Transparent Inner Product

Bulletproofs[1] create arguments of knowledge of the inner product of two vectors $\vec{a}, \vec{b} \in \mathbb{Z}_q^m$ with prime q, denoted $\langle \vec{a}, \vec{b} \rangle \in \mathbb{Z}_q$. This is hadamard multiplication, followed by sum, yielding a scalar value. Bulletproofs have $\mathcal{O}(log(m))$ argument size, and $\mathcal{O}(m)$ proving/verification complexity.

However, to achieve hiding, bulletproofs require lightweight (scalar) linear homomorphism. This approach works poorly with post quantum arguments where hidden linear operations are much more expensive. However, a binding only variant is quite cheap using scalar SIS commitments to public coin algebraic structure.

This work proposes using the bulletproof algebraic inner product argument to achieve succinct, *binding only*, arguments of knowledge. This is designed to be composed on top of a module lattice argument of knowledge, which provides *hiding and binding*. Because the inner product argument is stricly logarithmic, scaling to statistical hiding in the module lattice construction has little practical impact on the final argument size.

0.1 TODO

Scalar SIS derivation

1 Argument

Given $\vec{a}, \vec{b} \in \mathbb{Z}_q^m$ yield $c \in \mathbb{Z}_q, \pi \in \mathbb{Z}_q^{log(m)}$, arguing $\langle \vec{a}, \vec{b} \rangle = c$. Denote $\mathcal{H} : \mathbb{Z}_q^{\mathbb{Z}^+} \to \mathbb{Z}_q$ as a collision and pre-image resistant hash function. Prover computes:

$$c \leftarrow \langle \vec{a}, \vec{b} \rangle$$

$$transcript : \vec{t} \xleftarrow{\$} \vec{a}, \vec{b}$$

$$\pi_k \leftarrow \sum_{i=0}^{log(m)}$$

References

[1] Benedikt Bünz and Jonathan Bootle and Dan Boneh and Andrew Poelstra and Pieter Wuille and Greg Maxwell, Bulletproofs: Short Proofs for Confidential Transactions and More, Cryptology ePrint Archive, Paper 2017/1066, 2017, https://eprint.iacr.org/2017/1066