02

Optimizaciones

El paper

8.3 The protocol

We describe the protocol below as a non-interactive protocol using the Fiat-Shamir heuristic. For this purpose we always denote by $\mathsf{transcript}$ the concatenation of the common preprocessed input, and public input, and the proof elements written by the prover up to a certain point in time. We use $\mathsf{transcript}$ for obtaining random challenges via Fiat-Shamir. One can alternatively, replace all points where we write below "compute challenges", by the verifier sending random field elements, to obtain the interactive protocol from which we derive the non-interactive one.

Common preprocessed input:

$$
\begin{array}{l}
n, (x \cdot [1]_1, \ldots, x^{n+5} \cdot [1]_1), (q_{Mi}, q_{Li}, q_{Ri}, q_{Oi}, q_{Ci})_{i=1}^{n}, \sigma^*, \\
\mathsf{q_M}(X) = \sum_{i=1}^{n} q_{Mi} \mathsf{L}_i(X), \\
\mathsf{q_L}(X) = \sum_{i=1}^{n} q_{Li} \mathsf{L}_i(X), \\
\mathsf{q_R}(X) = \sum_{i=1}^{n} q_{Ri} \mathsf{L}_i(X), \\
\mathsf{q_O}(X) = \sum_{i=1}^{n} q_{Oi} \mathsf{L}_i(X), \\
\mathsf{q_C}(X) = \sum_{i=1}^{n} q_{Ci} \mathsf{L}_i(X),
\end{array}
$$

El paper

8.3 The protocol

We describe the protocol below as a non-interactive protocol using the Fiat-Shamir heuristic. For this purpose we always denote by transcript the concatenation of the common preprocessed input, and public input, and the proof elements written by the prover up to a certain point in time. We use transcript for obtaining random challenges via Fiat-Shamir. One can alternatively, replace all points where we write below "compute challenges", by the verifier sending random field elements, to obtain the interactive protocol from which we derive the non-interactive one.

Common preprocessed input:

SRS

$$n, (x \cdot [1]_1, \dots, x^{n+5} \cdot [1]_1), (q_{Mi}, q_{Li}, q_{Ri}, q_{Oi}, q_{Ci})_{i=1}^n, \sigma^*,$$

$$\mathsf{q_M}(X) = \sum_{i=1}^n q_{Mi}\mathsf{L}_i(X),$$
$$\mathsf{q_L}(X) = \sum_{i=1}^n q_{Li}\mathsf{L}_i(X),$$
$$\mathsf{q_R}(X) = \sum_{i=1}^n q_{Ri}\mathsf{L}_i(X),$$
$$\mathsf{q_O}(X) = \sum_{i=1}^n q_{Oi}\mathsf{L}_i(X),$$
$$\mathsf{q_C}(X) = \sum_{i=1}^n q_{Ci}\mathsf{L}_i(X),$$

El paper

$$\mathsf{a}(X) = (b_1 X + b_2)\mathsf{Z_H}(X) + \sum_{i=1}^{n} w_i \mathsf{L}_i(X)$$

$$\mathsf{b}(X) = (b_3 X + b_4)\mathsf{Z_H}(X) + \sum_{i=1}^{n} w_{n+i} \mathsf{L}_i(X)$$

$$\mathsf{c}(X) = (b_5 X + b_6)\mathsf{Z_H}(X) + \sum_{i=1}^{n} w_{2n+i} \mathsf{L}_i(X)$$

$$\begin{aligned}
\mathsf{S}_{\sigma 1}(X) &= \textstyle\sum_{i=1}^{n} \sigma^*(i)\mathsf{L}_i(X), \\
\mathsf{S}_{\sigma 2}(X) &= \textstyle\sum_{i=1}^{n} \sigma^*(n+i)\mathsf{L}_i(X), \\
\mathsf{S}_{\sigma 3}(X) &= \textstyle\sum_{i=1}^{n} \sigma^*(2n+i)\mathsf{L}_i(X)
\end{aligned}$$

