Notes on Halo

arnaucube

July 2022

Abstract

Notes taken while reading Halo paper [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.

Contents

1 modified IPA (from Halo paper)

Notes taken while reading about the modified Inner Product Argument (IPA) from the Halo paper [1].

Objective: Prover wants to prove that the polynomial $p(X)$ from the commitment P evaluates to v at x, and that $deg(p(X)) \leq d-1$.

1.1 Notation

Scalar mul $[a]G$, where a is a scalar and $G \in \mathbb{G}$

Inner product $<\overrightarrow{a}, \overrightarrow{b}>= a_0b_0 + a_1b_1 + \ldots + a_{n-1}b_{n-1}$

Multiscalar mul $<\overrightarrow{a}, \overrightarrow{G}>= [a_0]G_0 + [a_1]G_1 + \ldots + [a_{n-1}]G_{n-1}$

1.2 Transparent setup

$\overrightarrow{G} \in^r \mathbb{G}^d$, $H \in^r \mathbb{G}$

Prover wants to commit to $p(x) = a_0$

1.3 Protocol

Prover:

$$P =< \overrightarrow{a}, \overrightarrow{G} > +[r]H$$

$$v =< \overrightarrow{a}, \{1, x, x^2, \ldots, x^{d-1}\} >$$

where $\{1, x, x^2, \ldots, x^{d-1}\} = \overrightarrow{b}$.

We can see that computing v is the equivalent to evaluating $p(X)$ at x ($p(x) = v$).

We will prove:

i. polynomial $p(X) = \sum a_i X^i$
$p(x) = v$ (that $p(X)$ evaluates x to v).

ii. $deg(p(X)) \leq d - 1$

Both parties know P, point x and claimed evaluation v. For $U \in^r \mathbb{G}$.

Prover computes P':

$$P' = P + [v]U =< \overrightarrow{a}, G > +[r]H + [v]U$$

Now, for k rounds ($d = 2^k$, from $j = k$ to $j = 1$):

- Prover sets random blinding factors: $l_j, r_j \in \mathbb{F}_p$
- Prover computes

$$L_j =< \overrightarrow{a}_{lo}, \overrightarrow{G}_{hi} > +[l_j]H + [< \overrightarrow{a}_{lo}, \overrightarrow{b}_{hi} >]U$$

$$R_j =< \overrightarrow{a}_{hi}, \overrightarrow{G}_{lo} > +[r_j]H + [< \overrightarrow{a}_{hi}, \overrightarrow{b}_{lo} >]U$$

- Verifier sends random challenge $u_j \in \mathbb{I}$
- Prover computes the halved vectors for next round:

$$\overrightarrow{a} \leftarrow \overrightarrow{a}_{hi} \cdot u_j^{-1} + \overrightarrow{a}_{lo} \cdot u_j$$

$$\overrightarrow{b} \leftarrow \overrightarrow{b}_{lo} \cdot u_j^{-1} + \overrightarrow{b}_{hi} \cdot u_j$$

$$\overrightarrow{G} \leftarrow \overrightarrow{G}_{lo} \cdot u_j^{-1} + \overrightarrow{G}_{hi} \cdot u_j$$

After final round, $\overrightarrow{a}, \overrightarrow{b}, \overrightarrow{G}$ are each of length 1.
Verifier can compute

$$G = \overrightarrow{G}_0 = < \overrightarrow{s}, \overrightarrow{G} >$$

and

$$b = \overrightarrow{b}_0 = < \overrightarrow{s}, \overrightarrow{b} >$$

where $\overrightarrow{s}$ is the binary counting structure:

$$\begin{aligned} s = (&u_1^{-1} \; u_2^{-1} \cdots \; u_k^{-1}, \\ &u_1 \quad u_2^{-1} \; \cdots \; u_k^{-1}, \\ &u_1^{-1} \; u_2 \quad \cdots \; u_k^{-1}, \\ &\qquad \vdots \\ &u_1 \quad u_2 \quad \cdots \; u_k) \end{aligned}$$

And verifier checks:

$$[a]G + [r']H + [ab]U == P' + \sum_{j=1}^{k}([u_j^2]L_j + [u_j^{-2}]R_j)$$

where the synthetic blinding factor r' is $r' = r + \sum_{j=1}^{k}(l_j u_j^2 + r_j u_j^{-2})$.

