Aggregating Lattice-Based Signatures

Challenges and New Results

Katharina Boudgoust

CNRS, Univ Montpellier, LIRMM, France

Once upon a time . . .


MATHEMATICAL INSTITUTE

UNIVERSITY OF OXFORD

Members Log in Search

About Us Study Here Research Outreach People Events

Home / Research / Cryptography

Spring School on Lattice-Based Cryptography

- Research
- Members
- Teaching activities
- Cryptography seminars
- Oxford Cryptography Day
- External links
- **Spring School on Lattice-Based Cryptography**

School Overview

The Spring school will take place in March (20-24th), 2017 at the Mathematical Institute, University of Oxford. It aims at covering lattices, their role in modern cryptography, and their potential use in the post-quantum era. Namely, it will cover the basics of lattices, "hard" lattice problems and the reductions between them, and advanced lattice-based cryptography constructions (e.g. Fully Homomorphic Encryption). The school will also have practical sessions using SageMath.

Target Audience: Graduate students and Postdocs.

Location: Lecture Rooms L1 (Mon/Tues) /L3 (Wed-Fri), Andrew Wiles Building, Radcliffe Observatory Site, Woodstock Road, Oxford OX2 6GG.

My very first contact with lattice-based cryptography ☺

Digital Signatures [DH76]*

* Diffie and Hellman, *New directions in cryptography*, IEEE Trans.Inf.Theory 1976

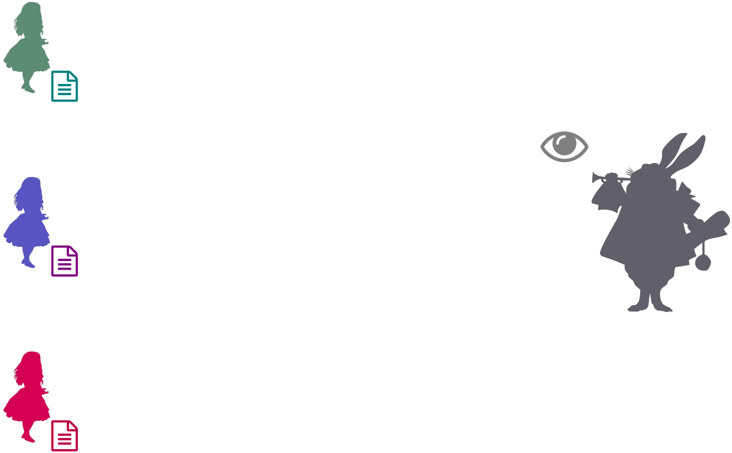
Digital Signatures [DH76]*

Motivation:

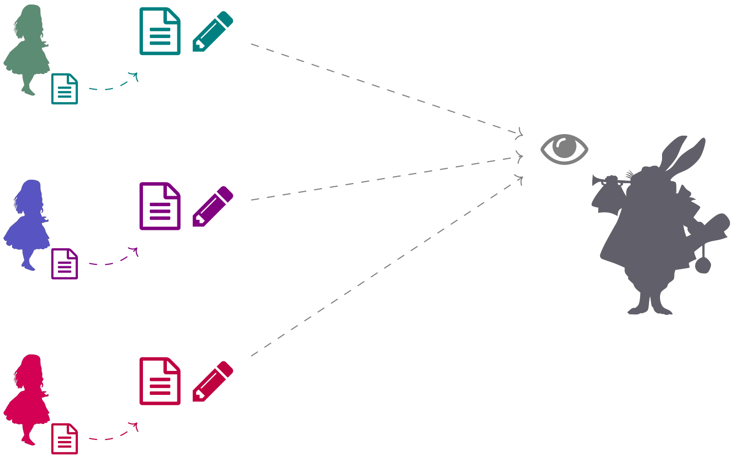
- Digital analogue of handprint signature
- Even more secure?
- Even more functionalities? ⇒ today

* Diffie and Hellman, *New directions in cryptography*, IEEE Trans.Inf.Theory 1976

