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

Ming-Shing Chen[1,2], Andreas Hülsing[3], **Joost Rijneveld**[4], Simona Samardjiska[5], Peter Schwabe[4]

National Taiwan University[1] / Academia Sinica[2], Taipei, Taiwan
Eindhoven University of Technology, The Netherlands[3]
Radboud University, Nijmegen, The Netherlands[4]
"Ss. Cyril and Methodius" University, Skopje, Republic of Macedonia[5]

2016-12-05
ASIACRYPT 2016

Post-quantum signatures

Problem: we want a post-quantum signature scheme

- Security arguments
- 'Acceptable' speed and size

Post-quantum signatures

Problem: we want a post-quantum signature scheme

- Security arguments
- 'Acceptable' speed and size

Solutions:

- Hash-based: SPHINCS [BHH+15], XMSS [BDH11, HRS16]
  - Slow or stateful
- Lattice-based: (Ring-)TESLA [ABB+16, ABB+15], BLISS [DDL+13], GLP [GLP12]
  - Large keys, or additional structure
- $\mathcal{MQ}$: ?
  - Unclear security: many broken (except HFEv-, UOV)

This work

- Transform class of 5-pass IDS to signature schemes
  - Extend Fiat Shamir transform
- Prove an earlier attempt [EDV+12] vacuous
  - Amended in [DGV+16]
- Propose MQDSS
  - Obtained by performing transform
  - Hardness of $\mathcal{MQ}$
- Instantiate and implement as MQDSS-31-64

But also:

- Reduction in the ROM (not in QROM)
- No tight proof

Canonical Identification Schemes

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

Informally:

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

Security of the IDS

- Passively secure IDS

Soundness: the probability that an adversary can convince is 'small'

Honest-Verifier Zero-Knowledge: simulator can 'fake' transcripts

Security of the IDS

- Passively secure IDS

Soundness: the probability that an adversary can convince is 'small'

- Shows knowledge of secret
- Adversary $\mathcal{A}$ can 'guess right': soundness error κ

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

Honest-Verifier Zero-Knowledge: simulator can 'fake' transcripts

- Shows that transcripts do not leak the secret

Fiat-Shamir transform

- First transform IDS with soundness error κ to negl(k)
  - Using parallel composition

Fiat-Shamir transform

- First transform IDS with soundness error κ to negl(k)
  - Using parallel composition
- Transform IDS into signature
- Non-interactive:

Fiat-Shamir transform

- First transform IDS with soundness error κ to negl(k)
  - Using parallel composition
- Transform IDS into signature
- Non-interactive:
  - Signer is ‘prover’
  - Function $\mathcal{H}$ provides challenges
  - Transcript is signature

Fiat-Shamir transform

- First transform IDS with soundness error κ to negl(k)
  - Using parallel composition
- Transform IDS into signature
- Non-interactive:
  - Signer is ‘prover’
  - Function $\mathcal{H}$ provides challenges
  - Transcript is signature
- Generalize to 5-pass
  - Benefit from lower soundness error

5-pass Fiat-Shamir transform

- Attempt in [EDV+12] incorrect
  - *'n-soundness'*
    - Two transcripts agree up to last challenge ⇒ extract sk
- Vacuous assumption: satisfying schemes reduce to 3-pass
  - HVZK: combine first 3 messages into 1
  - Special soundness: transform transcripts, use extractor

5-pass Fiat-Shamir transform

- Attempt in [EDV+12] incorrect
  - *‘n-soundness’*
    - Two transcripts agree up to last challenge $\Rightarrow$ extract sk
- Vacuous assumption: satisfying schemes reduce to 3-pass
  - HVZK: combine first 3 messages into 1
  - Special soundness: transform transcripts, use extractor
- Existing schemes do not satisfy n-soundness

5-pass Fiat-Shamir transform

- Attempt in [EDV+12] incorrect
  - *'n-soundness'*
    - Two transcripts agree up to last challenge $\Rightarrow$ extract sk
- Vacuous assumption: satisfying schemes reduce to 3-pass
  - HVZK: combine first 3 messages into 1
  - Special soundness: transform transcripts, use extractor
- Existing schemes do not satisfy n-soundness
- n-soundness fixed in [DGV+16]
  - Still does not apply to existing schemes

