

Impact of Quantum Computing to Cryptography – Part III

Ludovic Perret (ludovic.perret@lip6.fr)

Sorbonne University/CNRS
Co-founder of CryptoNext Security

Computability in Europe 2023, 24th-28th July 2023, Batumi, Georgia



Introduction & Organization of the Tutorial

Post-Quantum Cryptography

Cryptosystems secure both against classical and quantum adversaries

Part I. Cryptography in the era to quantum technologies

Part II. On the use of quantum algorithms in cryptanalysis

Part III. A zoom on the design of post-quantum signature schemes

Outline

- 1 Overview
- 2 One-Time Signature and Signature from Hash Functions
- 3 Designing a DSS from an Identification Scheme (IDS)
- 4 Some PQC Hot Topics

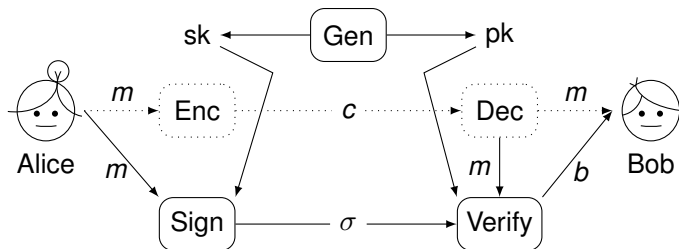
Outline

- 1 Overview
- 2 One-Time Signature and Signature from Hash Functions
- 3 Designing a DSS from an IDentification Scheme (IDS)
- 4 Some PQC Hot Topics

Outline

- 1 **Overview**
- 2 One-Time Signature and Signature from Hash Functions
- 3 Designing a DSS from an IDentification Scheme (IDS)
- 4 Some PQC Hot Topics

Syntax of Digital Signature Schemes



A DSS is a triple of ppt algorithms $\Pi = (\text{KeyGen}, \text{Sign}, \text{Verify})$ such that :

- ❑ Key-generation. $(pk, sk) \leftarrow \text{KeyGen}(1^\lambda)$.
- ❑ Signing. $\sigma \leftarrow \text{Sign}_{sk}(m)$.
- ❑ Verification. $b \leftarrow \text{Verify}_{pk}(m, \sigma)$ (valid if $b = 1$, invalid if $b = 0$)
- ❑ **Basic correctness requirement:** $\text{Verify}_{pk}(m, \text{Sign}_{sk}(m)) = 1$.

Adversarial Models

- ❑ **Key-Only Attacks (KOA)**, unavoidable scenario.
- ❑ **Known Message Attacks (KMA)** where an adversary has access to signatures for a set of known messages.
- ❑ **Chosen-Message Attacks (CMA)** the adversary is allowed to use the signer as an oracle (full access), and may request the signature of any message of his choice

Security Goals

[Unbreakability] the attacker recovers the secret key sk from the public key pk (or an equivalent key if any). This goal is denoted **UB**. Implicitly appeared with public-key cryptography.

[Universal Unforgeability] the attacker, without necessarily having recovered sk , can produce a valid signature of any message in the message space. Noted **UUF**.

[Existential Unforgeability] the attacker creates a message and a valid signature of it (likely not of his choosing). Denoted **EUUF**.

Defining Signature Security

$\text{Sigforge}_{\mathcal{A}, \Pi}(\lambda)$:

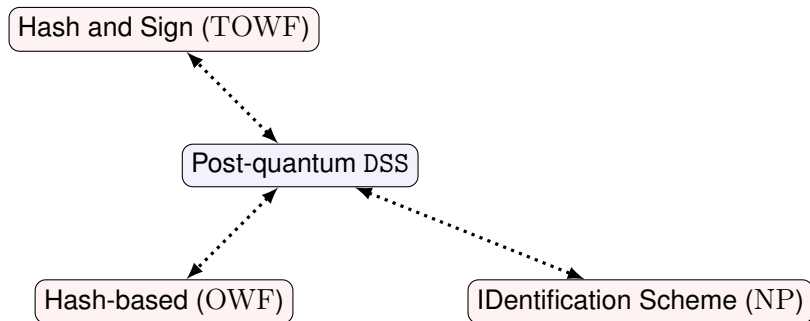
- ❑ $(pk, sk) \leftarrow \text{KeyGen}(1^\lambda)$.
- ❑ \mathcal{A} is given input 1^λ and oracle access to $\text{Sign}_{sk}(\cdot)$, and outputs (m, σ) .
 \mathcal{Q} is the set of queries to its oracle.
- ❑ $\text{Sigforge}_{\mathcal{A}, \Pi}(\lambda) = 1 \iff \text{Verify}_{pk}(m, \sigma) = 1 \wedge m \notin \mathcal{Q}$.