Compute linearisation polynomial $\mathsf{r}(X)$:

$$\begin{aligned}
&\mathsf{r}(X) = \\
&\quad \left[\bar{a}\bar{b} \cdot \mathsf{q_M}(X) + \bar{a} \cdot \mathsf{q_L}(X) + \bar{b} \cdot \mathsf{q_R}(X) + \bar{c} \cdot \mathsf{q_O}(X) + \mathsf{PI}(\mathfrak{z}) + \mathsf{q_C}(X)\right] \\
&+\alpha[(\bar{a} + \beta\mathfrak{z} + \gamma)(\bar{b} + \beta k_1 \mathfrak{z} + \gamma)(\bar{c} + \beta k_2 \mathfrak{z} + \gamma) \cdot \mathsf{z}(X) \\
&-(\bar{a} + \beta\bar{\mathsf{s}}_{\sigma 1} + \gamma)(\bar{b} + \beta\bar{\mathsf{s}}_{\sigma 2} + \gamma)(\bar{c} + \beta \cdot \mathsf{S}_{\sigma 3}(X) + \gamma)\bar{z}_\omega] \\
&+\alpha^2\left[(\mathsf{z}(X) - 1)\mathsf{L}_1(\mathfrak{z})\right] \\
&-Z_H(\mathfrak{z}) \cdot (t_{lo}(X) + \mathfrak{z}^n t_{mid}(X) + \mathfrak{z}^{2n} t_{hi}(X))
\end{aligned}$$

Compute permutation polynomial $\mathsf{z}(X)$:

$$\mathsf{z}(X) = (b_7 X^2 + b_8 X + b_9)\mathsf{Z_H}(X)$$

$$+\mathsf{L}_1(X) + \textstyle\sum_{i=1}^{n-1} \left(\mathsf{L}_{i+1}(X) \prod_{j=1}^{i} \frac{(w_j + \beta\omega^j + \gamma)(w_{n+j} + \beta k_1 \omega^j + \gamma)(w_{2n+j} + \beta k_2 \omega^j + \gamma)}{(w_j + \sigma^*(j)\beta + \gamma)(w_{n+j} + \sigma^*(n+j)\beta + \gamma)(w_{2n+j} + \sigma^*(2n+j)\beta + \gamma)}\right)$$

El paper

$$\mathsf{a}(X) = (b_1 X + b_2)\mathsf{Z}_{\mathsf{H}}(X) + \sum_{i=1}^{n} w_i \mathsf{L}_i(X)$$

