrow \mathbf{F}(\mathbf{s}) = \mathbf{G}(\mathbf{r}_0, \mathbf{r}_1) + \mathbf{F}(\mathbf{r}_0) + \mathbf{F}(\mathbf{r}_1)$
  - Split $\mathbf{r}_0$ and $\mathbf{F}(\mathbf{r}_0)$ further into $\mathbf{t}_0, \mathbf{t}_1$ resp. $\mathbf{e}_0, \mathbf{e}_1$

Sakumoto-Shirai-Hiwatari IDS

- Smaller soundness error ($\frac{q+1}{2q}$ over $\mathbb{F}_q$) $\Rightarrow$ **smaller signatures**
- Key technique: **cut-and-choose for** $\mathcal{MQ}$

- Bilinear map $\mathbf{G}(\mathbf{x}, \mathbf{y}) = \mathbf{F}(\mathbf{x} + \mathbf{y}) - \mathbf{F}(\mathbf{x}) - \mathbf{F}(\mathbf{y})$
  - Split $\mathbf{s}$ and $\mathbf{F}(\mathbf{s})$ into $\mathbf{r}_0, \mathbf{r}_1$ and $\mathbf{F}(\mathbf{r}_0), \mathbf{F}(\mathbf{r}_1)$
    - Since then $\mathbf{s} = \mathbf{r}_0 + \mathbf{r}_1 \Rightarrow \mathbf{F}(\mathbf{s}) = \mathbf{G}(\mathbf{r}_0, \mathbf{r}_1) + \mathbf{F}(\mathbf{r}_0) + \mathbf{F}(\mathbf{r}_1)$
  - Split $\mathbf{r}_0$ and $\mathbf{F}(\mathbf{r}_0)$ further into $\mathbf{t}_0, \mathbf{t}_1$ resp. $\mathbf{e}_0, \mathbf{e}_1$
  - $\mathbf{r_0} = \mathbf{t_0} + \mathbf{t_1}$
  - $\mathbf{F(r_0)} = \mathbf{e_0} + \mathbf{e_1}$
- Using bilinearity, $\mathbf{v} = (\mathbf{G(t_0, r_1)} + \mathbf{e_0}) + (\mathbf{F(r_1)} + \mathbf{G(t_1, r_1)} + \mathbf{e_1})$
- Result: reveal either $\mathbf{r}_0$ or $\mathbf{r}_1$, and $(\mathbf{t}_1, \mathbf{e}_1)$
- **Zero knowledge property satisfied**

Sakumoto-Shirai-Hiwatari 5-pass IDS does not fulfill special 2-soundness!

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

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

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

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

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

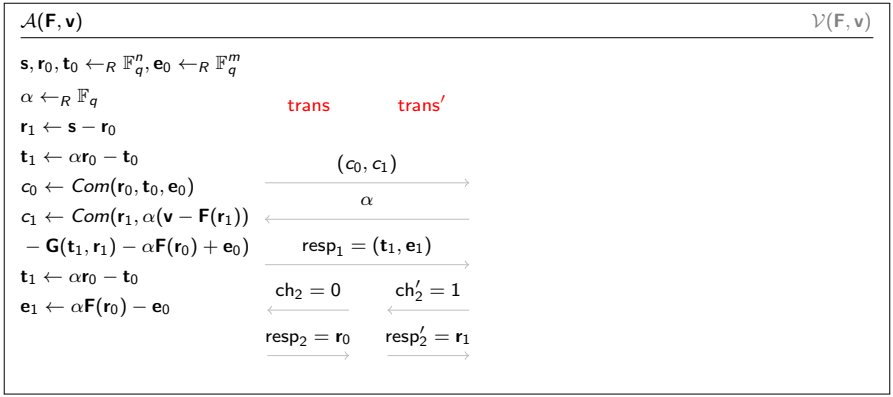
$c_0 \leftarrow \mathit{Com}(\mathbf{r}_0, \mathbf{t}_0, \mathbf{e}_0)$