Definition

A signature scheme Π is **EUF-CMA** if $\forall \text{ppt } \mathcal{A}, \exists \text{negl}(\cdot)$ such that:

$$\Pr[\text{Sigforge}_{\mathcal{A}, \Pi}(\lambda) = 1] \leq \text{negl}(\lambda).$$

Design of post-quantum signature schemes



Selected NIST Post-Quantum Signature Candidates

	Category	Problem	#pk	#sig
Dilithium2	FS	Lattice (structured)	1 312 Bytes	2 430 Bytes
Falcon512	HS	Lattice (structured)	897 Bytes	666 Bytes
SPHINCS+s	HB	Hash	32 Bytes	7 856 Bytes
SPHINCS+f	HB	Hash	32 Bytes	17 008 Bytes
GeMSS	HS	Multivariate	352,19 Kytes	0,258 KBytes
Rainbow	HS	Multivariate	58,1 KBytes	48 Bytes
MQDSS	FS	Multivariate	46 Bytes	28 400 Bytes

Outline

- 1 Overview
- 2 One-Time Signature and Signature from Hash Functions**
- 3 Designing a DSS from an Identification Scheme (IDS)
- 4 Some PQC Hot Topics

Security Requirements for Cryptographic Hash Functions

Given a function $F : X \rightarrow Y$:

pre-image resistant (one-way):

if given $y \in Y$ it is computationally infeasible to find a value $x \in X$ s.t.
 $F(x) = y$

second pre-image resistant (weak collision resistant):

if given $x \in X$ it is computationally infeasible to find a value $x' \in X$, s.t.
 $x' \neq x$ and $F(x') = F(x)$

collision resistant (strong collision resistant):

if it is computationally infeasible to find two distinct values $x', x \in X$, s.t.
 $x' \neq x$ and $F(x') = F(x)$

Lamport signatures



L. Lamport.

“Constructing digital signatures from a one-way function.”

Tech. Report SRI-CSL-98, 1979.

- ❑ **Lamport signature** or **Lamport one-time signature scheme** is a method for constructing efficient digital signatures.
- ❑ Lamport signatures can be built from any cryptographically secure **one-way** function; usually a **cryptographic hash function** is used.
- ❑ Unfortunately each Lamport key can only be used to sign a **single** message.

One-Time Signature

$\text{Sigforge}_{\mathcal{A}, \Pi}^{1\text{-time}}(\lambda)$:

- $(pk, sk) \leftarrow \text{KeyGen}(1^\lambda)$.
- \mathcal{A} is given input 1^λ and a **single query** m' to $\text{Sign}_{sk}(\cdot)$, and outputs (m, σ) , $m \neq m'$. and oracle access to $\text{Sign}_{sk}(\cdot)$, and outputs (m, σ) . \mathcal{Q} is the set of queries to its oracle.
- $\text{Sigforge}_{\mathcal{A}, \Pi}^{1\text{-time}}(\lambda) = 1 \iff \text{Verify}_{pk}(m, \sigma) = 1 \wedge m \notin \mathcal{Q}$.

Definition

A signature scheme Π is **EUF under a single-message attack** if

$\forall \text{ppt } \mathcal{A}, \exists \text{negl}(\cdot)$ such that:

$$\Pr[\text{Sigforge}_{\mathcal{A}, \Pi}^{1\text{-time}}(\lambda) = 1] \leq \text{negl}(\lambda).$$

How to sign one bit just once ?

$$\mathcal{M} = \{0, 1\}$$

KeyGen

Generate $F : X \rightarrow Y$ a **one-way function**

Select two random elements $x_0, x_1 \in X$

Compute their images $y_i = F(x_i)$

pk = (y_0, y_1)

sk = (x_0, x_1)