$_{+i}\mathsf{L}_i(X)$

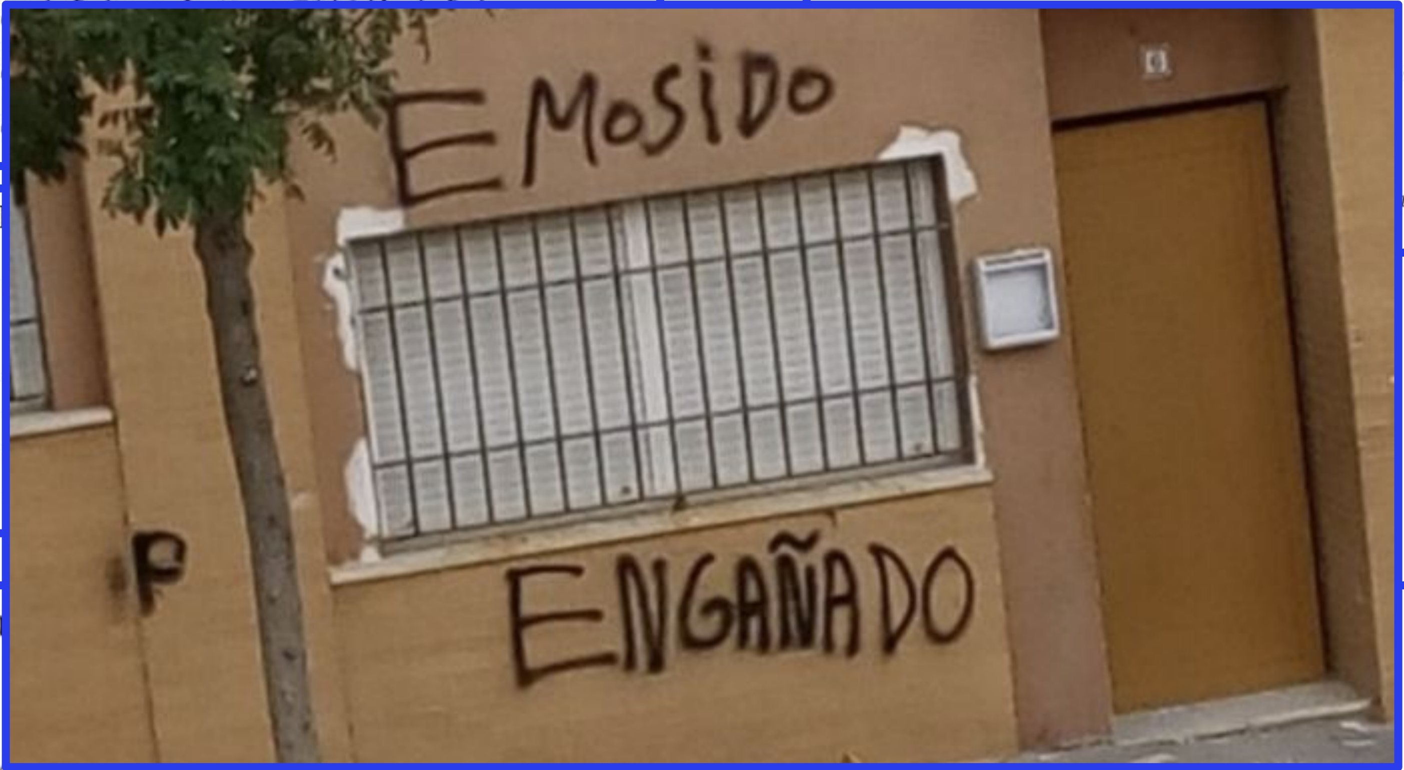
$_{+i}\mathsf{L}_i(X)$

S

S

S

Compute



Compu

$$+\mathsf{L}_1(X) + \sum_{i=1} \Big(\mathsf{L}_{i+1}(X) \prod_{j=1} \frac{\ldots}{(w_j+\sigma^*(j)\beta+\gamma)(w_{n+j}+\sigma^*(n+j)\beta+\gamma)(w_{2n+j}+\sigma^*(2n+j)\beta+\gamma)}\Big)$$

02

Entendiendo el paper

Interpolación de la traza

$$\mathsf{a}(X) = (b_1 X + b_2)\mathsf{Z_H}(X) + \boxed{\sum_{i=1}^{n} w_i \mathsf{L}_i(X)}$$

$$\mathsf{b}(X) = (b_3 X + b_4)\mathsf{Z_H}(X) + \boxed{\sum_{i=1}^{n} w_{n+i} \mathsf{L}_i(X)}$$

$$\mathsf{c}(X) = (b_5 X + b_6)\mathsf{Z_H}(X) + \boxed{\sum_{i=1}^{n} w_{2n+i} \mathsf{L}_i(X)}$$

Interpolación de la traza

$$\mathsf{a}(X) = \qquad + \boxed{\sum_{i=1}^{n} w_i \mathsf{L}_i(X)}$$

- Base de Lagrange:

$$L_i(g^i) = 1$$

$$L_i(g^j) = 0$$ para todo j distinto de i

- $a(g^i) = w_i$

Blindings (ZK!)

$$Z_H = X^n - 1$$

$$\mathsf{a}(X) = \boxed{(b_1 X + b_2)\mathsf{Z_H}(X)} + \sum_{i=1}^{n} w_i \mathsf{L}_i(X)$$

$$\mathsf{b}(X) = \boxed{(b_3 X + b_4)\mathsf{Z_H}(X)} + \sum_{i=1}^{n} w_{n+i} \mathsf{L}_i(X)$$

$$\mathsf{c}(X) = \boxed{(b_5 X + b_6)\mathsf{Z_H}(X)} + \sum_{i=1}^{n} w_{2n+i} \mathsf{L}_i(X)$$

Blindings (ZK!)