5-pass Fiat-Shamir transform

- Restrict to challenge spaces of size q resp. 2
  - *'q2-IDS'*
- Prove EU-CMA using dedicated forking lemma

5-pass Fiat-Shamir transform

- Restrict to challenge spaces of size q resp. 2
  - *'q2-IDS'*
- Prove EU-CMA using dedicated forking lemma
  - Assuming a successful forgery ..
  - .. generate 4 signatures fulfilling pattern on challenges
  - .. obtain 4 traces with same commitments, pattern on challenges
  - Use *q2-IDS* that allow extracting sk

$\mathcal{MQ}$ 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:

$$\begin{aligned} y_0 &= a_{0,0}^{(0)} x_0 x_0 + a_{0,1}^{(0)} x_0 x_1 + \ldots + a_{n,n}^{(0)} x_n x_n + b_0^{(0)} x_0 + \ldots + b_n^{(0)} x_n \\ &\vdots \\ y_m &= a_{0,0}^{(m)} x_0 x_0 + a_{0,1}^{(m)} x_0 x_1 + \ldots + a_{n,n}^{(m)} x_n x_n + b_0^{(m)} x_0 + \ldots + b_n^{(m)} x_n \end{aligned}$$

Sakumoto et al. 5-pass IDS [SSH11]

$\mathcal{P} : (\mathbf{F}, \mathbf{v}, \mathbf{s})$		$\mathcal{V} : (\mathbf{F}, \mathbf{v})$
$\mathbf{r}_0, \mathbf{t}_0 \leftarrow_R \mathbb{F}_q^n, \mathbf{e}_0 \leftarrow_R \mathbb{F}_q^m$		
$\mathbf{r}_1 \leftarrow \mathbf{s} - \mathbf{r}_0$		
$c_0 \leftarrow Com(\mathbf{r}_0, \mathbf{t}_0, \mathbf{e}_0)$		
$c_1 \leftarrow Com(\mathbf{r}_1, \mathbf{G}(\mathbf{t}_0, \mathbf{r}_1) + \mathbf{e}_0)$	$\xrightarrow{(c_0, c_1)}$	
	$\xleftarrow{\alpha}$	$\alpha \leftarrow_R \mathbb{F}_q$
$\mathbf{t}_1 \leftarrow \alpha \mathbf{r}_0 - \mathbf{t}_0$		
$\mathbf{e}_1 \leftarrow \alpha \mathbf{F}(\mathbf{r}_0) - \mathbf{e}_0$	$\xrightarrow{\mathrm{resp}_1 = (\mathbf{t}_1, \mathbf{e}_1)}$	
	$\xleftarrow{\mathrm{ch}_2}$	$\mathrm{ch}_2 \leftarrow_R \{0, 1\}$
If $\mathrm{ch}_2 = 0$, $\mathrm{resp}_2 \leftarrow \mathbf{r}_0$		
Else $\mathrm{resp}_2 \leftarrow \mathbf{r}_1$	$\xrightarrow{\mathrm{resp}_2}$	
		If $\mathrm{ch}_2 = 0$, Parse $\mathrm{resp}_2 = \mathbf{r}_0$, 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 $\mathrm{resp}_2 = \mathbf{r}_1$, 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 [SSH11]

- Relies only on $\mathcal{MQ}$, not IP
- Key technique: cut-and-choose for $\mathcal{MQ}$
  - Analogously, consider DLP: $s = r_0 + r_1 \Rightarrow g^s = g^{r_0} \cdot g^{r_1}$
- 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 $\mathbf{F}(\mathbf{r}_0), \mathbf{F}(\mathbf{r}_1)$
  - Split again into $\mathbf{t}_0, \mathbf{t}_1$ resp. $\mathbf{e}_0, \mathbf{e}_1$, using α
  - See [SSH11] for details
- Result: reveal either $(\mathbf{r}_0, \mathbf{t}_1, \mathbf{e}_1)$ or $(\mathbf{r}_1, \mathbf{t}_1, \mathbf{e}_1)$