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

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

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

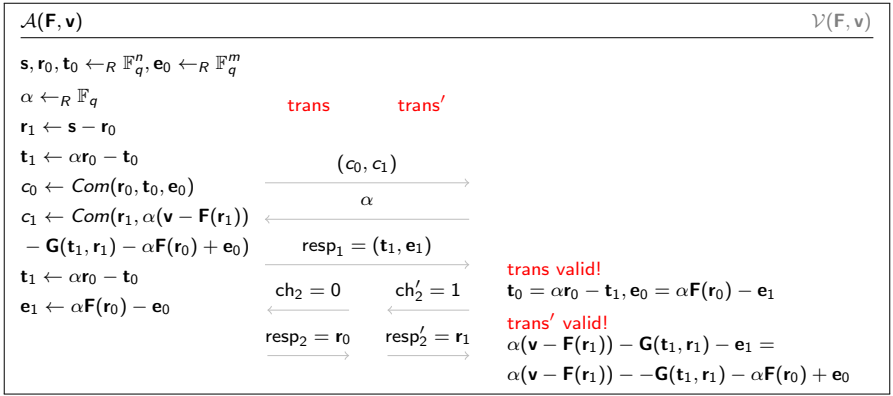
Sakumoto-Shirai-Hiwatari 5-pass IDS does not fulfill special 2-soundness!



Sakumoto-Shirai-Hiwatari 5-pass IDS does not fulfill special 2-soundness!

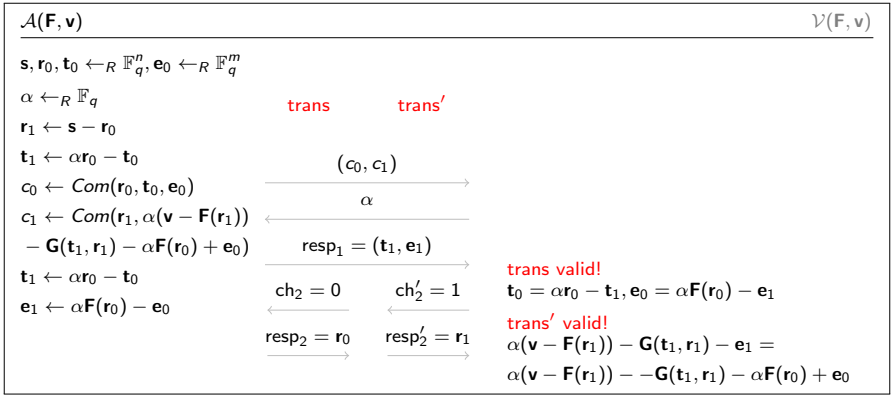
$\mathcal{A}(\mathbf{F}, \mathbf{v})$			$\mathcal{V}(\mathbf{F}, \mathbf{v})$
$\mathbf{s}, \mathbf{r}_0, \mathbf{t}_0 \leftarrow_R \mathbb{F}_q^n, \mathbf{e}_0 \leftarrow_R \mathbb{F}_q^m$			
$\alpha \leftarrow_R \mathbb{F}_q$	trans	trans′	
$\mathbf{r}_1 \leftarrow \mathbf{s} - \mathbf{r}_0$			
$\mathbf{t}_1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

Sakumoto-Shirai-Hiwatari 5-pass IDS does not fulfill special 2-soundness!



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

Sakumoto-Shirai-Hiwatari 5-pass IDS does not fulfill special 2-soundness!