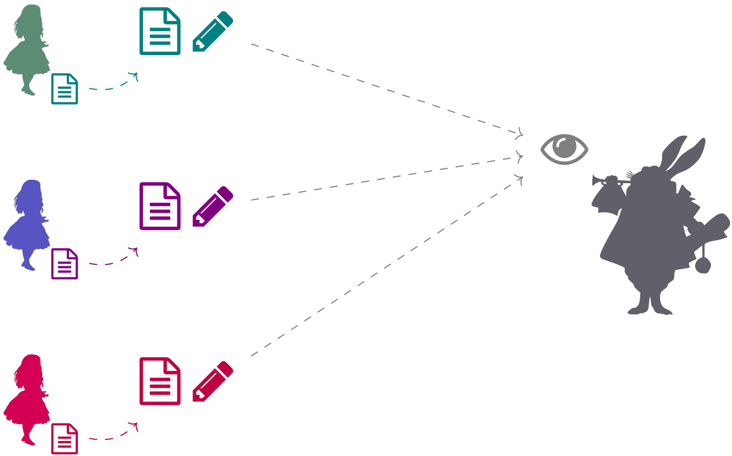
Multiple Signers and Messages, but Same Verifier



Multiple Signers and Messages, but Same Verifier



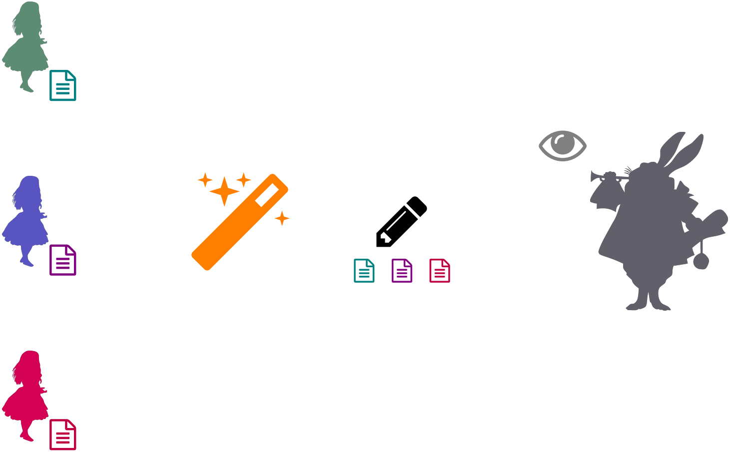
Multiple Signers and Messages, but Same Verifier



Q: Can we combine , and into a single compact signature?

And more generally for $N \gg 3$ many signatures?

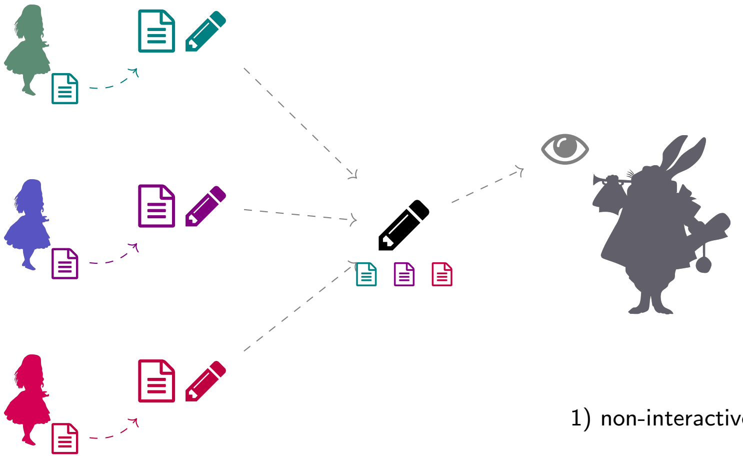
Aggregate Signatures [BGLS03]*



---

*Boneh, Gentry, Lynn and Shacham, *Aggregate and Verifiably Encrypted Signatures from Bilinear Maps*, EUROCRYPT'03

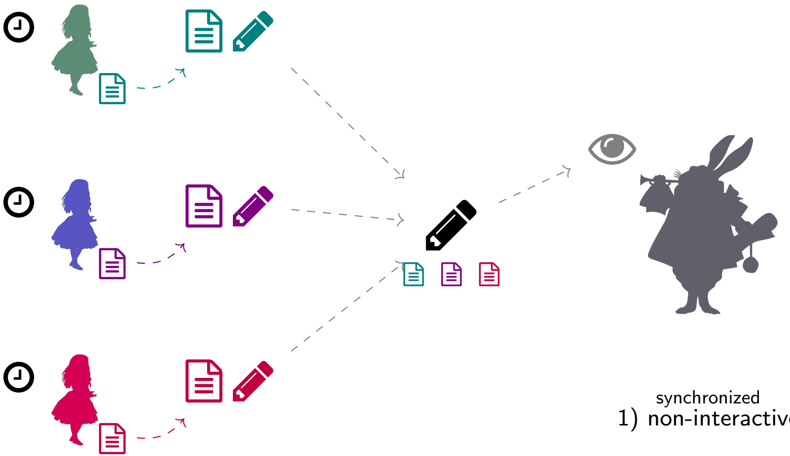
Aggregate Signatures [BGLS03]*



1) non-interactive

*Boneh, Gentry, Lynn and Shacham, *Aggregate and Verifiably Encrypted Signatures from Bilinear Maps*, EUROCRYPT'03

