SNARKs

Thursday, November 30, 2017
12:32 PM

More Notebooks
Andrew's Notebook

Verifiable Encryption and the CRS model

Common Reference String

Start with relating RICS (w, y, z)

Prover (\text{Prover})

CRS ← Setup (\text{Public parameters})

Verifier (\text{Verifier})

\[ \text{Verifier} \rightarrow \text{Prover} \]

- Correctness
- Extractability
- (optimal) Zero Knowledge

Trusted Setup:
- Like choosing generators for discrete logs
  \[ g^k \in G \]
- If uniform parameters should use "NUMS"!
- Otherwise, need to flip coins, then forget the coins

Ex. \begin{align*}
  \text{Setup}(\mathcal{P}) &= \frac{p}{2} \\
  z &\in \mathbb{Z}_p, \quad g \in G \\
  \text{CRS} &= (g, g^2, g^3, \ldots, g^n)
\end{align*}

Succinct Non-Interactive Argument of Knowledge

\[ \text{verify is fast} \]

Recall RICS over a field \( F \)

in variables \( a, \ldots, a_m \):

\[ \exists a \mid 3 \text{ ranges over 1, \ldots, m} \]
Also \( a_0 = 1 \)

In all constraints \( U, V, W \) are \( m \times n \) matrices of coefficients of \( F \)

(1) \( \forall q \quad (\sum_i U_{i,q} \cdot a_i) \cdot (\sum_i V_{i,q} \cdot a_i) = (\sum_i W_{i,q} \cdot a_i) \)

Encode computations:

\[
\begin{align*}
\begin{array}{cccc}
\text{a_1,} & \text{...} & \text{a_{m}} \\
\text{inputs} & & \text{outputs} & \text{internal wires} \\
\end{array}
\end{align*}
\]

For V.C.

\( F(q) = \text{out} \quad \text{Statement} \quad \text{witness} \)

For ZK

\[
\text{witness} \quad \text{public inputs} \quad \text{private inputs} \quad \text{also be part of the witness}.
\]

\[\text{ZK} \{ (a, \text{witness}) : R1CSUYW (a, \text{witness} \oplus a \text{ statement}) \} \]

**Step 1.** Encode \( U, V, W \) as polynomials

Take arbitrary roots \( r_1, \ldots, r_n \in F \)

Could be \( r_1 = 1, r_2 = 2, \ldots \) one for each constraint.

\( \forall i \), define \( U_i (X) \) by interpolation so that

\[
\begin{align*}
U_i (r_1) &= U_{i,1} \\
U_i (r_2) &= U_{i,2} \\
U_i (r_n) &= U_{i,n} \\
\end{align*}
\]

\( U_i (X) \) each polynomial is degree \( (n-1) \)

(2) \( \forall q \quad (\sum_i U_i (r_q) \cdot a_i) \cdot (\sum_i V_i (a_i) \cdot a_i) = (\sum_i W_i (a_i) \cdot a_i) \)

Define \( P(X) = (\sum_i U_i (X) a_i) \cdot (\sum_i V_i (X) a_i) - (\sum_i W_i (X) a_i) \)

(3) \( \forall q \quad P(r_a) = 0 \quad \text{a degree } 2(n-1) \text{ over } X \)

with roots at least \( n \) roots
Define a smaller degree polynomial \( + (X) \) that has the same:

- has roots at each \( r_a \)
- degree \( n \)
- "monic" leading coefficient is 1

\[ + (X) = X^n + \alpha x^{n-1} + \ldots \]

If \( p(X) \) shares \( n \) roots with \( + (X) \), then \( p(X) \) is a multiple of \( + (X) \).

4) \[ p(X) \equiv 0 \mod + (X) \]

5) \( \exists \) polynomial \( h(X) \) s.t. \[ + (X) \cdot h(X) = p(X) \]

\[
\begin{align*}
p(x) & = 5x^4 + \ldots \quad \text{divides by } t(x) = x^3 + \ldots \\
p(x) &= (5x) \cdot + (x) + \text{(rem}(x)) \quad \text{degree 3 or less} \\
p(x) &= (5x^4 + \ldots) + \text{(rem}(x)) \\
p_1(x) &= + (x) \cdot h(x) + \text{rem}(x) \\
\text{deg}(\text{rem}) &\leq \text{deg}(p) - \text{degree}(+) 
\end{align*}
\]

Step 3) Sufiices to check \( p(s) = h(s) \cdot t(s) \)

for a randomly chosen \( s \) in \( \mathbb{F} \).

