Bulletproofs

10.12.2019
Random self-reducibility of DL

- Let us have a cyclic group $G$ of size $p \in \mathbb{P}$
- Suppose that we have a machine $O$ that takes two elements of $G$ and outputs an element of $\mathbb{Z}_p$, such that

$$\Pr[g^x = h \mid g, h \leftarrow G, x \leftarrow O(g, h)] \geq 5\%$$

(probabilities over the choices of $g, h$, and the randomness used by $O$)

- Exercise. You are given some $g, h \in G$. You have access to $O$. Find $\log_g h$
Discrete Log Relations

- Fix $n$. Suppose that we have a machine $O$ that takes $n$ elements of $G$ and outputs $n$ elements of $\mathbb{Z}_p$, such that

$$\Pr \left[ g_1^{x_1} \cdots g_n^{x_n} = 1 \mid \exists i : x_i \neq 0 \right]$$

is non-negligible, where probabilities are over the choice of $g_1, \ldots, g_n$ and the randomness used by $O$.

- **Exercise.** You are given some $g, h \in G$. You have access to $O$. Find $\log_g h$.
Commitments to vectors

Pedersen commitments
- Group $\mathbb{G}$, size $p$, elements $g, h \in \mathbb{G}$ with unknown $\log g h$
- $\text{Com}(x; r) = g^x h^r$
- To open, give $x$ and $r$

Pedersen vector commitments
- Commitments to elements of $\mathbb{Z}_p^n$
- Elements $g_1, \ldots, g_n, h \in \mathbb{G}$ with no known non-trivial discrete log relations
- $\text{Com}(x_1, \ldots, x_n; r) = g_1^{x_1} \cdots g_n^{x_n} h^r$
- Opening: give $x_1, \ldots, x_n, r$
- Homomorphic (for operations on vectors)
Committing to a polynomial

Functionality

- $P$ becomes bound to a polynomial $f \in \mathbb{Z}_p[X]$
- $V$ picks a value $x \in X$
- $P$ gives $f(x)$ to $V$ and convinces him of its correctness

Implementation

A simple implementation is sufficient for us:

- $P$ commits to all coefficients of $f$, using Pedersen commitments
- $V$ sends $x$ to $P$
- Both compute commitment to $f(x)$, as the linear combination of commitments to coefficients
- $P$ opens $f(x)$ to $V$
Multi-round arguments

- We have a protocol, where $P$ and $V$ exchange many messages.
- Similarly to $\Sigma$-protocols:
  - $P$ sends the first and the last message.
  - Each time, $V$ reacts by generating a random value and sending it to $P$.
- ZK — given the instance and $V$’s challenges in all rounds, generate a transcript.
- Soundness: by rewinding many times at different places, extract the witness.
  - Total number of rewindings must be “small”.
  - The “fork” must have only a polynomial number of prongs.
- Fiat-Shamir heuristic is applicable.
Inner product argument

- Cyclic group $G$ of size $p \in \mathbb{P}$
- Public elements $g_1, \ldots, g_n, h_1, \ldots, h_n, P \in G$, $c \in \mathbb{Z}_p$
  - $g_1, \ldots, g_n, h_1, \ldots, h_n$ come from the CRS
  - No known non-trivial discrete log relations among all $g_i, h_i$
- $P$ wants to convince $V$ that he knows $a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathbb{Z}_p$, such that
  \[
  \prod_{i=1}^{n} g_i^{a_i} h_i^{b_i} = P \quad \text{and} \quad \sum_{i=1}^{n} a_i b_i = c
  \]

- Privacy is not important
- Can we be more efficient than $P$ just sending over all $a_i, b_i$?
Modified inner product argument

- Public elements $g_1, \ldots, g_n, h_1, \ldots, h_n, P, u \in G$
  - $g_1, \ldots, g_n, h_1, \ldots, h_n, u$ come from the CRS
  - No known non-trivial discrete log relations among $u$ and all $g_i, h_i$
- $P$ wants to convince $V$ that he knows $a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathbb{Z}_p$, such that
  \[ u \sum_{i=1}^n a_i b_i \cdot \prod_{i=1}^n g_i^{a_i} h_i^{b_i} = P \]
- Privacy is still not important
Reduction from modified to original argument