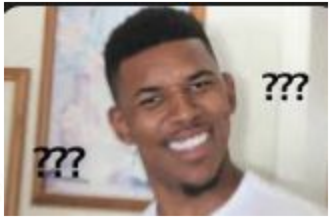
$$Z_H = X^n - 1$$

$$\mathsf{a}(X) = \boxed{(b_1 X + b_2)\mathsf{Z}_\mathsf{H}(X)} + \sum_{i=1}^{n} w_i \mathsf{L}_i(X)$$

- No modifica los valores en el dominio $a(g^i) = w_i$
- Randomiza los valores por fuera del dominio.
  - Consultar $a(z_1)$ y $a(z_2)$ no revela info sobre la traza

El S_σ está raro...

$$
\begin{aligned}
\mathsf{S}_{\sigma 1}(X) &= \textstyle\sum_{i=1}^{n} \sigma^*(i)\mathsf{L}_i(X),\\
\mathsf{S}_{\sigma 2}(X) &= \textstyle\sum_{i=1}^{n} \sigma^*(n+i)\mathsf{L}_i(X),\\
\mathsf{S}_{\sigma 3}(X) &= \textstyle\sum_{i=1}^{n} \sigma^*(2n+i)\mathsf{L}_i(X)
\end{aligned}
$$



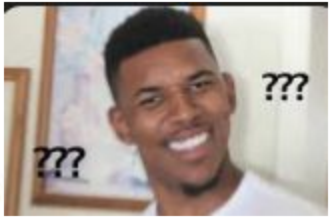
Cuando vimos el protocolo para las máscaras **con la traza aplanada**:

$$\boxed{Z(X)(v_1(X)+\alpha) - Z(gX)(v_2(X)+\alpha)}$$

$$
\begin{aligned}
v_1(X) &\rightsquigarrow \beta D + W\\
v_2(X) &\rightsquigarrow \beta\sigma(D) + W
\end{aligned}
$$

El S_σ está raro...

$$\mathsf{S}_{\sigma 1}(X) = \sum_{i=1}^{n} \sigma^*(i)\mathsf{L}_i(X),$$
$$\mathsf{S}_{\sigma 2}(X) = \sum_{i=1}^{n} \sigma^*(n+i)\mathsf{L}_i(X),$$
$$\mathsf{S}_{\sigma 3}(X) = \sum_{i=1}^{n} \sigma^*(2n+i)\mathsf{L}_i(X)$$



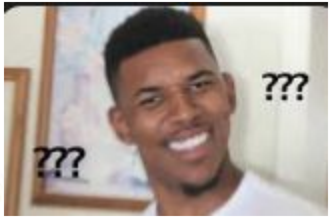
Cuando vimos el protocolo para las máscaras **con la traza W aplanada**:

$$\boxed{Z(X)(v_1(X)+\alpha) - Z(gX)(v_2(X)+\alpha)}$$

$$v_1(X) = \beta X + w(X)$$
$$v_2(X) = \beta S_\sigma(X) + w(X)$$

El S_σ está raro...

$$\mathsf{S}_{\sigma 1}(X) = \sum_{i=1}^{n} \sigma^*(i)\mathsf{L}_i(X),$$
$$\mathsf{S}_{\sigma 2}(X) = \sum_{i=1}^{n} \sigma^*(n+i)\mathsf{L}_i(X),$$
$$\mathsf{S}_{\sigma 3}(X) = \sum_{i=1}^{n} \sigma^*(2n+i)\mathsf{L}_i(X)$$



Cuando vimos el protocolo para las máscaras **con la traza W aplanada**:

$$\boxed{Z(X)(\beta X + w(X) + \alpha) - Z(gX)(\beta S_\sigma(X) + w(X) + \alpha)}$$

El S_σ está raro...

$$
\begin{aligned}
\mathsf{S}_{\sigma 1}(X) &= \textstyle\sum_{i=1}^{n} \sigma^*(i)\mathsf{L}_i(X),\\
\mathsf{S}_{\sigma 2}(X) &= \textstyle\sum_{i=1}^{n} \sigma^*(n+i)\mathsf{L}_i(X),\\
\mathsf{S}_{\sigma 3}(X) &= \textstyle\sum_{i=1}^{n} \sigma^*(2n+i)\mathsf{L}_i(X)
\end{aligned}
$$