MQDSS

- Generate keys
  - Sample seed $\mathcal{S}_F \in \{0,1\}^k$, $\mathbf{sk} \in \mathbb{F}_q^n$ $\Rightarrow (\mathcal{S}_F, \mathbf{sk})$
  - Expand $\mathcal{S}_F$ to $\mathbf{F}$, compute $\mathbf{pk} = \mathbf{F}(\mathbf{sk})$ $\Rightarrow (\mathcal{S}_F, \mathbf{pk})$

MQDSS

- Generate keys
  - Sample seed $\mathcal{S}_F \in \{0,1\}^k$, $\mathbf{sk} \in \mathbb{F}_q^n$ $\Rightarrow (\mathcal{S}_F, \mathbf{sk})$
  - Expand $\mathcal{S}_F$ to $\mathbf{F}$, compute $\mathbf{pk} = \mathbf{F}(\mathbf{sk})$ $\Rightarrow (\mathcal{S}_F, \mathbf{pk})$
- Signing
  - Sign randomized digest D over M

MQDSS

- Generate keys
  - Sample seed $\mathcal{S}_F \in \{0,1\}^k$, $\textbf{sk} \in \mathbb{F}_q^n$ $\Rightarrow (\mathcal{S}_F, \textbf{sk})$
  - Expand $\mathcal{S}_F$ to $\textbf{F}$, compute $\textbf{pk} = \textbf{F}(\textbf{sk})$ $\Rightarrow (\mathcal{S}_F, \textbf{pk})$
- Signing
  - Sign randomized digest D over M
  - Perform r rounds of transformed IDS
    - $2r$ commitments, some multiplications in $\mathbb{F}_q$
    - $2r$ $\mathcal{MQ}$ evaluations

MQDSS

- Generate keys
  - Sample seed $\mathcal{S}_F \in \{0,1\}^k$, $\mathbf{sk} \in \mathbb{F}_q^n$ $\Rightarrow (\mathcal{S}_F, \mathbf{sk})$
  - Expand $\mathcal{S}_F$ to $\mathbf{F}$, compute $\mathbf{pk} = \mathbf{F}(\mathbf{sk})$ $\Rightarrow (\mathcal{S}_F, \mathbf{pk})$
- Signing
  - Sign randomized digest D over M
  - Perform r rounds of transformed IDS
    - $2r$ commitments, some multiplications in $\mathbb{F}_q$
    - $2r$ $\mathcal{MQ}$ evaluations
  - Tricks to reduce size
    - Only include necessary commits (hash others) [SSH11]
    - Commit to seeds

MQDSS

- Generate keys
  - Sample seed $\mathcal{S}_F \in \{0,1\}^k$, $\mathbf{sk} \in \mathbb{F}_q^n$ $\Rightarrow (\mathcal{S}_F, \mathbf{sk})$
  - Expand $\mathcal{S}_F$ to $\mathbf{F}$, compute $\mathbf{pk} = \mathbf{F}(\mathbf{sk})$ $\Rightarrow (\mathcal{S}_F, \mathbf{pk})$
- Signing
  - Sign randomized digest D over M
  - Perform r rounds of transformed IDS
    - $2r$ commitments, some multiplications in $\mathbb{F}_q$
    - $2r$ $\mathcal{MQ}$ evaluations
  - Tricks to reduce size
    - Only include necessary commits (hash others) [SSH11]
    - Commit to seeds
- Verifying
  - Reconstruct D, $\mathbf{F}$