To make the original argument:

- $V$ picks a random $x \in \mathbb{Z}_p$, sends it to $P$;
- Run the modified protocol with

$$P \leftarrow P_{\text{orig}} \cdot u^{x \cdot c_{\text{orig}}}$$

$$u \leftarrow u_{\text{CRS}}^x$$

Exercise. Soundness. Assume you can extract witness from the modified protocol
The protocol

- Let $m = n/2$. $P$ computes and sends to $V$:

  $$L = u \sum_{i=1}^{m} a_i b_{i+m} \cdot \prod_{i=1}^{m} g_i^{a_i} h_i^{b_{i+m}}$$

  $$R = u \sum_{i=1}^{m} a_{i+m} b_i \cdot \prod_{i=1}^{m} g_i^{a_{i+m} h_i^{b_i}}$$

- $V$ sends random challenge $x \leftarrow Z_p$

- $P$ sends $a'_i = x a_i + x^{-1} a_{i+m}$ and $b'_i = x^{-1} b_i + x b_{i+m}$ to $V$ for $1 \leq i \leq m$

- $V$ checks

  $$L^x P R^{x^{-2}} \overset{?}= u \sum_{i=1}^{m} a'_i b'_i \cdot \prod_{i=1}^{m} g_i^{x^{-1} a'_i} g_i^{a'_i} g_{i+m} h_i^{xb'_i} h_i^{x^{-1} b'_i}$$

Exercise. Correctness?
Recursion

- $P$ has to convince $V$ that he knows $a'_i, b'_i$, such that

$$L^{x^2} PR^{x^{-2}} \overset{?}{=} u \sum_{i=1}^{m} a'_i b'_i \cdot \prod_{i=1}^{m} g_i^{-a'_i} x^{a'_i} g_{i+m} h_i x^{b'_i} h_{i+m}^{x^{-1} b'_i}$$

$$= u \sum_{i=1}^{m} a'_i b'_i \cdot \prod_{i=1}^{m} (g_i^{-a'_i} g_{i+m}^{x^{-1}})^{a'_i} (h_i^{x} h_{i+m}^{x^{-1}})^{b'_i}$$

- The same inner product argument, same $u$, changed $P$, new $g_i, h_i$, halved $n$
- Do $\log n$ steps, $P$ sends two elements of $\mathbb{G}$ at each step
Soundness

- Get a forked transcript

\[ L, R, x_I, \vec{a}'_I, \vec{b}'_I, x_{II}, \vec{a}'_{II}, \vec{b}'_{II}, x_{III}, \vec{a}'_{III}, \vec{b}'_{III}, x_{IV}, \vec{a}'_{IV}, \vec{b}'_{IV} \]

where \( x_I^2, x_{II}^2, x_{III}^2, x_{IV}^2 \) are all different

- They satisfy (for \( q \in \{I, II, III, IV\} \))

\[ L x_q^2 PR x_q^{-2} = u \sum_{i=1}^{m} a'_{q,i} b'_{q,i} \prod_{i=1}^{m} \left( g_i x_q^{-1} g_{i+m} \right)^{a'_{q,i}} \left( h_i x_q^{x_q^{-1}} h_{i+m} \right)^{b'_{q,i}} \]

- Let \( \nu_I, \nu_{II}, \nu_{III} \) satisfy

\[ \sum_{q=1}^{III} \nu_q x_q^2 = 1 \quad \sum_{q=1}^{III} \nu_q = 0 \quad \sum_{q=1}^{III} \nu_q x_q^{-2} = 0 \]
Linear combination gives...