Sin aplanar esto queda así:

$$
\boxed{\begin{aligned}
&Z(X)(\beta X + a(X) + \alpha)(\beta X + b(X) + \alpha)(\beta X + c(X) + \alpha)\\
&\qquad - Z(gX)(\beta S_{\sigma 1}(X) + a(X) + \alpha)(\beta S_{\sigma 2}(X) + b(X) + \alpha)(\beta S_{\sigma 3}(X) + c(X) + \alpha)
\end{aligned}}
$$

Juntar los dos protocolos

Vimos protocolos para probar que

- La traza resuelve las ecuaciones Q fila a fila

$$\boxed{a(X)q_L(X) + b(X)q_R(X) + a(X)b(X)q_M(X) + c(X)q_O(X) + q_C(X)}$$

- La traza respeta la máscara

$$\boxed{\begin{aligned}&Z(X)(\beta X + a(X) + \alpha)(\beta X + b(X) + \alpha)(\beta X + c(X) + \alpha)\\&\quad - Z(gX)(\beta S_{\sigma 1}(X) + a(X) + \alpha)(\beta S_{\sigma 2}(X) + b(X) + \alpha)(\beta S_{\sigma 3}(X) + c(X) + \alpha)\end{aligned}}$$

Juntar los dos protocolos

Un solo polinomio haciendo una combinación lineal aleatoria **con γ random**

$$a(X)q_L(X) + b(X)q_R(X) + a(X)b(X)q_M(X) + c(X)q_O(X) + q_C(X)$$

$$+\gamma\left(\begin{array}{l} Z(X)(\beta X + a(X) + \alpha)(\beta X + b(X) + \alpha)(\beta X + c(X) + \alpha) \\ \qquad - Z(gX)(\beta S_{\sigma 1}(X) + a(X) + \alpha)(\beta S_{\sigma 2}(X) + b(X) + \alpha)(\beta S_{\sigma 3}(X) + c(X) + \alpha) \end{array}\right)$$

Juntar los dos protocolos

después de dividir por $Z_H = X^n - 1$

$$
\begin{aligned}
\mathsf{t}(X) = &\\
&(\mathsf{a}(X)\mathsf{b}(X)\mathsf{q_M}(X) + \mathsf{a}(X)\mathsf{q_L}(X) + \mathsf{b}(X)\mathsf{q_R}(X) + \mathsf{c}(X)\mathsf{q_O}(X) + \mathsf{PI}(X) + \mathsf{q_C}(X))\,\frac{1}{\mathsf{Z_H}(X)}\\
&+ ((\mathsf{a}(X) + \beta X + \gamma)(\mathsf{b}(X) + \beta k_1 X + \gamma)(\mathsf{c}(X) + \beta k_2 X + \gamma)\mathsf{z}(X))\,\frac{\alpha}{\mathsf{Z_H}(X)}\\
&- ((\mathsf{a}(X) + \beta \mathsf{S}_{\sigma 1}(X) + \gamma)(\mathsf{b}(X) + \beta \mathsf{S}_{\sigma 2}(X) + \gamma)(\mathsf{c}(X) + \beta \mathsf{S}_{\sigma 3}(X) + \gamma)\mathsf{z}(X\omega))\,\frac{\alpha}{\mathsf{Z_H}(X)}
\end{aligned}
$$

En el paper α es γ y γ es α

Pero en realidad...