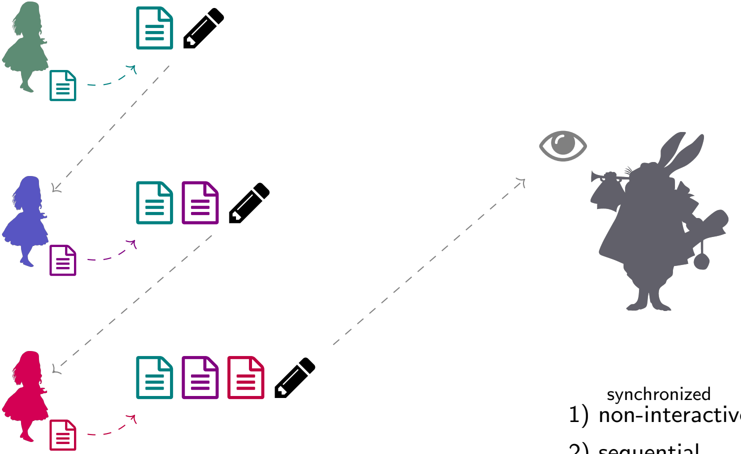
Aggregate Signatures [BGLS03]*



synchronized
1) non-interactive

*Boneh, Gentry, Lynn and Shacham, *Aggregate and Verifiably Encrypted Signatures from Bilinear Maps*, EUROCRYPT'03

Aggregate Signatures [BGLS03]*

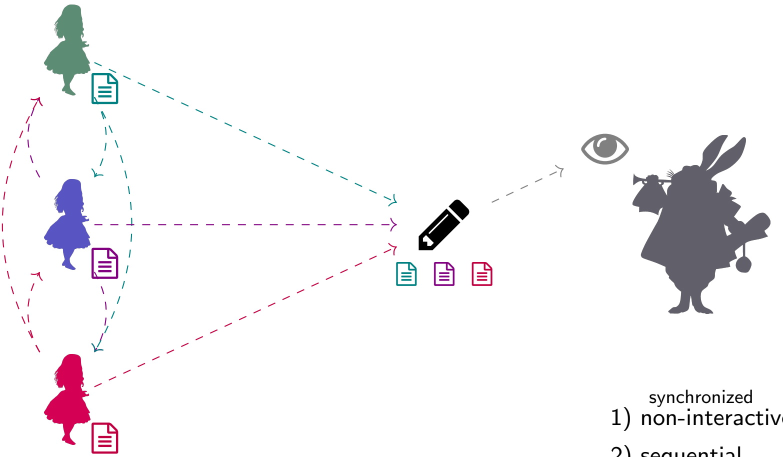


synchronized
1) non-interactive
2) sequential

---

* Boneh, Gentry, Lynn and Shacham, *Aggregate and Verifiably Encrypted Signatures from Bilinear Maps*, EUROCRYPT'03

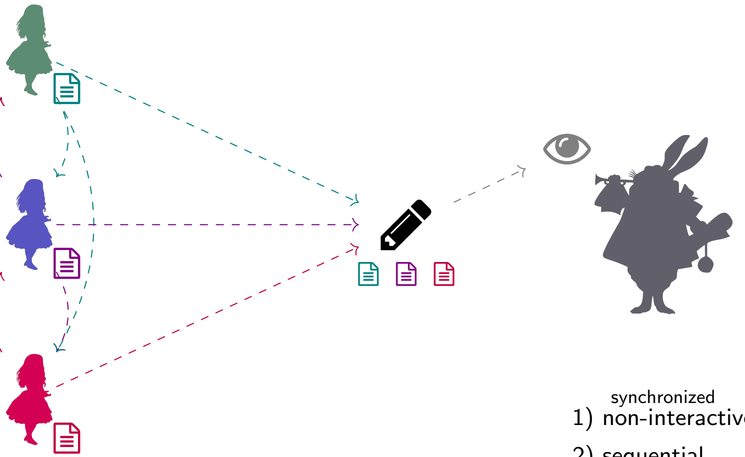
Aggregate Signatures [BGLS03]*



synchronized
1) non-interactive
2) sequential
3) interactive

* Boneh, Gentry, Lynn and Shacham, *Aggregate and Verifiably Encrypted Signatures from Bilinear Maps*, EUROCRYPT'03