\[
L = \prod_{q=1}^{III} L_{q}^{x_{q}^{2}} P_{q}^{\nu_{q}} R_{q}^{\nu_{q}x_{q}^{-2}} \\
= \prod_{q=1}^{III} \left( u \sum_{i=1}^{m} a'_{q,i} b'_{q,i} \right) \prod_{i=1}^{m} \left( g_{i}^{x_{q}^{-1}} g_{i+m}^{x_{q}} \right)^{a'_{q,i}} \left( h_{i}^{x_{q}} h_{i+m}^{x_{q}^{-1}} \right)^{b'_{q,i}} \\
= u \sum_{q=1}^{III} \left( \sum_{i=1}^{m} \nu_{q} a'_{q,i} b'_{q,i} \right) \prod_{i=1}^{m} g_{i}^{x_{q}^{-1}} a'_{q,i} h_{i}^{x_{q}} b'_{q,i} \prod_{i=1}^{m} g_{i+m}^{x_{q}} a'_{q,i} \left( \sum_{q=1}^{III} \nu_{q} b'_{q,i} \right) \left( \sum_{q=1}^{III} \nu_{q} x_{q}^{-1} b'_{q,i} \right) \\
= u^{c_{L}} \prod_{j=1}^{n} g_{j}^{a_{L,j}} h_{j}^{b_{L,j}}
\]
Representations of $L$, $R$, $P$

- If we let $\nu_1$, $\nu_{II}$, $\nu_{III}$ satisfy different systems of linear equations, we will also get

$$R = u^{c_R} \cdot \prod_{j=1}^{n} g_{j}^{a_{R,j}} h_{j}^{b_{R,j}}$$

$$P = u^{c_P} \cdot \prod_{j=1}^{n} g_{j}^{a_{P,j}} h_{j}^{b_{P,j}}$$

- The representation of $P$ almost looks like a witness
  - It would be a witness, if $c_P = \sum_{j=1}^{n} a_{P,j} b_{P,j}$
Verification equation again

$q$ ranges over $\{I, II, III, IV\}$

\[
\sum_{i=1}^{m} a'_{q,i} b'_{q,i} \cdot \prod_{i=1}^{m} g_{i}^{a'_{q,i} x_{q}^{-1}} h_{i}^{b'_{q,i} x_{q}} \prod_{i=1}^{m} g_{i+m}^{a'_{q,i} x_{q}} h_{i+m}^{b'_{q,i} x_{q}^{-1}} =
\]

\[
L_{q}^{x_{q}^{2}} PR_{q}^{x_{q}^{-2}} =
\]

\[
u^{c_{L} x_{q}^{2} + c_{P} + c_{R} x_{q}^{-2}} \prod_{j=1}^{n} g_{i}^{a_{L,j} x_{q}^{2} + a_{P,j} + a_{R,j} x_{q}^{-2}} h_{j}^{b_{L,j} x_{q}^{2} + b_{P,j} + b_{R,j} x_{q}^{-2}}
\]

The powers of $u$, $g_j$, $h_j$ have to be equal (or we have a non-trivial discrete log relation)
Equal exponents

\[ c_L x_q^2 + c_P + c_R x_q^{-2} = \sum_{i=1}^{m} a'_{q,i} b'_{q,i} \]
\[ a_L, i x_q^2 + a_P, i + a_R, i x_q^{-2} = a'_{q,i} x_q^{-1} \]
\[ a_L, i+m x_q^2 + a_P, i+m + a_R, i+m x_q^{-2} = a'_{q,i} x_q \]
\[ b_L, i x_q^2 + b_P, i + b_R, i x_q^{-2} = b'_{q,i} x_q \]
\[ b_L, i+m x_q^2 + b_P, i+m + b_R, i+m x_q^{-2} = b'_{q,i} x_q^{-1} \]

Take \( x_q \) times the 2nd/5th equation, \( x_q^{-1} \) times the 3rd/4th equation and subtract:

\[ a_{L,i} x_q^3 + (a_{P,i} - a_{L,i+m}) x_q + (a_{R,i} - a_{P,i+m}) x_q^{-1} - a_{R,i+m} x_q^{-3} = 0 \]
\[ b_{L,i+m} x_q^3 + (b_{P,i+m} - b_{L,i}) x_q + (b_{R,i+m} - b_{P,i}) x_q^{-1} - b_{R,i} x_q^{-3} = 0 \]