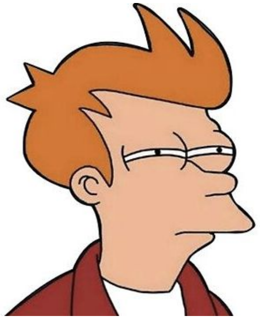
$$
\begin{aligned}
&\mathsf{t}(X) = \\
&\quad (\mathsf{a}(X)\mathsf{b}(X)\mathsf{q_M}(X) + \mathsf{a}(X)\mathsf{q_L}(X) + \mathsf{b}(X)\mathsf{q_R}(X) + \mathsf{c}(X)\mathsf{q_O}(X) + \mathsf{PI}(X) + \mathsf{q_C}(X))\,\frac{1}{\mathsf{Z_H}(X)} \\
&+ ((\mathsf{a}(X) + \beta X + \gamma)(\mathsf{b}(X) + \beta k_1 X + \gamma)(\mathsf{c}(X) + \beta k_2 X + \gamma)\mathsf{z}(X))\,\frac{\alpha}{\mathsf{Z_H}(X)} \\
&- ((\mathsf{a}(X) + \beta \mathsf{S}_{\sigma 1}(X) + \gamma)(\mathsf{b}(X) + \beta \mathsf{S}_{\sigma 2}(X) + \gamma)(\mathsf{c}(X) + \beta \mathsf{S}_{\sigma 3}(X) + \gamma)\mathsf{z}(X\omega))\,\frac{\alpha}{\mathsf{Z_H}(X)} \\
&\boxed{+ (\mathsf{z}(X) - 1)\,\mathsf{L}_1(X)\frac{\alpha^2}{\mathsf{Z_H}(X)}}
\end{aligned}
$$

Pero en realidad...

$$
\begin{aligned}
&\mathsf{t}(X) = \\
&\quad (\mathsf{a}(X)\mathsf{b}(X)\mathsf{q_M}(X) + \mathsf{a}(X)\mathsf{q_L}(X) + \mathsf{b}(X)\mathsf{q_R}(X) + \mathsf{c}(X)\mathsf{q_O}(X) + \mathsf{PI}(X) + \mathsf{q_C}(X))\,\frac{1}{\mathsf{Z_H}(X)} \\
&+ ((\mathsf{a}(X) + \beta X + \gamma)(\mathsf{b}(X) + \beta k_1 X + \gamma)(\mathsf{c}(X) + \beta k_2 X + \gamma)\mathsf{z}(X))\,\frac{\alpha}{\mathsf{Z_H}(X)} \\
&- ((\mathsf{a}(X) + \beta \mathsf{S}_{\sigma 1}(X) + \gamma)(\mathsf{b}(X) + \beta \mathsf{S}_{\sigma 2}(X) + \gamma)(\mathsf{c}(X) + \beta \mathsf{S}_{\sigma 3}(X) + \gamma)\mathsf{z}(X\omega))\,\frac{\alpha}{\mathsf{Z_H}(X)} \\
&\boxed{+ (\mathsf{z}(X) - 1)\,\mathsf{L}_1(X)\,\frac{\alpha^2}{\mathsf{Z_H}(X)}}
\end{aligned}
$$

Equivalente a chequear Z(1) distinto de cero sin hacer openings

Y eso?



$$
\begin{aligned}
&\mathsf{t}(X) = \\
&\quad (\mathsf{a}(X)\mathsf{b}(X)\mathsf{q_M}(X) + \mathsf{a}(X)\mathsf{q_L}(X) + \mathsf{b}(X)\mathsf{q_R}(X) + \mathsf{c}(X)\mathsf{q_O}(X) + \boxed{\mathsf{PI}(X)} + \mathsf{q_C}(X))\,\frac{1}{\mathsf{Z_H}(X)} \\
&+ ((\mathsf{a}(X) + \beta X + \gamma)(\mathsf{b}(X) + \beta k_1 X + \gamma)(\mathsf{c}(X) + \beta k_2 X + \gamma)\mathsf{z}(X))\,\frac{\alpha}{\mathsf{Z_H}(X)} \\
&- ((\mathsf{a}(X) + \beta \mathsf{S}_{\sigma 1}(X) + \gamma)(\mathsf{b}(X) + \beta \mathsf{S}_{\sigma 2}(X) + \gamma)(\mathsf{c}(X) + \beta \mathsf{S}_{\sigma 3}(X) + \gamma)\mathsf{z}(X\omega))\,\frac{\alpha}{\mathsf{Z_H}(X)} \\
&+ (\mathsf{z}(X) - 1)\,\mathsf{L}_1(X)\frac{\alpha^2}{\mathsf{Z_H}(X)}
\end{aligned}
$$