Aggregate Signatures [BGLS03]*

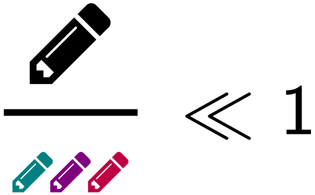


synchronized
1) non-interactive
2) sequential
3) interactive

*Boneh, Gentry, Lynn and Shacham, *Aggregate and Verifiably Encrypted Signatures from Bilinear Maps*, EUROCRYPT'03

Objectives

Compression Rate:



Preferable Goals:

- As few interaction as possible
- As low compression rates as possible
- Presumed post-quantum security
- Compatible with NIST standards (Dilithium and Falcon)
- As fast signing, aggregation and verification as possible

Research Question:

Can we construct an
aggregate signature scheme
based on **Euclidean lattices?**

Research Question:

Can we construct an
aggregate signature scheme
based on **Euclidean lattices?**

Failure:
non-interactive aggregation
compression rate > 1
Dilithium-type
ia.cr/2021/263
CFAIL'22
with A. Roux-Langlois

Semi-Success:
sequential aggregation
$1 >$ compression rate > 0.99
Dilithium-type
ia.cr/2023/159
ESORICS'23
with A. Takahashi

Success:
non-interactive aggregation
compression rate $\rightarrow 0.06$
Falcon
ia.cr/2024/311
CRYPTO'24
with M. Aardal, D. Aranha
S. Kolby, A. Takahashi

Part 1:

Failed Approach

Dilithium-type Signatures

Cyclotomic ring R
Modulus q
Random oracle H
Matrix A over R_q

 🗎

KGen
secret: $s \leftarrow R^k$ small
public: $t = As \mod q$

Sig
$y \leftarrow R^k$ small
$u = Ay \mod q$
$c = H(u, 🗎, t) \in R$ small
$z = s \cdot c + y$ (rejection/drowning)

$\xrightarrow{🗎, ✎ = (u, z)}$

Vf
if $Az \stackrel{?}{=} t \cdot H(u, 🗎, t) + u$
and z small
accept ✎

Dilithium-type Signatures

Cyclotomic ring R
Modulus q
Random oracle H
Matrix A over R_q

 🗎

KGen
secret: $s \leftarrow R^k$ small
public: $t = As \bmod q$

Sig
$y \leftarrow R^k$ small
$u = Ay \bmod q$
$c = H(u, 🗎, t) \in R$ small
$z = s \cdot c + y$ (rejection/drowning)

$\xrightarrow{🗎,\ ✎ = (u, z)}$

Correctness:

$$\begin{aligned} & Az \\ = \ & A(sc + y) \\ = \ & (As)c + Ay \\ = \ & t \cdot H(u, 🗎, t) + u \end{aligned}$$

Vf
if $Az \stackrel{?}{=} t \cdot H(u, 🗎, t) + u$
and z small
accept ✎

Non-interactive Aggregation of Dilithium-type Signatures

 🗎_1

KGen $s_1, t_1 = As_1$

Sig $u_1 = Ay_1$

$c_1 = H(u_1, \text{🗎}_1, t_1)$

$z_1 = s_1 c_1 + y_1$

$\text{✎}_1 = (u_1, z_1)$

 🗎_2

$s_2, t_2 = As_2$

$u_2 = Ay_2$

$c_2 = H(u_2, \text{🗎}_2, t_2)$

$z_2 = s_2 c_2 + y_2$

$\text{✎}_2 = (u_2, z_2)$

Naive idea: $\text{✎} = (u, z) = (u_1 + u_2, z_1 + z_2)$ Vf $Az = t_1 c_1 + t_2 c_2 + u$

---

* Chalkias, Garillot, Kondi and Nikolaenko, *Non-interactive half-aggregation of eddsa and variants of schnorr signatures*, CT-RSA'21

Non-interactive Aggregation of Dilithium-type Signatures

	 📄$_1$	 📄$_2$
KGen	$s_1, t_1 = As_1$	$s_2, t_2 = As_2$
Sig	$u_1 = Ay_1$	$u_2 = Ay_2$
	$c_1 = H(u_1,$ 📄$_1, t_1)$	$c_2 = H(u_2,$ 📄$_2, t_2)$
	$z_1 = s_1 c_1 + y_1$	$z_2 = s_2 c_2 + y_2$
	✎$_1 = (u_1, z_1)$	✎$_2 = (u_2, z_2)$