Sign: $m = m_1$, output $\sigma = x_{m_1}$

Verify: $(m = m_1, \sigma)$, outputs 1 $\iff F(\sigma) = y_{m_1}$

How to sign ℓ bits just once ?

$$\mathcal{M} = \{0, 1\}^\ell$$

KeyGen: for $i \in \{1, \dots, \ell\}$:

Generate $F : X \rightarrow Y$ a **one-way function**

choose random $x_{i,0}, x_{i,1} \leftarrow X$.

compute $y_{i,0} := F(x_{i,0})$ and $y_{i,1} := F(x_{i,1})$.

$$\text{pk} = \begin{pmatrix} y_{1,0} & y_{2,0} & \cdots & y_{\ell,0} \\ y_{1,1} & y_{2,1} & \cdots & y_{\ell,1} \end{pmatrix} \quad \text{sk} = \begin{pmatrix} x_{1,0} & x_{2,0} & \cdots & x_{\ell,0} \\ x_{1,1} & x_{2,1} & \cdots & x_{\ell,1} \end{pmatrix}.$$

Sign: $m = m_1 \cdots m_\ell$, output $\sigma = (x_{1,m_1}, \dots, x_{\ell,m_\ell})$.

Verify: $(m = m_1 \cdots m_\ell, \sigma = (x_1, \dots, x_\ell))$, output

$1 \iff F(x_i) = y_{i,m_i}$, for all i .

Theorem

If F is OWF, Π is **EUF** under a single-message attack.

Lamport's signatures: variants

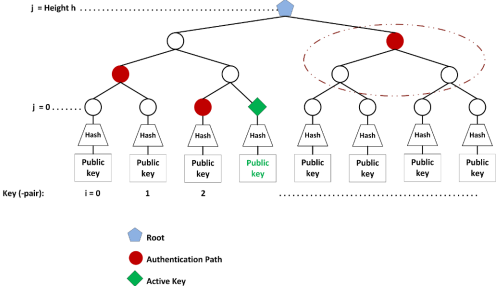
Public key for multiple messages.

many keys have to be published if many messages are to be signed.

a **hash tree** can be used on those public keys, publishing the top hash of the hash tree instead.

this increases the size of the resulting signature (parts of the hash tree have to be included in the signature)


it makes it possible to publish a **single hash** that then can be used to verify any given number of future signatures.



Outline

- 1 Overview
- 2 One-Time Signature and Signature from Hash Functions
- 3 Designing a DSS from an IDentification Scheme (IDS)**
- 4 Some PQC Hot Topics

Multivariate Quadratic Digital Signature Scheme (MQDSS)

 A. Hülsing, J. Rijneveld, S. Samardjiska, P. Schwabe.
"From 5-pass MQ-Based Identification to MQ-Based Signatures."
Asiacrypt 2016.

Provable Security of MQDSS (EU-CMA)

➡ Hardness of solving **random instances** of PoSSo_q+CR of a hash function

PoSSo_q

Input. non-linear **quadratic** polynomials $p_1, \dots, p_m \in \mathbb{F}_q[x_1, \dots, x_n]$

Question. Find – if any – $(z_1, \dots, z_n) \in \mathbb{F}_q^n$ such that:

$$\begin{cases} p_1(z_1, \dots, z_n) = 0, \\ \vdots \\ p_m(z_1, \dots, z_n) = 0. \end{cases}$$

Commitment scheme

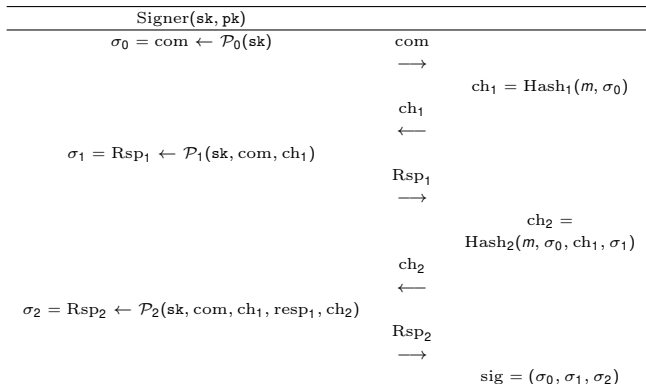
$$\text{com} : \{0, 1\}^* \times \{0, 1\}^\lambda \rightarrow \{0, 1\}^{2\lambda}$$

