(Sequential) Aggregate Signatures Based on Lattices

Katharina Boudgoust

Aarhus University, Denmark

Journées Nationales du GdR Sécurité, Paris

Joint works with Adeline Roux-Langlois & Akira Takahashi

(Sequential) Aggregate Signatures Based on Lattices

Digital Signatures (Informal)

Motivation:

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

Digital Signatures (Formal)

$\Pi_S = (\mathsf{KGen}, \mathsf{Sig}, \mathsf{Vf})$

message 🗎

(sk, vk) ← KGen

🗎, ✎ = Sig(sk, 🗎)
⟶

{0, 1} ← Vf(vk, 🗎, ✎)

Signature is **valid** if 1 ← Vf.

Properties

Correctness

Unforgeability

Applications

Authentication

Multiple Signatures

message 🗎_1

$(\mathsf{sk}_1, \mathsf{vk}_1) \leftarrow \mathsf{KGen}$

$$\xrightarrow{\text{🗎}_1, \text{✎}_1 = \mathsf{Sig}(\mathsf{sk}_1, \text{🗎}_1)}$$

message 🗎_2

$\{0,1\} \leftarrow \mathsf{Vf}(\mathsf{vk}_1, \text{🗎}_1, \text{✎}_1)$

$(\mathsf{sk}_2, \mathsf{vk}_2) \leftarrow \mathsf{KGen}$

$$\xrightarrow{\text{🗎}_2, \text{✎}_2 = \mathsf{Sig}(\mathsf{sk}_2, \text{🗎}_2)}$$

$\{0,1\} \leftarrow \mathsf{Vf}(\mathsf{vk}_2, \text{🗎}_2, \text{✎}_2)$

Q: Can we combine both $(\text{🗎}_1, \text{✎}_1)$ and $(\text{🗎}_2, \text{✎}_2)$ to something shorter?

And more generally for $N \gg 2$ many signatures?

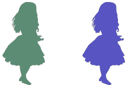
1

(Sequential) Aggregate Signatures Based on Lattices

2

3

Aggregate Signatures: AggSig and AggVf [BGLS03]



$✎_j = \mathsf{Sig}(\mathsf{sk}_j, 🗎_j)$ for $j = 1, 2$

$\mathsf{vk} = (\mathsf{vk}_1, \mathsf{vk}_2)$

$✎ \leftarrow \mathsf{AggSig}(\mathsf{vk}, 🗎_1, 🗎_2, ✎_1, ✎_2)$

$$\xrightarrow{🗎_1, 🗎_2, ✎}$$

only public input

$\{0, 1\} \leftarrow \mathsf{AggVf}(\mathsf{vk}, 🗎_1, 🗎_2, ✎)$

Properties

Correctness

Unforgeability

Compactness

Public aggregation

Applications

Consensus Protocols

Certificate Chains

Aggregate Signatures: AggSig and AggVf [BGLS03]

$\text{✎}_j = \mathrm{Sig}(\mathrm{sk}_j, \text{🗎}_j)$ for $j = 1, 2$

$\mathrm{vk} = (\mathrm{vk}_1, \mathrm{vk}_2)$

$\text{✎} \leftarrow \mathrm{AggSig}(\mathrm{vk}, \text{🗎}_1, \text{🗎}_2, \text{✎}_1, \text{✎}_2)$

$$\xrightarrow{\text{🗎}_1, \text{🗎}_2, \text{✎}}$$

$\{0, 1\} \leftarrow \mathrm{AggVf}(\mathrm{vk}, \text{🗎}_1, \text{🗎}_2, \text{✎})$

Properties

Correctness

Unforgeability

Compactness

Public aggregation

hard to obtain!

Sequential Aggregation: SeqSig and SeqVf [LMRS04]

$✎_1 = \mathsf{Sig}(\mathsf{sk}_1, 🗎_1)$

$\mathsf{vk} = (\mathsf{vk}_1, \mathsf{vk}_2)$

$✎ \leftarrow \mathsf{SeqSig}(\mathsf{sk}_2, 🗎_2, 🗎_1, ✎_1)$

$\xrightarrow{🗎_1, 🗎_2, ✎}$

$\{0,1\} \leftarrow \mathsf{SeqVf}(\mathsf{vk}, 🗎_1, 🗎_2, ✎)$

Properties

Correctness

Compactness

Unforgeability

Applications

Certification Chains

Authenticated Network Routing Protocols

Smart Production

Research Question:

Can we construct a

(sequential) aggregate signature scheme

based on **Euclidean lattices?**

Fail:
public aggregation
ia.cr/2021/263
accepted at CFAIL'22

Success:
sequential aggregation
soon on e-print

1

(Sequential) Aggregate Signatures Based on Lattices

2

3

Signatures on Lattices [Lyu12]

Let $R = \mathbb{Z}[x]/(x^n+1)$, $R_q = R/qR$ and $A' \leftarrow U(R_q^{k\times\ell})$ defining $A = [A'|I_k]$ and $H\colon \{0,1\}^* \to C \subseteq R$ be a random oracle