💡 Naive idea: ✎ $= (u, z) = (u_1 + u_2, z_1 + z_2)$ Vf $Az = t_1 c_1 + t_2 c_2 + u$

✖ Problem: How to compute c_1, c_2? Verifier doesn't know u_1, u_2

⚙ Interactive solution: agree on the same $u_1 = u_2$

⚙ Half-aggregation: ✎ $= (u_1, u_2, z)$, $z = z_1 + z_2$

$\Rightarrow$ successful in discrete log case [CGKN21]*

* Chalkias, Garillot, Kondi and Nikolaenko, *Non-interactive half-aggregation of eddsa and variants of schnorr signatures*, CT-RSA'21

Half-Aggregation - Fail!

Single signature: $= (u, z)$ Verification: $Az = t \cdot H(u, , t) + u$

Smaller signature: $= (c, z)$ Verification: $c = H(Az - tc, , t)$

This works only if you know z

Same trick not possible in the aggregate-over-z setting

Half-aggregation: $= (u_1, u_2, z_1 + z_2)$

Trivial: $= (c_1, z_1, c_2, z_2)$

Fail: $|\;| > |(u_1, u_2)| \quad > \quad |(c_1, z_1, c_2, z_2)| = |\;|$

Dilithium 3:	8.8 KB	1.6 KB

More details ia.cr/2021/263

Part 2:

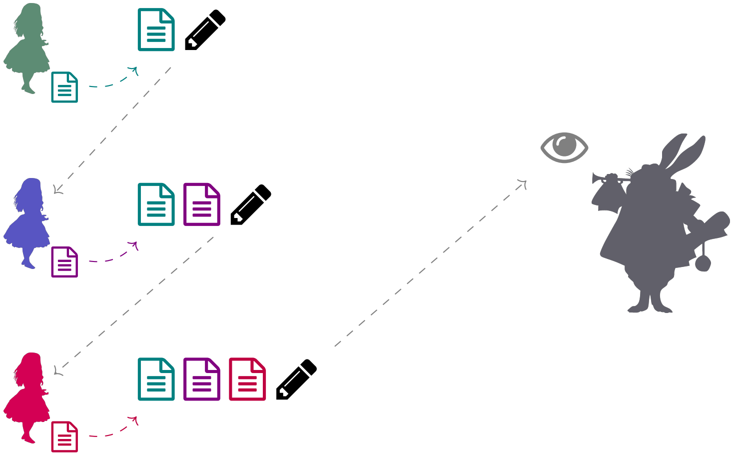
Semi-Successful Approach

Idea

Instead of aggregating the **small** z-parts
Aggregate the **large** u-parts

but requires some form of interaction . . .

Sequential Aggregate Signature [LMRS04]*



* Lysyanskaya, Micali, Reyzin and Shacham, *Sequential aggregate signatures from trapdoor permutations,* EUROCRYPT'04

Sequential Aggregation of Dilithium-type Signatures

🗎$_1$

$s_1, t_1 = A s_1$

$u_1 = A y_1$

$c_1 = H(u_1, 🗎_1, t_1)$

$z_1 = s_1 c_1 + y_1$

✎$_1 = (u_1, z_1)$

🗎$_2$

$s_2, t_2 = A s_2$

$u_2 = A y_2 + u_1$

$c_2 = H(u_2, 🗎_2, t_2, z_1)$

$z_2 = s_2 c_2 + y_2$

✎$_2 = (u_2, z_1, z_2)$

0) compute c_2

1) $u_2 + c_2 \cdot t_2 - A z_2 =: u_1$

2) compute c_1

3) $u_1 + c_1 \cdot t_1 - A z_1 \stackrel{!}{=} 0$

Observations

Security:

- Security tightly implied by security of the plain signature scheme
- No Forking lemma needed
- In the random oracle model

Dilithium:

- Cutting low-order bits does not behave well with aggregation
- We showed an attack against a prior (inter-active) aggregate signature [FH20]*
- ⚠ Our approach does not (directly) apply to to-be-standardized Dilithium

* Fukumitsu and Hasegawa, *A lattice-based provably secure multisignature scheme in quantum random oracle model*, ProvSec'20

Semi-Success

After N sequential aggregations:

Sequential aggregation:	$= (u_N, z_1, \cdots, z_N)$
Trivial:	$= (c_1, \ldots, c_N, z_1, \cdots, z_N)$