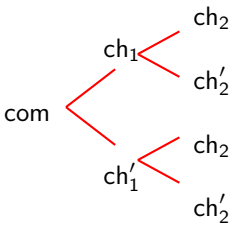


$\mathcal{K}(\mathsf{trans}, \mathsf{trans}') \longrightarrow \mathsf{sk} = \mathbf{s}'$
s.t. $\mathbf{F}(\mathbf{s}') = \mathbf{v} \Rightarrow \mathcal{MQ}$ **problem solved!**

Sakumoto et al. 5-pass IDS

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

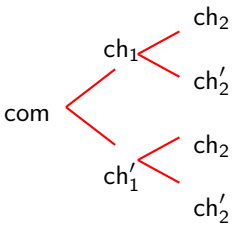
$(\text{com}, \text{ch}_1, \text{resp}_1, \text{ch}_2, \text{resp}_2)$
$(\text{com}, \text{ch}_1, \text{resp}_1, \text{ch}_2', \text{resp}_2')$
$(\text{com}, \text{ch}_1', \text{resp}_1', \text{ch}_2, \text{resp}_2'')$
$(\text{com}, \text{ch}_1', \text{resp}_1', \text{ch}_2', \text{resp}_2''')$



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

$q2$ signatures - Security

$q2$ - **IDS**

soundness + $q2$-extractor

+

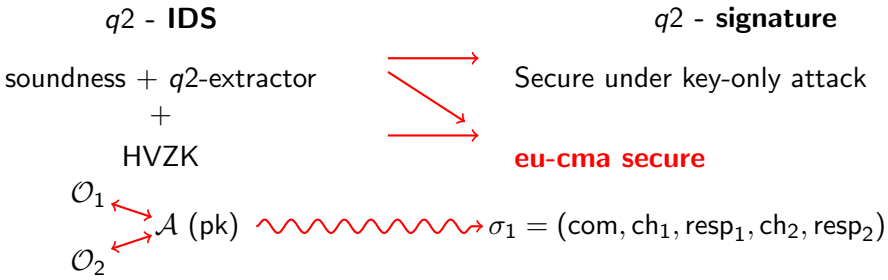
HVZK

$q2$ - **signature**

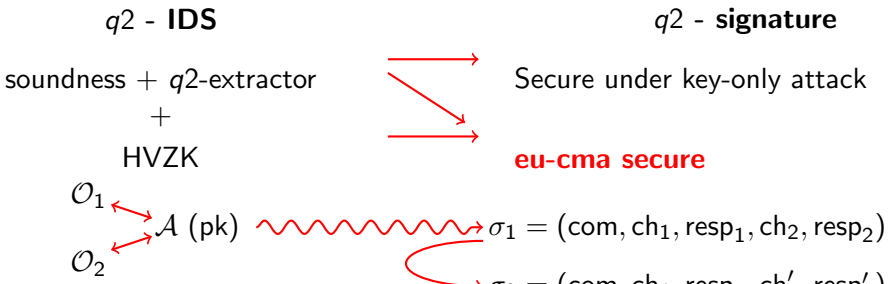
Secure under key-only attack

eu-cma secure

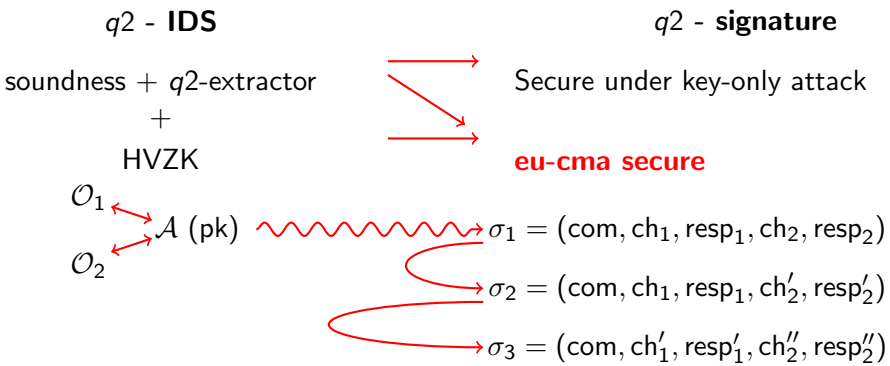
$q2$ signatures - Security



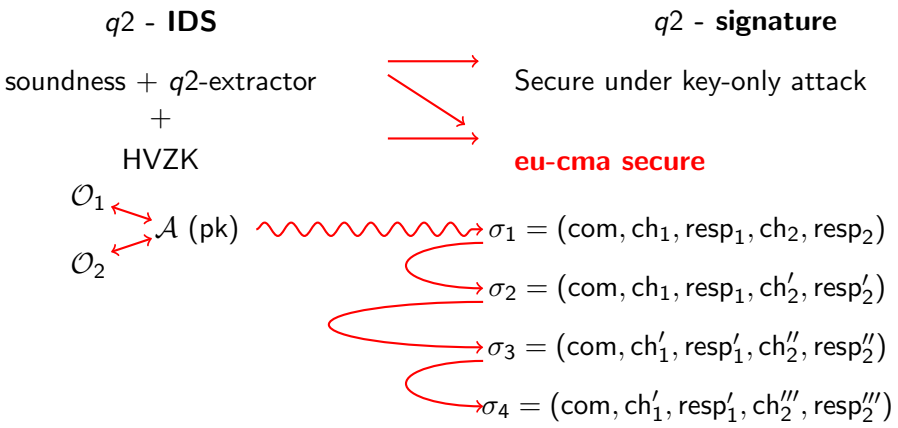
$q2$ signatures - Security