📄

KGen

$\mathsf{sk} = s \leftarrow R^{k+\ell}$ small

$\mathsf{vk} = t = As \mod q$

Sig

$y \leftarrow R^{k+\ell}$ small, $u = Ay \mod q$

$c = H(u,$ 📄$, t) \in R$ small

$z = s \cdot c + y$ (rejection sampling)

📄, ✏ $= (u, z)$ $\longrightarrow$

Correctness:

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

Vf

if $Az \overset{?}{=} t \cdot H(u,$ 📄$, t) + u$

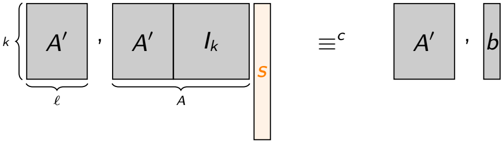
and z small, accept ✏

Unforgeability Based on Lattices

Theorem ([Lyu12])

Assuming the hardness of the lattice problem Module LWE, the signature is secure against forgeries.

Module Learning With Errors (Module LWE): Distinguish



where $s \leftarrow R^{\ell+k}$ small and $(A', b) \leftarrow U(R_q^{k\times\ell} \times R_q^k)$.

- Presumably post-quantum secure
- Strong security guarantees
- Many cryptographic applications

Public Aggregation - First Attempt

🗎_1

🗎_2

KGen

Sig

$\text{sk}_1 = s_1, \text{vk}_1 = t_1 = As_1$	$\text{sk}_2 = s_2, \text{vk}_2 = t_2 = As_2$
$u_1 = Ay_1$	$u_2 = Ay_2$
$c_1 = H(u_1, \text{🗎}_1, t_1)$	$c_2 = H(u_2, \text{🗎}_2, t_2)$
$z_1 = s_1 c_1 + y_1$ (rej. sampling)	$z_2 = s_2 c_2 + y_2$ (rej. sampling)
$✎_1 = (u_1, z_1)$	$✎_2 = (u_2, z_2)$

💡 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

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

Half-Aggregation - Fail!

Single signature: $\text{✎} = (u, z)$ Verification: $Az = t \cdot H(u, \text{📄}, t) + u$
Smaller signature: $\text{✎} = (c, z)$ Verification: $c = H(Az - tc, \text{📄}, t)$

Half-aggregation: $\text{✎} = (u_1, u_2, z_1 + z_2)$
Trivial: $\text{✎} = (c_1, z_1, c_2, z_2)$

Fail: $|\text{✎}| > |(u_1, u_2)| \quad > \quad |(c_1, z_1, c_2, z_2)| = |\text{✎}|$

Dilithium 3: 8.8 KB 1.6 KB

More details ia.cr/2021/263

Sequential Aggregate Signature

$\mathsf{sk}_1 = s_1, \mathsf{vk}_1 = t_1 = As_1$

Sig(sk_1, 🗎$_1$):

$u_1 = Ay_1$

$c_1 = H(u_1,$ 🗎$_1$, $t_1)$

$z_1 = s_1 c_1 + y_1$ (rej. sampling)

✎$_1 = (u_1, z_1)$

$\mathsf{sk}_2 = s_2, \mathsf{vk}_2 = t_2 = As_2$

SeqSig(sk_2, 🗎$_2$, 🗎$_1$, ✎$_1$):

$u_2 = Ay_2 + u_1$

$c_2 = H(u_2,$ 🗎$_2$, $t_2, z_1)$

$z_2 = s_2 c_2 + y_2$ (rej. sampling)

✎$_2 = (u_2, z_1, z_2)$

SeqVf(vk, 🗎$_1$, 🗎$_2$, ✎$_2$): $u_2 + c_2 \cdot t_2 - Az_2 = u_1$

→ ✎$_1 = (u_1, z_1)$

→ Vf(vk_1, 🗎$_1$, ✎$_1$)

Security

Theorem

If $\Pi_S = (\mathsf{KGen}, \mathsf{Sig}, \mathsf{Vf})$ *is secure against forgeries, so is* $\Pi_{SAS} = (\mathsf{KGen}, \mathsf{Sig}, \mathsf{SeqSig}, \mathsf{SeqVf})$ *secure against forgeries as well.*

- Without Forking Lemma → better tightness
- Recall: Π_S is secure assuming lattice problem Module LWE
- In the Random Oracle Model

Parameters

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

$$nk \log_2 q = |u_N| < |(c_1, \ldots, c_N)| = Nn \log_2 3$$

Dilithium Level 3: $N > 69$

Related Works and Open Questions

Related work 🗎

- Inter-active aggregation of FSwA-signatures (aka multi-signatures) [DOTT21, BTT22]
- Sequential half-aggregation of GPV-signatures [BB14, WW19]

Open questions ?

- Non-trivial signatures on lattices with public aggregation and security proof

Thank you.

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.

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

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.

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.

Vadim Lyubashevsky.
Lattice signatures without trapdoors.
In *EUROCRYPT*, volume 7237 of *Lecture Notes in Computer Science*, pages 738–755. Springer, 2012.

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.