



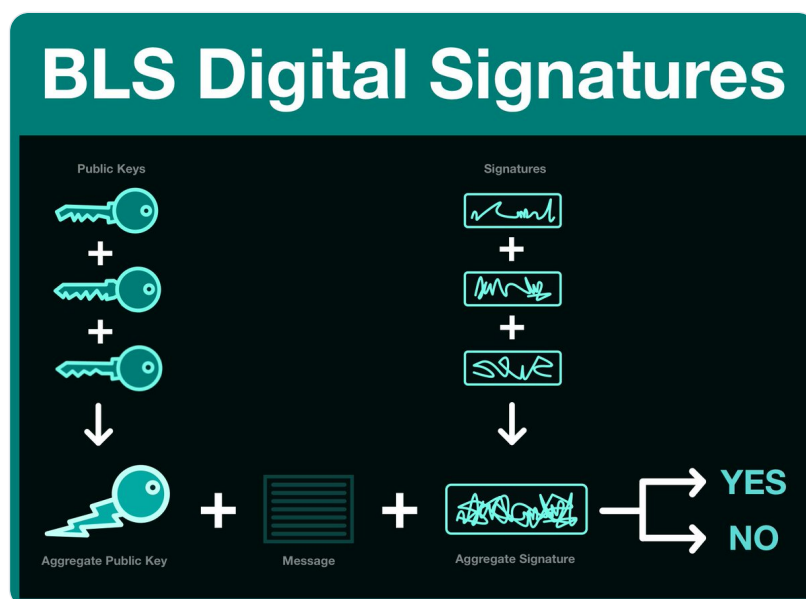
Haym @SalomonCrypto

Sep 29 · 13 tweets · [SalomonCrypto/status/1575279806618292226](https://twitter.com/SalomonCrypto/status/1575279806618292226)

(1/12) Cryptography 201: BLS Digital Signatures

Digital signatures provide cryptographic assurance that a specific person sent a specific message. Their existence is critical, but traditional digital signatures are not scalable.

A manual for aggregation and acceleration.



(2/12) Boneh–Lynn–Shacham Digital Signatures (BLS signatures) are a specific type of digital signature

BLS signatures support the basic properties of digital signatures: proof that the:

- 1) message was sent by the person claiming to send it
- 2) message has not been tampered with

The image shows a screenshot of a Twitter post from a user named Haym (@SalomonCrypto). The tweet is titled "(1/7) Cryptography 101: Digital Signatures" and contains a question about digital trust on the internet. It includes a diagram titled "Digital Signatures" that illustrates the process of signing a message with a private key and verifying it with a public key. The tweet is dated 2:17 PM on Sep 28, 2022, and has 135 likes. Below the tweet are icons for liking, replying, and copying the link.

Haym
@SalomonCrypto · Follow

(1/7) Cryptography 101: Digital Signatures

The internet is the Wild West... how can we know who created a particular piece data? Can we be sure the data hasn't been altered? How can you create trust, trustlessly?

A primer on digital authenticity and integrity.

2:17 PM · Sep 28, 2022

[Read the full conversation on Twitter](#)

135 Reply Copy link

(3/12) Digital signatures in 1 tweet:

Private Key + Message = Signature

Public Key + Message + Signature = Verification

Verification = SPECIFIC message was sent by SPECIFIC sender

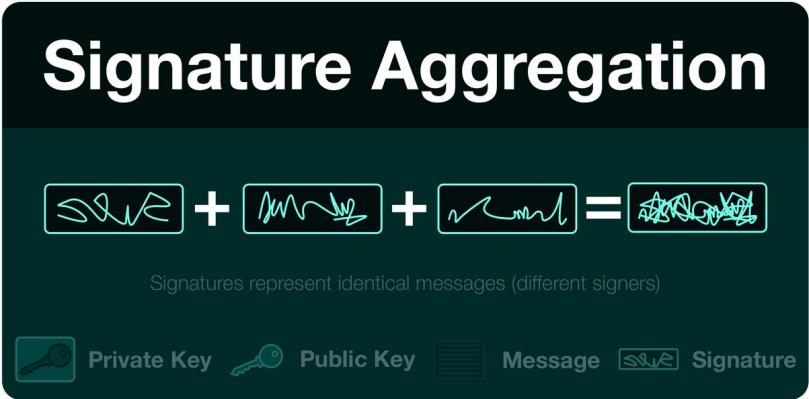


(4/12) BLS signatures function perfectly fine (albeit relatively slowly) as standard cryptographic scheme, but the real magic comes from aggregation.

Aggregation means that given a single message, multiple signatures can be verified with a single operation.