Unfold:

$$[a]G + [r']H + [ab]U == P' + \sum_{j=1}^{k}([u_j^2]L_j + [u_j^{-2}]R_j)$$

$$\begin{aligned} &Left\ side = [a]G + [r']H + [ab]U \\ &= < \overrightarrow{a}, \overrightarrow{G} > \\ &+ [r + \sum_{j=1}^{k}(l_j \cdot u_j^2 + r_j u_j^{-2})] \cdot H \\ &+ < \overrightarrow{a}, \overrightarrow{b} > U \end{aligned}$$

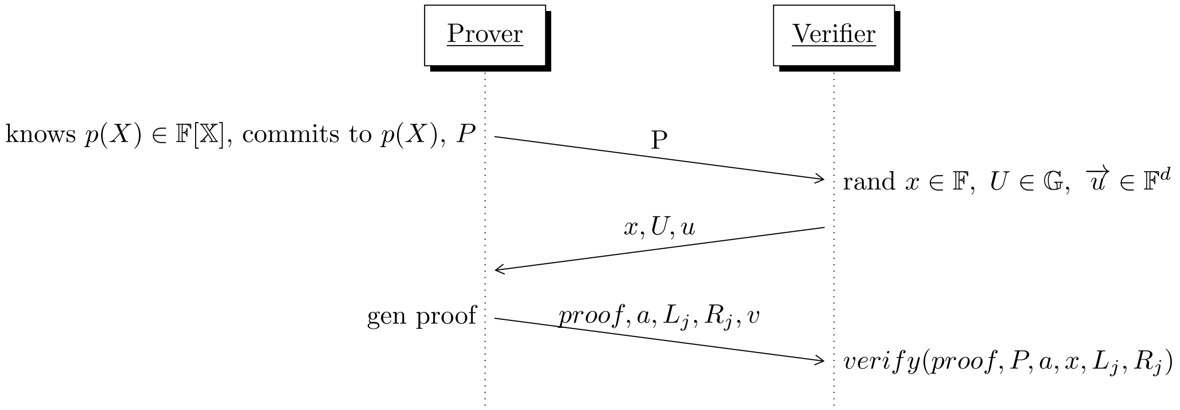
$$Right\ side = P' + \sum_{j=1}^{k}([u_j^2]L_j + [u_j^{-2}]R_j)$$

$$= < \overrightarrow{a}, \overrightarrow{G} > +[r]H + [v]U$$

$$+ \sum_{j=1}^{k}([u_j^2]\cdot < \overrightarrow{a}_{lo}, \overrightarrow{G}_{hi} > +[l_j]H + [< \overrightarrow{a}_{lo}, \overrightarrow{b}_{hi} >]U$$

$$+[u_j^{-2}]\cdot < \overrightarrow{a}_{hi}, \overrightarrow{G}_{lo} > +[r_j]H + [< \overrightarrow{a}_{hi}, \overrightarrow{b}_{lo} >]U)$$

The following diagram ilustrates the main steps in the scheme:


Prover
Verifier
knows $p(X) \in \mathbb{F}[\mathbb{X}]$, commits to $p(X)$, P
P
rand $x \in \mathbb{F},\ U \in \mathbb{G},\ \overrightarrow{u} \in \mathbb{F}^d$
x, U, u
gen proof
$proof, a, L_j, R_j, v$
$verify(proof, P, a, x, L_j, R_j)$

2 Amortization Strategy

TODO

References

[1] Sean Bowe, Jack Grigg, and Daira Hopwood. Recursive proof composition without a trusted setup. Cryptology ePrint Archive, Paper 2019/1021, 2019. https://eprint.iacr.org/2019/1021.