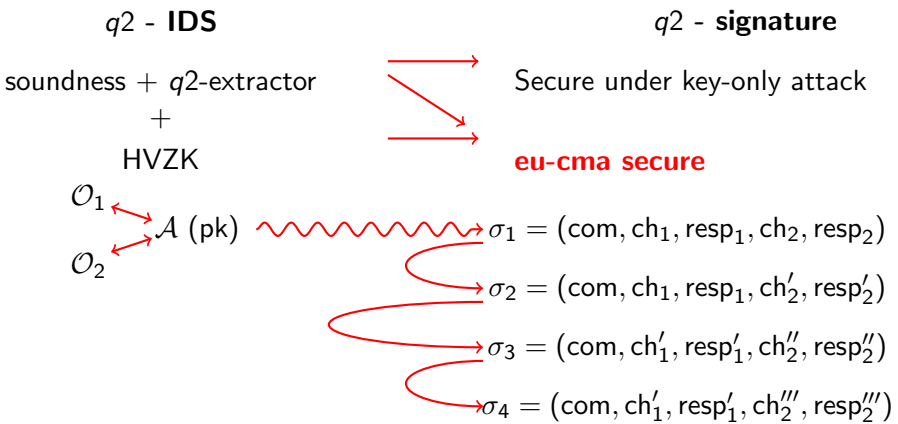
$q2$ signatures - Security



$q2$ signatures - Security



$q2$ signatures - Security



Generalized Forking lemma - ensures existence of the 4 transcripts

Next step ...

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 ...$\mathcal{MQ}$ signatures in the 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 directly available

Unruh transform for $q2$ IDS (informally)

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

MQDSS vs SOFIA

	Sec.	q	n $(= m)$	r	pk (bytes)	sk (bytes)	Signature (bytes)
MQDSS-31-64 (AC '16)	128 (ROM)	31	48	269	72	64	40952
SOFIA-4-128 (PKC '18)	128 (QROM)	4	128	438	64	32	126176

- SOFIA still comparable to Picnic (with QROM proof),
- but much slower than SPHINCS + and lattice based schemes

NIST Parameter Sets MQDSS

	Sec. cat.	q	n $(= m)$	r	pk (bytes)	sk (bytes)	Signature (bytes)
MQDSS-31-48 (Round 2)	1-2	31	48	135	46	16	20854
MQDSS-31-48 (Round 1)				269	62	32	32882
MQDSS-31-64 (Round 2)	3-4	31	64	202	64	24	43728
MQDSS-31-64 (Round 1)				403	88	48	67800

Table: Round 1 parameters in black, Round 2 parameters in red.