- ❑ *computationally hiding*, output is computationally indistinguishable from random
- ❑ *computationally binding*, computationally impossible to find different messages committing to the same value
- ☞ Can be constructed from CR hash functions

Canonical 5-pass IDentification Scheme (IDS)

Prover(sk, pk)		Verifier(pk)
$com \leftarrow \mathcal{P}_0(sk)$	com →	
	ch ₁ ←	ch ₁
$Rsp_1 \leftarrow \mathcal{P}_1(sk, com, ch_1)$	Rsp ₁ →	
	ch ₂ ←	ch ₂
$Rsp_2 \leftarrow \mathcal{P}_2(sk, com, ch_1, rsp_1, ch_2)$	Rsp ₂ →	
		$b \leftarrow$ $\mathcal{V}(pk, com, ch_1, rsp_1, ch_2, rsp_2)$

From 5-Pass Zero-Knowledge IDS to Signature – Generic Transform



Properties of an IDS

Definition

IDS is :

- **sound** with **soundness error** κ if \forall ppt adversary \mathcal{A} :

$$\Pr [\langle \mathcal{A}(\text{pk}), \mathcal{V}(\text{pk}) \rangle = 1] \leq \kappa + \text{negl}(\lambda)$$

- **Honest-verifier zero-knowledge** if \exists ppt *simulator* $\mathcal{S}(\text{pk})$ that outputs a transcript $(\text{com}, \text{ch}_1, \text{rsp}_1, \text{vh}_2, \text{rsp}_2)$ from a distribution that is comp. indis. from the distribution of transcripts of an honest execution of the protocol between $\text{Prover}(\text{pk}, \text{sk})$ and $\text{Verifier}(\text{pk})$.

- r iterations of the IDS leads to a soundness error κ^r . Thus:

$$\kappa^r \leq 2^{-\lambda}.$$

- Soundness has direct impact on the signature size

MQDSS



A. Hülsing, J. Rijneveld, S. Samardjiska, P. Schwabe.

"From 5-pass MQ-Based Identification to MQ-Based Signatures."

Asiacrypt 2016.

General idea

Let hom. quad. poly. $\mathbf{p} = (p_1, \dots, p_m) \in \mathbb{F}_q[x_1, \dots, x_n]^m$, $\mathbf{s} \in \mathbb{F}_q^n$ and $\mathbf{v} = \mathbf{p}(\mathbf{s}) \in \mathbb{F}_q^m$.

- Public-key is $(\mathbf{p}, \mathbf{v}) \in \mathbb{F}_q[x_1, \dots, x_n]^m \times \mathbb{F}_q^m$ /secret-key is $\mathbf{s} \in \mathbb{F}_q^n$.
- The coefficients of \mathbf{p} are **random and can be generated from a PRNG**.

The public-key is then given by:

$$(\text{seed}_{\mathbf{p}}, \mathbf{v}) \in \{0, 1\}^\lambda \times \mathbb{F}_q^m,$$

where $\text{seed}_{\mathbf{p}} \in \{0, 1\}^\lambda$ is the seed of the PRNG.

Protocol considers the bilinear form:

$$\mathbf{G}(\mathbf{x}_0, \mathbf{x}_1) = \mathbf{p}(\mathbf{x}_0 + \mathbf{x}_1) - \mathbf{p}(\mathbf{x}_0) - \mathbf{p}(\mathbf{x}_1).$$

5-pass IDS for PoSSo_q [Sakumoto-Shirai-Hiwatari, CRYPTO 2011]