Starts to be an improvement when

(large vector over R_q) $\quad |u_N| < |(c_1, \ldots, c_N)| \quad$ (N small scalars over R_q)

Dilithium Level 3: $N > 69$

Compression rate for $N \to \infty$: > 0.99

Part 3:

Successful Approach

Aggregation seems difficult with **Dilithium**

Let's try **Falcon** ☺

Falcon-type Signatures

Cyclotomic ring R
Modulus q
Random oracle H

 📄

secret: 🪄

public: $h \in R_q$

$r \leftarrow \{0,1\}^\lambda$

$t = H(📄, r) \in R_q$

$(s, s') \leftarrow$ 🪄(t) small

$\xrightarrow{📄,\ ✎ = (r, s, s')}$

if $s \cdot h + s' = H(📄, r)$
and (s, s') small
accept ✎

Intuition: difficult to directly aggregate as h different for every Alice

Idea

Tailored aggregation seems difficult

Let's try **generic** solutions ☺

Context and Motivation

Folklore Observation:

Given a generic argument of knowledge with compact proof sizes, one can aggregate signatures.

In particular, proposed for Falcon-like signatures [ACL+22]* and Falcon [HFKC23]*

Caveat:

This is not true for arbitrary signatures. Subtleties occur when random oracles, extractors and additional signing oracles interleave [FN16]*.

We formally prove this approach for the class of hash-then-sign signatures.

Goal:

Find a suitable argument of knowledge, then apply it to Falcon signatures.
Provide rigorous security proofs as well as concrete size estimates.

---

* Albrecht, Cini, Lai, Malavolta and Thyagarajan, *Lattice-based snarks: Publicly verifiable, preprocessing, and recursively composable*, CRYPTO'22

* Hsiang, Fu, Kuo and Cheng, *PQScale: A post-quantum signature aggregation algorithm*, Website 2023

* Fiore and Nitulescu, *On the (in)security of snarks in the presence of oracles*, TCC'16

Folklore Approach

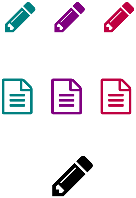
Argument of knowledge (AoK): Let L be a language with corresponding relation R. Given a witness w for a statement x such that $(x, w) \in R$, generate a convincing proof π such that $|\pi| \ll |w|$.

Application to aggregating signatures (AS):

$w :=$

$x :=$

$\pi =:$



R : signature verification

Properties:

- Completeness of AoK $\Rightarrow$ Correctness of AS
- Compact AoK proof sizes $\Rightarrow$ Compact AS sizes
- Knowledge soundness of AoK and security of underlying signature $\Rightarrow$ Security of AS

Folklore Approach

Argument of knowledge (AoK): Let L be a language with corresponding relation R. Given a witness w for a statement x such that $(x, w) \in R$, generate a convincing proof π such that $|\pi| \ll |w|$.

Application to aggregating signatures (AS):

$w :=$ 

$x :=$ 

R : signature verification

$\pi =:$ 

Properties:

- Completeness of AoK $\Rightarrow$ Correctness of AS
- Compact AoK proof sizes $\Rightarrow$ Compact AS sizes
- Knowledge soundness of AoK and security of underlying signature $\Rightarrow$ Security of AS

The AoK of our Choice: LaBRADOR [BS23]*

Witness: $\vec{w}_1, \ldots, \vec{w}_r \in R_q^n$ (r multiplicity, n rank)

Statement: bound β and family $\mathcal{F}$ with functions of the form

$$f(\vec{w}_1, \ldots, \vec{w}_r) = \sum_{i,j=1}^{r} a_{ij} \langle \vec{w}_i, \vec{w}_j \rangle + \sum_{i=1}^{r} \langle \vec{\varphi}_i, \vec{w}_i \rangle - b,$$

with $b, a_{ij} \in R_q$ and $\vec{\varphi}_i \in R_q^n$.