- q, $n = m$ chosen using best attacks on $\mathcal{MQ}$
  - q additionally chosen for fast arithmetic

NIST Parameter Sets MQDSS

	Sec. cat.	q	n $(= m)$	r	pk (bytes)	sk (bytes)	Signature (bytes)
MQDSS-31-48 (Round 2)	1-2	31	48	135	46	16	20854
MQDSS-31-48 (Round 1)				269	62	32	32882
MQDSS-31-64 (Round 2)	3-4	31	64	202	64	24	43728
MQDSS-31-64 (Round 1)				403	88	48	67800

Table: Round 1 parameters in black, Round 2 parameters in red.

- q, $n = m$ chosen using best attacks on $\mathcal{MQ}$
  - q additionally chosen for fast arithmetic
- r chosen such that $2^{-(r \log \frac{2q}{q+1})} < 2^{-k}$
  - **mistake in calculation in Round 1, chose k too large**

Recent attack

- August 2019, Daniel Kales and Greg Zaverucha - forgery in approx. 2^{95} hash calls for MQDSS-31-48
- Can be mitigated by $\approx 1.4\times$(number of rounds)
- **Proof still valid!**
  - Attack is result of not taking into account non-tightness of proof for choosing parameters

Recent attack

- August 2019, Daniel Kales and Greg Zaverucha - forgery in approx. 2^{95} hash calls for MQDSS-31-48
- Can be mitigated by $\approx 1.4\times$(number of rounds)
- **Proof still valid!**
  - Attack is result of not taking into account non-tightness of proof for choosing parameters
- **New parameters after attack (estimate):**

	Sec. cat.	q	n	r	pk	sk	Signature
MQDSS-31-48 (new)	1-2	31	48	184	46B	16B	28400B
Round 1				269	62B	32B	32882B
MQDSS-31-64 (new)	3-4	31	64	277	64B	24B	59928B
Round 1				403	88B	48B	67800B

Table: Round 1 parameters in black, New parameters (attack fixed) in red.

Summary of MQDSS (new)

- Fiat-Shamir transform from $\mathcal{MQ}$-based 5-pass identification scheme
- Security proof in ROM, instead of typical 'break and tweak' in $\mathcal{MQ}$ cryptography
- Very small keys, big signatures

Summary of MQDSS (new)

- Fiat-Shamir transform from $\mathcal{MQ}$-based 5-pass identification scheme
- Security proof in ROM, instead of typical 'break and tweak' in $\mathcal{MQ}$ cryptography
- Very small keys, big signatures
- **Main improvement in Round 2: Smaller signatures**
  - Even after: Recent attack + Added randomness in commitments

	Sec. cat.	q	n	r	pk	sk	Signature
MQDSS-31-48 (new)	1-2	31	48	184	46B	16B	28400B
Round 1				269	62B	32B	32882B
MQDSS-31-64 (new)	3-4	31	64	277	64B	24B	59928B
Round 1				403	88B	48B	67800B

Table: Round 1 parameters in black, New parameters (attack fixed) in red.

Summary of MQDSS (new)

- Fiat-Shamir transform from $\mathcal{MQ}$-based 5-pass identification scheme
- Security proof in ROM, instead of typical 'break and tweak' in $\mathcal{MQ}$ cryptography
- Very small keys, big signatures
- **Main improvement in Round 2: Smaller signatures**
  - Even after: Recent attack + Added randomness in commitments

	Sec. cat.	q	n	r	pk	sk	Signature
MQDSS-31-48 (new)	1-2	31	48	184	46B	16B	28400B
Round 1				269	62B	32B	32882B
MQDSS-31-64 (new)	3-4	31	64	277	64B	24B	59928B
Round 1				403	88B	48B	67800B

Table: Round 1 parameters in black, New parameters (attack fixed) in red.

Thank you for your attention!