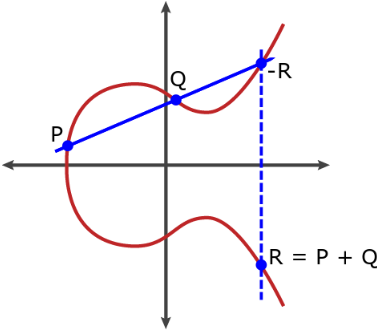
Group Based SNARKs

Carla Ràfols

September 2024

Universitat Pompeu Fabra Barcelona

Lectures 1,2,3



- $(\mathbb{G}, +)$ group of prime order p;
- (Algebraic) proof systems where DLOG problem is hard;

$$\mathsf{Pr}(x \leftarrow \mathcal{A}(\mathcal{P}, H) \wedge H = x\mathcal{P} \mid x \leftarrow \mathbb{Z}_p^*) \approx 0$$

- Lecture 1: techniques in groups without efficiently computable bilinear maps/pairings;
- Lecture 2: techniques in groups with efficiently computable pairings
- Lecture 3: Polynomial Commitments in pairing groups

Organization

- Commitments
- Bulletproofs
- Accumulators

Commitments

Algebraic Commitments

Pedersen Vector Commitments

$(\mathbb{G}, +)$ group of prime order p.

- $\mathsf{ck} \leftarrow \mathsf{Setup}(\mathbb{G}, n)$: sample $\mathsf{ck} = \vec{G} = (G_1, \ldots, G_n) \in \mathbb{G}^n$ from some distribution $\mathcal{D}_n$.
- $C \leftarrow \mathsf{Commit}(\mathsf{ck} \in \mathbb{G}^n, \vec{m} \in \mathbb{Z}_p^n)$:

$$\begin{cases} \mathsf{ck} = \vec{G} = (G_1, \ldots, G_n) \\ (m_1, \ldots, m_n) \in \mathbb{Z}_p^n \end{cases} \quad \longrightarrow \quad C = < \vec{m}, \vec{G} > = \sum_{i=1}^{n} m_i G_i$$

$(\mathbb{G}, +)$ group of prime order p.

- ck $\leftarrow$ Setup$(\mathbb{G}, n)$: sample ck $= \vec{G} = (G_1, \ldots, G_n) \in \mathbb{G}^n$ from some distribution $\mathcal{D}_n$.
- $C \leftarrow$ Commit(ck $\in \mathbb{G}^n, \vec{m} \in \mathbb{Z}_p^n$):

$$\begin{cases} \text{ck} = \vec{G} = (G_1, \ldots, G_n) \\ (m_1, \ldots, m_n) \in \mathbb{Z}_p^n \end{cases} \longrightarrow \quad C = <\vec{m}, \vec{G}> = \sum_{i=1}^{n} m_i G_i$$

Binding: If adversary finds one commitment and two valid openings $C, \vec{m}, \vec{m}'$ then:

$$\begin{cases} C = \sum_{i=1}^{n} m_i G_i \\ C = \sum_{i=1}^{n} m'_i G_i \end{cases} \implies \quad \mathcal{O} = <\vec{m} - \vec{m}', \vec{G}>$$

$(\mathbb{G}, +)$ group of prime order p.

- ck $\leftarrow$ Setup$(\mathbb{G}, n)$: sample ck $= \vec{G} = (G_1, \ldots, G_n) \in \mathbb{G}^n$ from some distribution $\mathcal{D}_n$.
- $C \leftarrow$ Commit(ck $\in \mathbb{G}^n, \vec{m} \in \mathbb{Z}_p^n$):

$$\begin{cases} \text{ck} = \vec{G} = (G_1, \ldots, G_n) \\ (m_1, \ldots, m_n) \in \mathbb{Z}_p^n \end{cases} \longrightarrow \quad C =< \vec{m}, \vec{G} >= \sum_{i=1}^{n} m_i G_i$$

Binding: If adversary finds one commitment and two valid openings $C, \vec{m}, \vec{m}'$ then:

$$\begin{cases} C = \sum_{i=1}^{n} m_i G_i \\ C = \sum_{i=1}^{n} m_i' G_i \end{cases} \implies \quad \mathcal{O} =< \vec{m} - \vec{m}', \vec{G} >$$

$\mathcal{D}_n$-FINDREP problem (also kernel problem, or discrete log relations):

$$\Pr\left(\vec{v} \leftarrow \mathcal{A}(\vec{G}) \wedge \mathcal{O} = \langle \vec{v}, \vec{G} \rangle \mid \vec{G} \leftarrow \mathcal{D}_n\right) \approx 0$$

Algebraic Commitments

$(\mathbb{G}, +)$ group of prime order p.