Relation:

$$f(\vec{w}_1, \ldots, \vec{w}_r) = 0 \quad \forall f \in \mathcal{F}$$

and

$$\sum_{i=1}^{r} \|\vec{w}_i\|^2 \leq \beta^2$$

* Beullens and Seiler, *LaBRADOR: Compact Proofs for R1CS from Module-SIS*, CRYPTO'23

Falcon-type Signatures

Cyclotomic ring R
Modulus q
Random oracle H

secret:

public: h

$r \leftarrow \{0,1\}^{\lambda}$

$t = H(\,\cdot\,, r) \in R_q$

$(s, s') \leftarrow (t)$ small

$\xrightarrow{\;,\; = (r, s, s')}$

if $s \cdot h + s' = H(\,\cdot\,, r)$

and (s, s') small

accept

Falcon-type Signatures

Cyclotomic ring R
Modulus q
Random oracle H

involves random oracle

secret:

public: h

$r \leftarrow \{0,1\}^\lambda$

$t = H(\,, r) \in R_q$

$(s, s') \leftarrow (t)$ small

witness

$, = (r, s, s')$

statement

$, h$

relation

if $s \cdot h + s' = H(\,, r)$
and (s, s') small

accept

Falcon-type Signatures

Cyclotomic ring R
Modulus q
Random oracle H

 📄

secret: 🪄

public: h

$r \leftarrow \{0,1\}^{\lambda}$

$t = H(📄, r) \in R_q$

$(s, s') \leftarrow$ 🪄(t) small

witness

📄, ✏️ $= (r, s, s')$

statement

📄, h, $t = H(📄, r)$

relation

if $s \cdot h + s' - t = 0$

and (s, s') small

accept ✏️

Choices and Challenges

Our choice: sticking to Falcon design and parameters

Linear vs. Logarithmic

- Moving seed r to proof $\Rightarrow$ linear proof sizes
- If deterministic or synchronized Falcon $\Rightarrow$ logarithmic proof sizes

Falcon Modulus q vs. LaBRADOR Modulus q'

- Pretty small $q = 12289$, not enough 'room' for LaBRADOR
- Introduce larger q', have to guarantee no wrap-around mod q

Falcon Degree d vs. LaBRADOR Degree d'

- Pretty large $d \in \{512, 1024\}$, yields large proof sizes
- Move to subring of degree $d' \in \{64, 128\}$

And much more: non-interactive knowledge soundness of LaBRADOR, re-arranging starting witness vectors, exact norm bounds, . . .

More details ia.cr/2024/311

Estimates

Non-interactive AS	# signatures N	security level λ	$\lvert$✎$\rvert$
Phoenix [JRLS23]*	500	128	3616 KB
Ours for Falcon-512	500	121	93 KB
Phoenix [JRLS23]	1000	128	3616 KB
Ours for Falcon-512	1000	121	120 KB

Insights:

- Starting to be better than trivial concatenation: $N \approx 100$
- For N towards infinity, compression rate $\rightarrow 0.06$

Some Caveats:

- Parameters set up for $N \leq 10.000$
- Only size estimates, no implementation yet
- New numbers not yet updated on e-print, sorry!

* Jeudy, Roux-Langlois and Sanders, *Phoenix: Hash-and-sign with aborts from lattice gadgets*, PQCrypto'24

Estimates

Non-interactive AS	# signatures N	security level λ	|✎|
Phoenix [JRLS23][⋆]	500	128	3616 KB
Ours for Falcon-512	500	121	93 KB
Phoenix [JRLS23]	1000	128	3616 KB
Ours for Falcon-512	1000	121	120 KB

Synchronized AS	# signatures N	security level λ	|✎|
Chipmunk [FHSZ23][⋆]	1024	128	118 KB
Ours for Falcon-512[⋆]	1024	121	81 KB
Chipmunk [FHSZ23]	8129	128	160 KB
Ours for Falcon-512	8129	121	89 KB

[⋆] Jeudy, Roux-Langlois and Sanders, *Phoenix: Hash-and-sign with aborts from lattice gadgets*, PQCrypto'24

[⋆] Fleischhacker, Herold, Simkin and Zhang, *Chipmunk: Better Synchronized Multi-Signatures from Lattices*, CCS'23

[⋆] Fresh salt replaced by common time stamp

Related Works and Open Questions

Related work

- Interactive aggregation of Dilithium-type signatures (aka multi-signatures) [DOTT21, BTT22]
- Sequential half-aggregation of Falcon-type signatures [BB14, WW19]
- Synchronized aggregate signatures **Chipmunk** [FHSZ23]
- Non-interactive aggregate signatures using MP12-trapdoor sampler **Phoenix** [JRLS23] $\Rightarrow$ on Thursday
- Use LaBRADOR with 'friendlier' signature [TS23]

Any questions or interested in my research?