Prover ($\mathbf{s}, (\mathbf{F}, \mathbf{v})$)	Verifier (\mathbf{F}, \mathbf{v})
Rand. pick $(\mathbf{r}_0, \mathbf{t}_0, \mathbf{e}_0) \in \mathbb{F}_q^n \times \mathbb{F}_q^n \times \mathbb{F}_q^m$ $\mathbf{r}_1 \leftarrow \mathbf{s} - \mathbf{r}_0$ $\mathbf{c}_0 \leftarrow \text{com}(\mathbf{r}_0, \mathbf{t}_0, \mathbf{e}_0)$ $\mathbf{c}_1 \leftarrow \text{com}(\mathbf{r}_1, \mathbf{G}(\mathbf{t}_0, \mathbf{r}_1) + \mathbf{e}_0)$	
	$(\mathbf{c}_0, \mathbf{c}_1)$
	\longrightarrow
	$\text{ch}_1 = \alpha \in \mathbb{F}_q$
	\longleftarrow
	ch_1
	\longleftarrow
$\mathbf{t}_1 \leftarrow \alpha \mathbf{r}_0 - \mathbf{t}_0, \mathbf{e}_1 \leftarrow \alpha \mathbf{p}(\mathbf{r}_0) - \mathbf{e}_0$	$(\mathbf{t}_1, \mathbf{e}_1)$
	\longrightarrow
	$\text{ch}_2 \in \{0, 1\}$
	\longleftarrow
	ch_2
	\longleftarrow
If $\text{ch}_2 = 0$, then $\text{Rsp}_2 = \mathbf{r}_0$ Else $\text{Rsp}_2 = \mathbf{r}_1$	Rsp_2
	\longrightarrow
	$b \leftarrow \mathcal{V}(\text{pk}, \text{com}, \text{ch}_1, \text{resp}_1, \text{ch}_2, \text{resp}_2)$

Zero-Knowledge Proof of Knowledge (ZKPoK) for PoSSo_q

Theorem [Sakumoto-Shirai-Hiwatari, CRYPTO 2011]

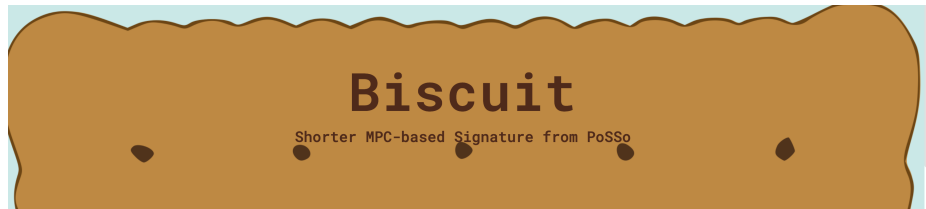
Assuming the hardness of random instances of PoSSo_q and CR hash functions, the 5-pass IDS is ZKPoK and has soundness error

$$\frac{1}{2} + \frac{1}{2q}$$

Provable Security of MQDSS (EUF-CMA)

- Hardness of solving **random instances** of PoSSo_q+CR hash functions

The Biscuit Signature Scheme



Team. L. Bettale, (IDEMIA, France), D. Kahrobaei (Queens College, City University of New York, USA), L. P., J. Verbel (Technology Innovation Institute, UAE)

<https://www.biscuit-pqc.org/>

The Biscuit Signature Scheme

ZK Proof Systems from MPCitH



C Baum, A. Nof.

“Concretely-efficient zero-knowledge arguments for arithmetic circuits and their application to lattice-based cryptography.”

PKC 2020.



D. Kales, G. Zaverucha.

“Efficient Lifting for Shorter Zero-Knowledge Proofs and Post-Quantum Signatures.”

ePrint Arch. 2022.

- ☛ Transform any arithmetic circuit into a ZKP_{oK}; efficiency depends on the number of multiplications

The Biscuit Signature Scheme

The PowAff2 problem

Input. $\mathbf{v} = (v_1, \dots, v_m) \in \mathbb{F}_q^m$ and quadratic equations :

$$p_k(x_1, \dots, x_n) = A_{k,0}(x_1, \dots, x_n) + \prod_{j=1}^2 A_{k,j}(x_1, \dots, x_n), \forall k, 1 \leq k \leq m,$$

with $A_{k,j} = a_0^{(k,j)} + \sum_{i=1}^n a_i^{(k,j)} x_i \in \mathbb{F}_q[x_1, \dots, x_n]$.