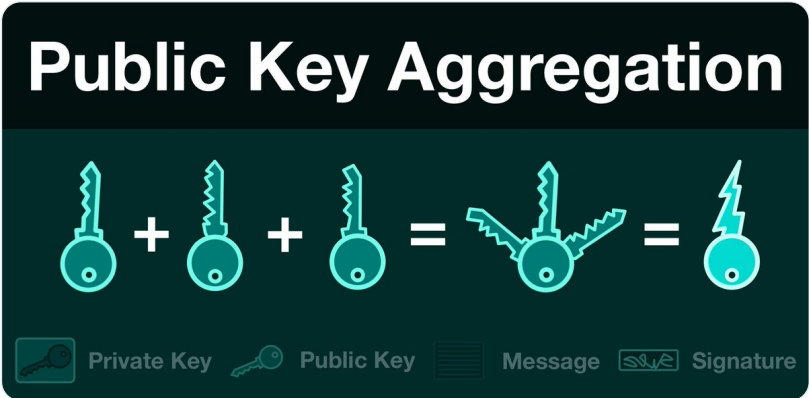
(5/12) Technically "signatures" represent a specific point in an elliptic curve and can be "added up." This is a (computationally) easy operation.

The final result is also a point in the elliptic curve, and is therefore indistinguishable from a non-aggregated signature.



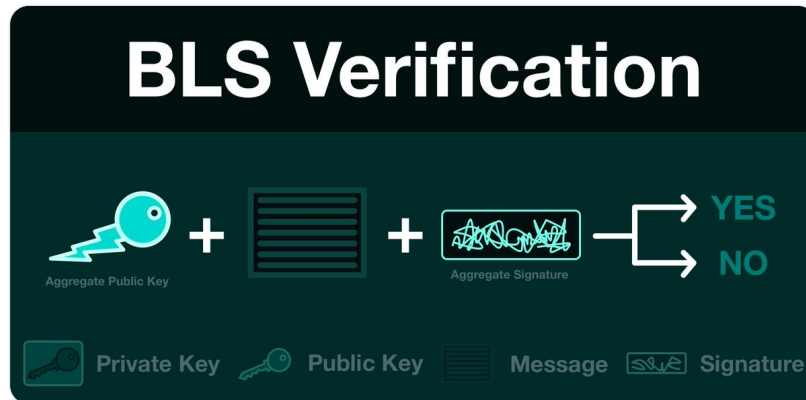
(6/12) Just like a signature, a "public key" is also a point on an elliptic curve and can be similarly "added up" (also computationally easy).

Once again, aggregated public keys are mathematically indistinguishable from non-aggregated public keys.



(7/12) Since aggregate signatures are indistinguishable from normal signatures, and aggregate public keys are indistinguishable from normal public keys, we can reuse our normal verification algorithm.

Thus, a single operation can verify a huge amount of signatures.



(8/12) As previously mentioned, BLS signatures are computationally expensive when compared to verifying a more standard scheme - more than an order of magnitude slower.

However, each verification can count for MUCH more than a standard scheme (a single verification).

(9/12) Imagine you need to verify 100 signatures:

Standard digital signature:

$$x \text{ time/verification} * 100 \text{ verifications} = 100x$$

BLS digital signature:

$$10x \text{ time/verification} * 1 \text{ verification} = 10x$$

The more signatures you can aggregate, the higher the savings

(10/12) But verification speed is not the only benefit: BLS signatures offer huge space savings over non-aggregated signatures.

An aggregated signatures is the same size as a single signature, regardless of how many signatures have been aggregated.

(11/12) Imagine you need to verify 100 signatures:

Standard digital signature:

$$x \text{ bytes/signature} * 100 \text{ signatures} = 100x$$

BLS digital signature:

$$x \text{ bytes/signature} * 1 \text{ signature} = x$$

More aggregation equals more savings, but even more with space than speed.

(12/12) BLS signatures are a type of digital signature that provide the same guarantees as any signature (authenticity and liveness) but provide huge scaling benefits when verifying large groups of signatures.

Can you think of anything that uses lots of digital signatures?

Like what you read? Help me spread the word by retweeting the thread (linked below).

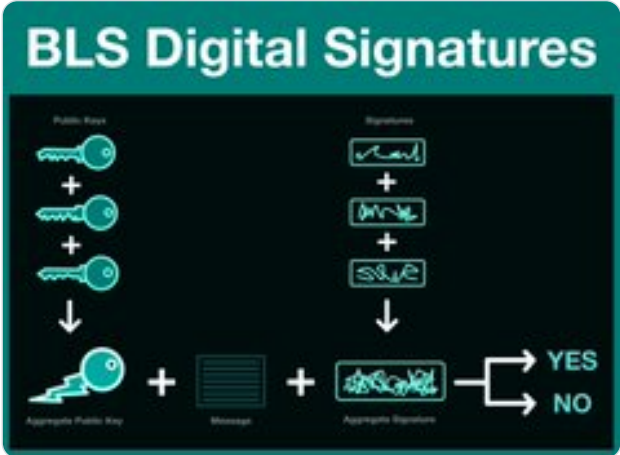
Follow me for more explainers and as much alpha as I can possibly serve.

 **Haym**
@SalomonCrypto · Follow

(1/12) Cryptography 201: BLS Digital Signatures

Digital signatures provide cryptographic assurance that a specific person sent a specific message. Their existence is critical, but traditional digital signatures are not scalable.

A manual for aggregation and acceleration.



12:22 AM · Sep 29, 2022

 [Read the full conversation on Twitter](#)

👍 44 🗨️ Reply 📌 Copy link

...