Notes on BLS Signatures

arnaucube

July 2022

Abstract

Notes taken while reading about BLS signatures [1]. Usually while reading papers I take handwritten notes, this document contains some of them re-written to $LaTeX$.

The notes are not complete, don't include all the steps neither all the proofs.

1 BLS signatures

Key generation $sk \in \mathbb{Z}_q$, $pk = [sk] \cdot g_1$, where $g_1 \in G_1$, and is the generator.

Signature

$$\sigma = [sk] \cdot H(m)$$

where H is a function that maps to a point in G_2. So $H(m), \sigma \in G_2$.

Verification

$$e(g_1, \sigma) == e(pk, H(m))$$

Unfold:

$$e(pk, H(m)) = e([sk] \cdot g_1, H(m) = e(g_1, H(m))^{sk} = e(g_1, [sk] \cdot H(m)) = e(g_1, \sigma))$$

Aggregation Signatures aggregation:

$$\sigma_{aggr} = \sigma_1 + \sigma_2 + \ldots + \sigma_n$$

where $\sigma_{aggr} \in G_2$, and an aggregated signatures is indistinguishable from a non-aggregated signature.

Public keys aggregation:

$$pk_{aggr} = pk_1 + pk_2 + \ldots + pk_n$$

where $pk_{aggr} \in G_1$, and an aggregated public keys is indistinguishable from a non-aggregated public key.

Verification of aggregated signatures Identical to verification of a normal signature as long as we use the same corresponding aggregated public key:

$$e(g_1, \sigma_{aggr}) == e(pk_{aggr}, H(m))$$

Unfold:

$$\begin{aligned}
e(pk_{aggr}, H(m)) = e(pk_1 + pk_2 + \ldots + pk_n, H(m)) = \\
= e([sk_1] \cdot g_1 + [sk_2] \cdot g_1 + \ldots + [sk_n] \cdot g_1, H(m)) = \\
= e([sk_1 + sk_2 + \ldots + sk_n] \cdot g_1, H(m)) = \\
= [sk_1 + sk_2 + \ldots + sk_n] \ \cdot \ e(g_1, H(m)) = \\
= e(g_1, [sk_1 + sk_2 + \ldots + sk_n] \cdot H(m)) = \\
= e(g_1, [sk_1] \cdot H(m) + [sk_2] \cdot H(m) + \ldots + [sk_n] \cdot H(m)) = \\
= e(g_1, \sigma_1 + \sigma_2 + \ldots + \sigma_n) = e(g_1, \sigma_{aggr})
\end{aligned}$$

Note: in the current notes $pk \in G_1$ and $\sigma, H(m) \in G_2$, but we could use $\sigma, H(m) \in G_1$ and $pk \in G_2$.

References

[1] Eth2.0. Eth2.0 book - bls signatures, 2010. https://eth2book.info/altair/part2/building_blocks/signatures.