Setup 1: \( U_i(X), V_i(X), W_i(X), \ldots, + (X) \) only depends on \( r_1 \ldots r_n \)

Prove: \( \bar{a} \) depends on \( U_1(X), V_1(X), W_1(X), \ldots, + (X) \)

Compute \( h(\bar{a}) = p(\bar{a}) / t(\bar{a}) \)

```
```

\[ h(\bar{a}) \]
Prover makes \( \pi = p(s), h(s), t(s) \)
Verify \( p(s) = h(s) + t(s) \)
Remaining problem: need to check that \( p(s) \) are done consistantly.

Step 3). Setup \( \Sigma \subseteq E \)

map \( u_i(X), v_i(x), w_i(X) \) to elements in \( G \)

\[
\text{CRS} := \{ g^{u_i(s)} \} \cup \{ g^{v_i(s)} \} \cup \{ g^{w_i(s)} \}, g^{t(s)} \quad \ldots
\]

Prover computes \( p(X), h(X) \)

\[
g_i = \prod (g^{u_i(s)})^{a_i}
\]

Same for \( g_j^{v_i(s)} a_j \) and \( g_j^{w_i(s)} a_j \)

Also add \( \text{CRS} := \ldots, g^s, g^2, g^3, \ldots, g^n \)

Prover has \( h(X) = p(X)/t(X) \quad h(X) = h_0 + h_1 x + \ldots + h_n x^n \)

\[
g = g_0^{h_0}(g^s)^{h_1} \ldots = \prod (g^{s_i})^{h_i}
\]

Sends \( g^{u_i(s)}, g^{v_i(s)}, g^{w_i(s)}, h(s) \) to verifier

\[
u_i(s) = \sum u_i(s) a_i
\]

\[
p(s) = u(s) \cdot v(s) - w(s) \quad \Rightarrow h(s) + t(s)
\]

Verifier checks

\[
e(g^{u(s)}, g^{v(s)})/e(g^{u(s)}, g^{v(s)}) \quad \Rightarrow e(g^{h(s)}, g^{t(s)})
\]

\[
e(g, g) \quad \Rightarrow e(g, g)
\]

\( u(s) \)
Remaining problem: Still need to check consistency of $g^-$, etc.

Step 4) Expanding CRS to include consistency checks.

Setup \((U,V,W)\):
Sample \(\xi, \alpha, \beta_u, \beta_v, \beta_w,\)

\[
\text{CRS} := g^- \text{ for each } \alpha.
\]

\[
\beta_u, \beta_v, \beta_w \leq \beta, \exists \alpha \leq \beta, \exists U, V, W, \exists U(s), \exists V(s), \exists W(s),
\]

\[
g^s, (\bar{g}^s): \text{like } h \text{ + pedro}
\]

Prover \((\text{CRS}, \bar{\alpha})\)

Compute \(p(x), h(x) = p(x)/t(x),\)

\[
\Pi := \left( g_{u(s)}, g_{v(s)}, g_{w(s)}, h(s),
\begin{array}{cccc}
\beta_{u(s)} & \alpha_u(s) & \alpha_v(s) & \alpha_w(s) & \beta_v(s) & \beta_w(s) & \beta_u(s)
\end{array}
\right)
\]

Verify:
- Check \(\alpha\) and \(\beta\) terms:
  - \(e(g_{u(s)}, g, \alpha) \rightleftharpoons e(g, g, \alpha)\)
    \hspace{1cm} \text{Same for } u, v, w\n  - \(e(g_{\beta_u(s)}, g) \rightleftharpoons e(g, g) \circ e(\beta_u(s), u(s)) \circ \cdots \circ e(\beta_u(s), u(s))\)
  - Finally \(e(g, g, g) \rightleftharpoons e(g, g, g) \circ e(g, g) \circ e(g, g)\)
- Normally remain.
  - How to make zero-knowledge.
  - Induce consistency for thwarting.