MQDSS

- Generate keys
  - Sample seed $\mathcal{S}_F \in \{0,1\}^k$, $\mathbf{sk} \in \mathbb{F}_q^n$ $\Rightarrow (\mathcal{S}_F, \mathbf{sk})$
  - Expand $\mathcal{S}_F$ to $\mathbf{F}$, compute $\mathbf{pk} = \mathbf{F}(\mathbf{sk})$ $\Rightarrow (\mathcal{S}_F, \mathbf{pk})$
- Signing
  - Sign randomized digest D over M
  - Perform r rounds of transformed IDS
    - $2r$ commitments, some multiplications in $\mathbb{F}_q$
    - $2r$ $\mathcal{MQ}$ evaluations
  - Tricks to reduce size
    - Only include necessary commits (hash others) [SSH11]
    - Commit to seeds
- Verifying
  - Reconstruct D, $\mathbf{F}$
  - Reconstruct challenges from σ_0, σ_1
  - Verify responses in σ_2

MQDSS

- Generate keys
  - Sample seed $\mathcal{S}_F \in \{0,1\}^k$, $\mathbf{sk} \in \mathbb{F}_q^n$ $\Rightarrow (\mathcal{S}_F, \mathbf{sk})$
  - Expand $\mathcal{S}_F$ to $\mathbf{F}$, compute $\mathbf{pk} = \mathbf{F}(\mathbf{sk})$ $\Rightarrow (\mathcal{S}_F, \mathbf{pk})$
- Signing
  - Sign randomized digest D over M
  - Perform r rounds of transformed IDS
    - $2r$ commitments, some multiplications in $\mathbb{F}_q$
    - $2r$ $\mathcal{MQ}$ evaluations
  - Tricks to reduce size
    - Only include necessary commits (hash others) [SSH11]
    - Commit to seeds
- Verifying
  - Reconstruct D, $\mathbf{F}$
  - Reconstruct challenges from σ_0, σ_1
  - Verify responses in σ_2
  - Reconstruct missing commitments
  - Check combined commitments hash

MQDSS

- Generate keys
  - Sample seed $\mathcal{S}_F \in \{0,1\}^k$, $\mathbf{sk} \in \mathbb{F}_q^n$ $\Rightarrow (\mathcal{S}_F, \mathbf{sk})$
  - Expand $\mathcal{S}_F$ to $\mathbf{F}$, compute $\mathbf{pk} = \mathbf{F}(\mathbf{sk})$ $\Rightarrow (\mathcal{S}_F, \mathbf{pk})$
- Signing
  - Sign randomized digest D over M
  - Perform r rounds of transformed IDS
    - $2r$ commitments, some multiplications in $\mathbb{F}_q$
    - $2r$ $\mathcal{MQ}$ evaluations
  - Tricks to reduce size
    - Only include necessary commits (hash others) [SSH11]
    - Commit to seeds
- Verifying
  - Reconstruct D, $\mathbf{F}$
  - Reconstruct challenges from σ_0, σ_1
  - Verify responses in σ_2
  - Reconstruct missing commitments
  - Check combined commitments hash
- Parameters: k, n, m, $\mathbb{F}_q$, Com, hash functions, PRGs

MQDSS-31-64

- Security parameter $k = 256$ ($\Rightarrow$ 128-bit PQ security)
- Soundness error κ depends on q
  - $\kappa = \frac{q+1}{2q}$
  - Determines number of rounds: $r = 269$, $\kappa^{269} < (\frac{1}{2})^{256}$
- $\mathbb{F}_q = \mathbb{F}_{31}$, $n = m = 64$
  - Restricted by security
  - Chosen for ease of implementation

MQDSS-31-64

- Security parameter $k = 256$ ($\Rightarrow$ 128-bit PQ security)
- Soundness error κ depends on q
  - $\kappa = \frac{q+1}{2q}$
  - Determines number of rounds: $r = 269$, $\kappa^{269} < (\frac{1}{2})^{256}$
- $\mathbb{F}_q = \mathbb{F}_{31}$, $n = m = 64$
  - Restricted by security
  - Chosen for ease of implementation
- Commitments, hashes, PRGs: SHA3-256, SHAKE-128