- Reach out to me today and tomorrow
- Write me an e-mail

Open Positions

Our group at the LIRMM in Montpellier **is hiring**:

- PhD students (3 years) & Postdocs (2 years)
- Cryptography (lattices, class groups, threshold), Codes, Computer Algebra

Open Positions

Our group at the LIRMM in Montpellier **is hiring**:

- PhD students (3 years) & Postdocs (2 years)
- Cryptography (lattices, class groups, threshold), Codes, Computer Algebra
- **Nice old town, see & a lot of sun!**

Open Positions

Our group at the LIRMM in Montpellier **is hiring**:

- PhD students (3 years) & Postdocs (2 years)
- Cryptography (lattices, class groups, threshold), Codes, Computer Algebra
- **Nice old town, see & a lot of sun!**

Thanks for listening

Martin R. Albrecht, Valerio Cini, Russell W. F. Lai, Giulio Malavolta, and Sri Aravinda Krishnan Thyagarajan.
Lattice-based snarks: Publicly verifiable, preprocessing, and recursively composable - (extended abstract).
In *CRYPTO (2)*, volume 13508 of *Lecture Notes in Computer Science*, pages 102–132. Springer, 2022.

Rachid El Bansarkhani and Johannes Buchmann.
Towards lattice based aggregate signatures.
In *AFRICACRYPT*, volume 8469 of *Lecture Notes in Computer Science*, pages 336–355. Springer, 2014.

Dan Boneh, Craig Gentry, Ben Lynn, and Hovav Shacham.
Aggregate and verifiably encrypted signatures from bilinear maps.
In *EUROCRYPT*, volume 2656 of *Lecture Notes in Computer Science*, pages 416–432. Springer, 2003.

Ward Beullens and Gregor Seiler.
Labrador: Compact proofs for R1CS from module-sis.
In *CRYPTO (5)*, volume 14085 of *Lecture Notes in Computer Science*, pages 518–548. Springer, 2023.

Cecilia Boschini, Akira Takahashi, and Mehdi Tibouchi.
Musig-l: Lattice-based multi-signature with single-round online phase, 2022.
Accepted at Crypto 2022.

Konstantinos Chalkias, François Garillot, Yashvanth Kondi, and Valeria Nikolaenko.
Non-interactive half-aggregation of eddsa and variants of schnorr signatures.
In *CT-RSA*, volume 12704 of *Lecture Notes in Computer Science*, pages 577–608. Springer, 2021.

Whitfield Diffie and Martin E. Hellman.
New directions in cryptography.
IEEE Trans. Inf. Theory, 22(6):644–654, 1976.

Ivan Damgård, Claudio Orlandi, Akira Takahashi, and Mehdi Tibouchi.
Two-round n-out-of-n and multi-signatures and trapdoor commitment from lattices.
In *Public Key Cryptography (1)*, volume 12710 of *Lecture Notes in Computer Science*, pages 99–130. Springer, 2021.

Masayuki Fukumitsu and Shingo Hasegawa.
A lattice-based provably secure multisignature scheme in quantum random oracle model.
pages 45–64, 2020.

Nils Fleischhacker, Gottfried Herold, Mark Simkin, and Zhenfei Zhang.
Chipmunk: Better synchronized multi-signatures from lattices.
pages 386–400, 2023.

Dario Fiore and Anca Nitulescu.
On the (in)security of snarks in the presence of oracles.

In *TCC (B1)*, volume 9985 of *Lecture Notes in Computer Science*, pages 108–138, 2016.

Jen-Hsuan Hsiang, Shiuan Fu, Po-Chun Kuo, and Chen-Mou Cheng.
Pqscale: A post-quantum signature aggregation algorithm.
2023.
https://uploads-ssl.webflow.com/642374103c1677f8f335c581/64771752dbe6933ceb1d712b_PQScale.pdf.

Corentin Jeudy, Adeline Roux-Langlois, and Olivier Sanders.
Phoenix: Hash-and-sign with aborts from lattice gadgets.
Cryptology ePrint Archive, 2023.
Accepted at PQCrypto'24.

Anna Lysyanskaya, Silvio Micali, Leonid Reyzin, and Hovav Shacham.
Sequential aggregate signatures from trapdoor permutations.
In *EUROCRYPT*, volume 3027 of *Lecture Notes in Computer Science*, pages 74–90. Springer, 2004.

Toi Tomita and Junji Shikata.
Compact aggregate signature from module-lattices.
Cryptology ePrint Archive, 2023.

Zhipeng Wang and Qianhong Wu.
A practical lattice-based sequential aggregate signature.

In *ProvSec*, volume 11821 of *Lecture Notes in Computer Science*, pages 94–109. Springer, 2019.