Partiendo t

x es nuestro τ

Common preprocessed input:

$$n, \boxed{(x \cdot [1]_1, \ldots, x^{n+5} \cdot [1]_1)}, (q_{Mi}, q_{i}$$
$$\mathsf{q_M}(X) = \sum_{i=1}^{n} q_{Mi} \mathsf{L}_i(X),$$
$$\mathsf{q_L}(X) = \sum_{i=1}^{n} q_{Li} \mathsf{L}_i(X),$$

Split $\mathsf{t}(X)$ into degree $< n$ polynomials $\mathsf{t}'_{\mathsf{lo}}(X), \mathsf{t}'_{\mathsf{mid}}(X)$ and $\mathsf{t}'_{\mathsf{hi}}(X)$ of degree at most $n+5$, such that

$$\mathsf{t}(X) = \mathsf{t}'_{\mathsf{lo}}(X) + X^n \mathsf{t}'_{\mathsf{mid}}(X) + X^{2n} \mathsf{t}'_{\mathsf{hi}}(X)$$

Now choose random scalars $b_{10}, b_{11} \in \mathbb{F}$ and define

$$\mathsf{t}_{\mathsf{lo}}(X) := \mathsf{t}'_{\mathsf{lo}}(X) + b_{10} X^n, \mathsf{t}_{\mathsf{mid}}(X) := \mathsf{t}'_{\mathsf{mid}}(X) - b_{10} + b_{11} X^n, \mathsf{t}_{\mathsf{hi}}(X) := \mathsf{t}'_{\mathsf{hi}}(X) - b_{11}$$

Partiendo t

Ariel Gabizon
@rel_zeta_tech

To all plonkers out there.
A talented student from TU Wien named Marek Sefranek has discovered a mistake in the implementation of zero-knowledge in Section 8 of the plonk paper.

8:44 AM · Jun 30, 2022

Paper 2024/848

How (Not) to Simulate PLONK

Marek Sefranek, TU Wien

Split $\mathsf{t}(X)$ into degree $< n$ polynomials t
$n+5$, such that

$$\mathsf{t}(X) = \mathsf{t}'_{\mathsf{lo}}(X) + X$$

Now choose random scalars $b_{10}, b_{11} \in \mathbb{F}$ and define

$$\mathsf{t}_{\mathsf{lo}}(X) := \mathsf{t}'_{\mathsf{lo}}(X) + b_{10}X^n, \mathsf{t}_{\mathsf{mid}}(X) := \mathsf{t}'_{\mathsf{mid}}(X) - b_{10} + b_{11}X^n, \mathsf{t}_{\mathsf{hi}}(X) := \mathsf{t}'_{\mathsf{hi}}(X) - b_{11}$$

Linearisation trick

Supongamos que ya commiteamos $[h_1], [h_2], [h_3]$

Y queremos probar

$$h_1(X)h_2(X) - h_3(X) = 0$$

Linearisation trick

Supongamos que ya committeamos $[h_1], [h_2], [h_3]$

Y queremos probar

$$h_1(X)h_2(X) - h_3(X) = 0$$

Opción 1: Enviar $h_1(z)$, $h_2(z)$, $h_3(z)$ con sus respectivas pruebas de KZG

Linearisation trick

Supongamos que ya commiteamos $[h_1], [h_2], [h_3]$

Y queremos probar

$$h_1(X)h_2(X) - h_3(X) = 0$$

Opción 1: Enviar $h_1(z)$, $h_2(z)$, $h_3(z)$ con sus respectivas pruebas de KZG

Opción 2:

1. Enviar $h_2(z)$ con su respectiva prueba de KZG.
2. Enviar la prueba de KZG de que $h_1(X)h_2(z) - h_3(X)$ vale 0 en z