Question. Find – if any – a vector $(\mathbf{s}_1, \dots, \mathbf{s}_n) \in \mathbb{F}_q^n$ such that:

$$f_1(\mathbf{s}_1, \dots, \mathbf{s}_n) = v_1, \dots, f_m(\mathbf{s}_1, \dots, \mathbf{s}_n) = v_m.$$

Regularity of $\text{PowAff}(2)$ ($m \leq n$ and big enough field)

Theorem

Let $p_1, \dots, p_m \in \mathbb{F}[x_1, \dots, x_n]$ be a $\text{PowAff}(2)$ instance and $h = n - m$.

There exist $\lambda_{i,j} \in \mathbb{F}$ for which the sequence

$g_1 = p_1^h, g_2 = p_2^h + \sum_{k=3}^m \lambda_{2,k} p_k^h g_k, g_3 = p_3^h + \sum_{k=4}^m \lambda_{3,k} p_k^h g_k, \dots,$
 $g_h = p_h^h + \sum_{k=h+1}^m \lambda_{h,k} p_k^h g_k, g_{h+1} = p_{h+1}^h, \dots, g_m = p_m^h$ is such that :

g_1, \dots, g_m generates the same ideal than p_1^h, \dots, p_m^h and

g_1, \dots, g_m is a regular sequence.

These properties hold for all $\lambda_{i,j} \in \mathbb{F}$ except for finitely many values.

Performances

Biscuit

Shorter MPC-based Signature from PoSSo

Name	Size (bytes)			Performance (cycles)		
	sk	pk	sig	KEYGEN	SIGN	VERIFY
biscuit128s	115	50	4 758	82 632	80 555 671	7 889 9797
biscuit128f	115	50	6 726	82 505	9 653 412	873 4302

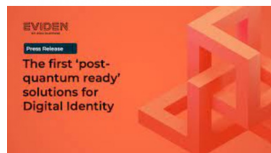
Outline

- 1 Overview
- 2 One-Time Signature and Signature from Hash Functions
- 3 Designing a DSS from an IDentification Scheme (IDS)
- 4 Some PQC Hot Topics

Post-Quantum Cryptography Market

PQC is becoming an industry

THALES



DOCAPOSTE



Challenge 1. Development of new primitives and protocols

New NIST Multi-Party Threshold Cryptography Standardization process

Combination of classical cryptography, PQC and quantum cryptography

- Full ITS solution : QKD with one-time pad

- PQC authentication (DSS or KEM) with QKD

- PQC KEM combined with QKD (defense in-depth)

Hot Topics

Challenge 1. Development of new primitives and protocols

Challenge 2. Asses the security of post-quantum schemes

Availability of small quantum computers

Use of AI for post-quantum cryptanalysis

 [E. Wenger, M. Chen, F. Charton, K. E. Lauter.](#)

“SALSA: Attacking Lattice Cryptography with Transformers.”

[NeurIPS 2022.](#)

Hot Topics

Challenge 1. Development of new primitives and protocols

Challenge 2. Asses the security of post-quantum schemes

Challenge 3. Deployment of quantum-safe cryptography

(open-source) Automatic tools for cryptographic discovery

Hybrid approaches

Adaptation of current security protocols to quantum-safe cryptography

(https, MacSec,...)

Hot Topics

Challenge 1. Development of new primitives and protocols

Challenge 2. Asses the security of post-quantum schemes

Challenge 3. Deployment of quantum-safe cryptography

Special Trimester on Post-Quantum Cryptography – Paris'2024

September 9th to December 13th, 2024

Organisers:

Delaram Kahrobaei (The City University of New York (QC and GC),
University of York (UK), NYU) (co-Chair)
Ludovic Perret (Sorbonne Université) (co-chair)
Jean-Charles Faugere (INRIA, Sorbonne Université)
Vladimir Shpilrain (City College of New York)



Institut
Henri
Poincaré



11, rue Pierre et Marie Curie
75231 Paris Cedex 05
France

Post-quantum algebraic cryptography

Thematic programme with short courses, seminars and workshops

**Introductory summer school at IES
Cargèse, Corsica**
September 9th to 13th, 2024

**Workshop on Deployment of Post-
quantum Cryptography**
October 7th to 11th, 2024

**Workshop on Emerging topics in
design and cryptanalysis of post-
quantum schemes**
November 4th to 8th, 2024

**Workshop on Quantum
technologies for Cryptography**
December 2nd to 6th, 2024