These must be zero polynomials
$\overrightarrow{a}_P, \overrightarrow{b}_P$ is the witness

\[ a'_{q,i} = a_{P,i}x_q + a_{P,i+m}x_q^{-1} \quad b'_{q,i} = b_{P,i}x_q^{-1} + b_{P,i+m}x_q \]

\[
\sum_{i=1}^{m} a'_{q,i}b'_{q,i} = \sum_{i=1}^{m} \left( a_{P,i}x_q + a_{P,i+m}x_q^{-1} \right) \left( b_{P,i}x_q^{-1} + b_{P,i+m}x_q \right)
\]

\[ = x_q^2 \sum_{i=1}^{m} a_{P,i}b_{P,i+m} + \sum_{j=1}^{n} a_{P,j}b_{P,j} + x_q^{-2} \sum_{i=1}^{m} a_{P,i+m}b_{P,i} \]

\[
\sum_{i=1}^{m} a'_{q,i}b'_{q,i} = c_L x_q^2 + c_P + c_R x_q^{-2}
\]

These polynomials have to be equal
Soundness of recursive protocol

- To get a witness of length $n$, we need four executions (and witnesses) of length $n/2$
- To get a witness of length $n/2$, we need four executions (and witnesses) of length $n/4$
- etc.
- To get a witness of length $n$, we need $4^\log_2 n \approx n^2$ executions
Representing arithmetic circuits

- There are \( n \) (binary) multiplication gates
  - \( i \)-th one has inputs \( a_{L,i} \) and \( a_{R,i} \), output \( a_{O,i} \)
  - These three values per multiplication gate are the witness
- There are \( Q \) affine relationships between \( a_{L,i} \), \( a_{R,i} \), \( a_{O,i} \)

\[
\sum_{i=1}^{n} w_{L,q,i} a_{L,i} + \sum_{i=1}^{n} w_{R,q,i} a_{R,i} + \sum_{i=1}^{n} w_{O,q,i} a_{O,i} = c_q
\]

\((1 \leq q \leq Q)\)
- All coefficients \( w_{?,q,i} \) and \( c_q \) are part of the instance
Start of the protocol

- CRS contains $g_1, \ldots, g_n, h_1, \ldots, h_n, h \in \mathbb{G}$
- $P$ picks $\alpha, \beta \leftarrow \mathbb{Z}_p$; computes and sends to $V$

$$A_I = h^{\alpha} \cdot \prod_{i=1}^{n} g_{i}^{a_{L,i}} h_{i}^{a_{R,i}}$$

$$A_O = h^{\beta} \cdot \prod_{i=1}^{n} g_{i}^{a_{O,i}}$$
Many equations to one

\[ a_{L,i}a_{R,i} - a_{O,i} = 0 \]

\[
\sum_{i=1}^{n} w_{L,q,i} a_{L,i} + \sum_{i=1}^{n} w_{R,q,i} a_{R,i} + \sum_{i=1}^{n} w_{O,q,i} a_{O,i} = c_q
\]

Turn it to a single polynomial equation (variables \(Y, Z\))

\[
\sum_{q=1}^{Q} \left( \sum_{i=1}^{n} w_{L,q,i} a_{L,i} + \sum_{i=1}^{n} w_{R,q,i} a_{R,i} + \sum_{i=1}^{n} w_{O,q,i} a_{O,i} \right) Z^q + \\
\sum_{i=1}^{n} (a_{L,i}a_{R,i} - a_{O,i}) Y^{i-1} = \sum_{q=1}^{Q} c_q Z^q
\]

\(\because\) \(V\) picks \(y, z \leftarrow \mathbb{Z}_p\), sends them to \(P\)
Arguments with polynomials...

- $P$ substitutes $y, z$ for $Y, Z$
- Define polynomials $\ell_i(X), r_i(X) \ (1 \leq i \leq n)$ so, that
  - (also define $t(X) = \sum_i \ell_i(X)r_i(X)$)
  - The coefficient of $X^2$ in $t(X)$ is the LHS of the equation on previous page (almost)
- For given $x \in \mathbb{Z}_p$, the verifier can compute something like
  $$h^{\text{smth}.} \cdot \prod_{i=1}^{n} g_i^{\ell_i(x)} h_i^{r_i(x)}$$
  (like a commitment)