Linearisation trick

Compute linearisation polynomial $\mathsf{r}(X)$:

$$
\begin{aligned}
\mathsf{r}(X) = \\
&\left[\bar{a}\bar{b} \cdot \mathsf{q_M}(X) + \bar{a} \cdot \mathsf{q_L}(X) + \bar{b} \cdot \mathsf{q_R}(X) + \bar{c} \cdot \mathsf{q_O}(X) + \mathsf{PI}(\mathfrak{z}) + \mathsf{q_C}(X)\right] \\
&+\alpha[(\bar{a} + \beta\mathfrak{z} + \gamma)(\bar{b} + \beta k_1\mathfrak{z} + \gamma)(\bar{c} + \beta k_2\mathfrak{z} + \gamma) \cdot \mathsf{z}(X) \\
&-(\bar{a} + \beta\bar{\mathsf{s}}_{\sigma 1} + \gamma)(\bar{b} + \beta\bar{\mathsf{s}}_{\sigma 2} + \gamma)(\bar{c} + \beta \cdot \mathsf{S}_{\sigma 3}(X) + \gamma)\bar{z}_\omega] \\
&+\alpha^2\left[(\mathsf{z}(X) - 1)\mathsf{L}_1(\mathfrak{z})\right] \\
&-Z_H(\mathfrak{z}) \cdot (t_{lo}(X) + \mathfrak{z}^n t_{mid}(X) + \mathfrak{z}^{2n} t_{hi}(X))
\end{aligned}
$$

Batch Opening (1)

Si necesitamos commitear polinomios $f_0, \ldots, f_k$ para luego abrirlos en un elemento random ζ

Basta con commitear solo

$$f_0 + \nu f_1 + \cdots + \nu^k f_k$$

donde ν es otro random elegido por el verifier

Batch Opening (1)

Compute opening proof polynomial $\mathsf{W}_{\mathfrak{z}}(X)$:

$$\mathsf{W}_{\mathfrak{z}}(X) = \frac{1}{X - \mathfrak{z}} \boxed{\left(\begin{array}{l} \mathsf{r}(X) \\ +v(\mathsf{a}(X) - \bar{a}) \\ +v^2(\mathsf{b}(X) - \bar{b}) \\ +v^3(\mathsf{c}(X) - \bar{c}) \\ +v^4(\mathsf{S}_{\sigma 1}(X) - \bar{\mathsf{s}}_{\sigma 1}) \\ +v^5(\mathsf{S}_{\sigma 2}(X) - \bar{\mathsf{s}}_{\sigma 2}) \end{array} \right)}$$

Batch Opening (1)

Compute opening proof polynomial $\mathsf{W}_{\mathfrak{z}}(X)$:

$$\mathsf{W}_{\mathfrak{z}}(X) = \frac{1}{X - \mathfrak{z}} \boxed{\begin{pmatrix} \mathsf{r}(X) \\ +v(\mathsf{a}(X) - \bar{a}) \\ +v^2(\mathsf{b}(X) - \bar{b}) \\ +v^3(\mathsf{c}(X) - \bar{c}) \\ +v^4(\mathsf{S}_{\sigma 1}(X) - \bar{\mathsf{s}}_{\sigma 1}) \\ +v^5(\mathsf{S}_{\sigma 2}(X) - \bar{\mathsf{s}}_{\sigma 2}) \end{pmatrix}}$$

Polinomio auxiliar en el batch Open de KZG

Batch Opening (2)

Si necesitamos commitear polinomios f_1, f_2 para luego abrirlos en elementos elemento random ζ_1 y ζ_2

Basta con chequear una sola igualdad de pairings

$$\boxed{e([t_1] + u[t_2], [\tau]) = e(\zeta_1[t_1] + u\zeta_2[t_2] + [f_1 - y_1] + [f_2 - y_2], [1])}$$

Batch Opening (2)

$$\boxed{e([t_1] + u[t_2], [\tau]) = e(\zeta_1[t_1] + u\zeta_2[t_2] + [f_1 - y_1] + [f_2 - y_2], [1])}$$

12. Batch validate all evaluations:

$$e([W_{\mathfrak{z}}]_1 + u \cdot [W_{\mathfrak{z}\omega}]_1, [x]_2) \stackrel{?}{=} e(\mathfrak{z} \cdot [W_{\mathfrak{z}}]_1 + u\mathfrak{z}\omega \cdot [W_{\mathfrak{z}\omega}]_1 + [F]_1 - [E]_1, [1]_2)$$

¡Muchas gracias!