MQDSS-31-64

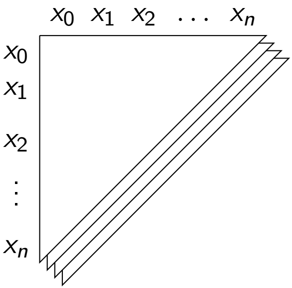
- Security parameter $k = 256$ ($\Rightarrow$ 128-bit PQ security)
- Soundness error κ depends on q
  - $\kappa = \frac{q+1}{2q}$
  - Determines number of rounds: $r = 269$, $\kappa^{269} < (\frac{1}{2})^{256}$
- $\mathbb{F}_q = \mathbb{F}_{31}$, $n = m = 64$
  - Restricted by security
  - Chosen for ease of implementation
- Commitments, hashes, PRGs: SHA3-256, SHAKE-128
- Signature σ contains:
  - R, for random digest $\Rightarrow$ 32B
  - Hash $\mathcal{H}(commits)$ $\Rightarrow$ 32B
  - For every round: $\Rightarrow 269\ \times$
    - Response vectors $\mathbf{t}$, $\mathbf{e}$, $\mathbf{r}$ $\Rightarrow 3 \times$ 40B
    - 'Missing commit' $\Rightarrow$ 32B

Evaluating $\mathcal{MQ}$

- From $\mathbf{F}(\mathbf{x})$ to $\mathbf{x}$ is hard
- From $\mathbf{x}$ to $\mathbf{F}(\mathbf{x})$ should be easy

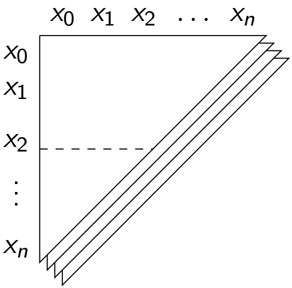
Evaluating $\mathcal{MQ}$

- From $\mathbf{F}(\mathbf{x})$ to $\mathbf{x}$ is hard
- From $\mathbf{x}$ to $\mathbf{F}(\mathbf{x})$ should be fast



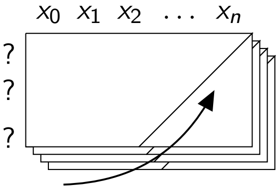
Evaluating $\mathcal{MQ}$

- From $\mathbf{F}(\mathbf{x})$ to $\mathbf{x}$ is hard
- From $\mathbf{x}$ to $\mathbf{F}(\mathbf{x})$ should be fast



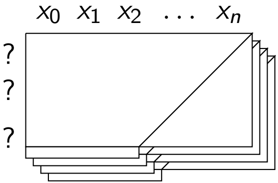
Evaluating $\mathcal{MQ}$

- From $\mathbf{F}(\mathbf{x})$ to $\mathbf{x}$ is hard
- From $\mathbf{x}$ to $\mathbf{F}(\mathbf{x})$ should be fast



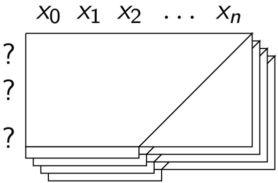
Evaluating $\mathcal{MQ}$

- From $\mathbf{F}(\mathbf{x})$ to $\mathbf{x}$ is hard
- From $\mathbf{x}$ to $\mathbf{F}(\mathbf{x})$ should be fast



Evaluating $\mathcal{MQ}$

- From $\mathbf{F}(\mathbf{x})$ to $\mathbf{x}$ is hard
- From $\mathbf{x}$ to $\mathbf{F}(\mathbf{x})$ should be fast



- Compute monomials, evaluate polynomials
- 64 elements in $\mathbb{F}_{31}$; 16 (or 32) per 256 bit AVX2 register

Benchmarks & conclusion

- Signatures: $\sim$40 KB ($\approx$ SPHINCS)
- Public and private keys: 72 resp. 64 bytes
- Signing time: $\sim$8.5M cycles (2.43ms @ 3.5GHz)
  - Verification 5.2M, key generation 1.8M
- $\sim$6x faster than SPHINCS, $>$10x slower than lattices

Benchmarks & conclusion

- Signatures: ~40 KB (≈ SPHINCS)
- Public and private keys: 72 resp. 64 bytes
- Signing time: ~8.5M cycles (2.43ms @ 3.5GHz)
  - Verification 5.2M, key generation 1.8M
- ~6x faster than SPHINCS, >10x slower than lattices

- Fiat-Shamir transform for *q2*-IDS
- Competitive signatures with (non-tight) reduction to $\mathcal{MQ}$

References I

Koichi Sakumoto, Taizo Shirai and Harunaga Hiwatari.
Public-key identification schemes based on multivariate quadratic polynomials.
In Phillip Rogaway, editor, *Advances in Cryptology – CRYPTO 2011*, volume 6841 of *LNCS*, pages 706-723. Springer, 2011.