- $P$ commits to $t(X)$. Shows, the coefficient of $X^2$ is $\approx \sum_q z^q c_q$
- $V$ challenges with $x \leftarrow \mathbb{Z}_p$
- $P$ opens $\ell_i(x), r_i(x)$ for all $i$
- $P$ also opens $t(x)$. $V$ checks that $t(x) = \sum_i \ell_i(x)r_i(x)$
The polynomials

\[ \ell_i(X) = a_{L,i}X + a_{O,i}X^2 + y^{-i+1} \left( \sum_{q=1}^{Q} w_{R,q,i} z^q \right) X \]

\[ r_i(X) = y^{-i} a_{R,i}X - y^{-i} + \left( \sum_{q=1}^{Q} w_{L,q,i} z^q \right) X + \left( \sum_{q=1}^{Q} w_{O,q,i} z^q \right) \]

Exercise. Compute coefficient of \( X^2 \) in \( t(X) \)
Committing to $t$ and opening

- $P$ commits to coefficients of $X$, $X^3$
- $V$ computes the commitment to the coefficient of $X^2$ himself
  - Using $h^0$ as the blinding factor
- $V$ sends the challenge $x$
- $P$ sends $t(x)$ to $V$, as well as the blinding exponent
  - Computed from the blinding exponents of the coefficients
Commitment to polynomials $\ell_i, r_i$

$$\ell_i(x) = a_{L,i}x + a_{O,i}x^2 + y^{-i+1} \left( \sum_{q=1}^{Q} w_{R,q,i}z^q \right) x$$

$$r_i(x) = y^{i-1}a_{R,i}x - y^{i-1} + \left( \sum_{q=1}^{Q} w_{L,q,i}z^q \right) x + \left( \sum_{q=1}^{Q} w_{O,q,i}z^q \right)$$

The commitment, computed by $V$, is

$$A_I^x \cdot A_O^{x^2} \cdot \prod_{i=1}^{n} g_i \quad y^{-i+1} \left( \sum_{q=1}^{Q} w_{R,q,i}z^q \right) x - y^{i-1} + \left( \sum_{q=1}^{Q} w_{L,q,i}z^q \right) x + \left( \sum_{q=1}^{Q} w_{O,q,i}z^q \right) \ldots$$

...but not quite...
Change the CRS

- Think of the CRS containing $h'_i = h_i^{y_i-1}$, instead of $h_i$
- Then $A_i^x$ contains $h'_i y_i^{-1} a_{R,i}$ as a factor
- The whole commitment $C$ is

$$A_1^x \cdot A_2^x \cdot \prod_{i=1}^{n} g_i \cdot y^{-i+1} \left( \sum_{q=1}^{Q} w_{R,q,i} z_q \right) x - y_i^{-1} + \left( \sum_{q=1}^{Q} w_{L,q,i} z_q \right) x + \left( \sum_{q=1}^{Q} w_{O,q,i} z_q \right)$$

- The blinding exponent of Pedersen’s commitment is $\alpha x + \beta x^2$
- $P$ opens $C$ as $\ell_1(x), r_1(x), \ldots, \ell_n(x), r_n(x)$
Blinding

- Problem: \( \ell_i(x), r_i(x), t(x) \) leak about \( a_{L,i}, a_{R,i}, a_{O,i} \)
- In the beginning, \( P \) also generates \( \vec{s}_L, \vec{s}_R \in \mathbb{Z}_p^n \)
- Commits to them:
  - Generates \( \rho \leftarrow \mathbb{Z}_p \)
  - Sends \( A_S = h^\rho \cdot \prod_{i=1}^n g_i^{s_{L,i}} h_i^{s_{R,i}} \) to \( V \), together with \( A_I \) and \( A_O \)
**Blinding of** $\ell_i$, $r_i$

\[
\ell_i(X) = a_{L,i}X + a_{O,i}X^2 + y^{-i+1} \left( \sum_{q=1}^{Q} w_{R,q,i}z^q \right) X \\
+ s_{L,i}X^3
\]

\[
r_i(X) = y^{i-1}a_{R,i}X - y^{i-1} + \left( \sum_{q=1}^{Q} w_{L,q,i}z^q \right) X + \left( \sum_{q=1}^{Q} w_{O,q,i}z^q \right) \\
+ y^{i-1}s_{R,i}X^3
\]
Changes to the construction, due to blinding

- Polynomial $t$: now has degree 6
  - No change to coefficient of $X^2$
- Commitment $C$ includes the factor $A_3^3$
  - ...and the blinding exponent adds $\rho x^3$