Sidi Mohamed El Yousfi Alaoui, Özgür Dagdelen, Pascal Véron, David Galindo and Pierre-Louis Cayrel.
Extended security arguments for signature schemes.
In Aikaterini Mitrokotsa and Serge Vaudenay, editors, *Progress in Cryptology – AFRICACRYPT 2012*, volume 7374 of *LNCS*, pages 19-34. Springer, 2012.

Özgür Dagdelen, David Galindo, Pascal Véron, Sidi Mohamed El Yousfi Alaoui, and Pierre-Louis Cayrel.
Extended security arguments for signature schemes.
In Designs, Codes and Cryptography, 78(2), pages 441–461. Springer, 2016.

References II

Daniel J. Bernstein, Diana Hopwood, Andreas Hülsing, Tanja Lange, Ruben Niederhagen, Louiza Papachristodoulou, Peter Schwabe and Zooko Wilcox O'Hearn.
SPHINCS: Stateless, practical, hash-based, incredibly nice cryptographic signatures.
In Marc Fischlin and Elisabeth Oswald, editors, *Advances in Cryptology – EUROCRYPT 2015*, volume 9056 of *LNCS*, pages 368-397. Springer, 2015.

Johannes Buchmann, Erik Dahmen and Andreas Hülsing.
XMSS – a practical forward secure signature scheme based on minimal security assumptions.
In Bo-Yin Yang, editor, *PQCrypto 2011*, volume 7071 of *LNCS*, pages 117-129. Springer, 2011.

Andreas Hülsing, Joost Rijneveld and Fang Song.
Mitigating multi-target attacks in hash-based signatures.
In Chen-Mou Cheng, Kai-Min Chung, Giuseppe Persiano and Bo-Yin Yang, editors, *Public-Key Cryptography – PKC 2016*, volume 9614 of *LNCS*, pages 387-416. Springer, 2016.

References III

Sedat Akleylek, Nina Bindel, Johannes Buchmann, Juliane Krämer and Giorgia Azzurra Marson.
An Efficient Lattice-Based Signature Scheme with Provably Secure Instantiation.
In David Pointcheval, Abderrahmane Nitaj, Tajjeeddine Rachidi, editors, *Progress in Cryptology – AFRICACRYPT 2016*, volume 9646 of *LNCS*, pages 44-60. Springer, 2016.

Erdem Alkim, Nina Bindel, Johannes Buchmann, Özgür Dagdelen and Peter Schwabe.
TESLA: Tightly-Secure Efficient Signatures from Standard Lattices.
In Cryptology ePrint Archive, Report 2015/755, 2015.

Léo Ducas, Alain Durmus, Tancrède Lepoint, and Vadim Lyubashevsky.
Lattice signatures and bimodal gaussians.
In Ran Canetti and Juan A. Garay, editors, *Advances in Cryptology – CRYPTO 2013*, volume 8042 of *LNCS*, pages 40-56. Springer, 2013.

References IV

Tim Güneysu, Vadim Lyubashevsky and Thomas Pöppelmann.
Practical Lattice-Based Cryptography: A Signature Scheme for Embedded Systems.
In Emmanuel Prouff and Patrick Schaumont, editors, *Cryptographic Hardware and Embedded Systems – CHES 2012*, volume 7428 of *LNCS*, pages 530-547. Springer, 2012.

David Pointcheval and Jacques Stern.
Security proofs for signature schemes.
In Ueli Maurer, editor, *Advances in Cryptology – EUROCRYPT 1996*, volume 1070 of *LNCS*, pages 387-398. Springer, 1996.