- **Example 1:** Uniform Key, transparent setup, $\mathcal{D}_n = \mathcal{U}_n$.

  ck $= \vec{G} = (G_1, \ldots, G_n)$, G_i uniformly and independently chosen from $\mathbb{G}$

  Binding Ex1: DLOG $\overset{tight}{\Longrightarrow} \mathcal{U}_n -$ FINDREP.

Algebraic Commitments

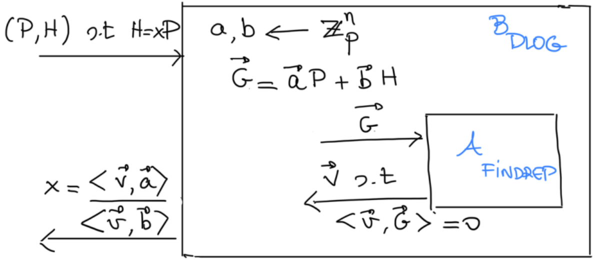
Pedersen Vector Commitments

$(\mathbb{G}, +)$ group of prime order p.

- **Example 1:** Uniform Key, transparent setup, $\mathcal{D}_n = \mathcal{U}_n$.

  ck $= \vec{G} = (G_1, \ldots, G_n)$, G_i uniformly and independently chosen from $\mathbb{G}$

  Binding Ex1: DLOG $\overset{tight}{\Longrightarrow} \mathcal{U}_n -$ FINDREP.



Proof: $0 = \langle \vec{v}, \vec{G} \rangle = \langle \vec{v}, \vec{a} \rangle P + \langle \vec{v}, \vec{b} \rangle H$

$\overset{(*)}{\Longrightarrow} \dfrac{\langle \vec{v}, \vec{a} \rangle}{\langle \vec{v}, \vec{b} \rangle} P = H.$

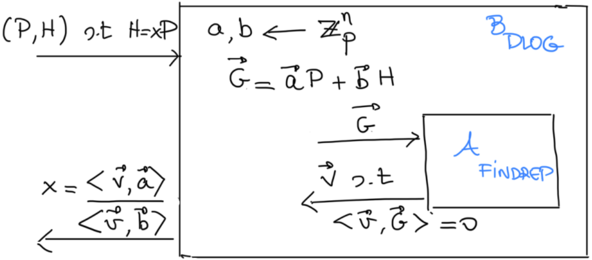
Algebraic Commitments

Pedersen Vector Commitments

- **Example 1:** Uniform Key, transparent setup, $\mathcal{D}_n = \mathcal{U}_n$.

  $\mathsf{ck} = \vec{G} = (G_1, \ldots, G_n)$, G_i uniformly and independently chosen from $\mathbb{G}$

  Binding Ex1: DLOG $\overset{tight}{\Longrightarrow}$ $\mathcal{U}_n$ − FINDREP.



Proof: $0 = \langle \vec{v}, \vec{G} \rangle = \langle \vec{v}, \vec{a} \rangle P + \langle \vec{v}, \vec{b} \rangle H$

$\overset{(*)}{\Longrightarrow} \frac{\langle \vec{v}, \vec{a} \rangle}{\langle \vec{v}, \vec{b} \rangle} P = H$

(*) except with probability $\frac{1}{|p|}$

Important Technique:
hide challenge information
theoretically in variables

Algebraic Commitments

Pedersen Vector Commitments

$(\mathbb{G}, +)$ group of prime order p.

- **Example 1:** Uniform Key, transparent setup, $\mathcal{D}_n = \mathcal{U}_n$.

  $\mathsf{ck} = \vec{G} = (G_1, \ldots, G_n)$, G_i uniformly and independently chosen from $\mathbb{G}$

  Binding Ex1: DLOG Assumption $\overset{tight}{\Longrightarrow} \mathcal{U}_n - \text{FINDREP}$ ($\Longleftarrow$ is trivial).

- **Example 2:** Structured Setup (powers of trapdoor)

  $$\mathsf{ck} = \vec{G} = (\mathcal{P}, x\mathcal{P}, \ldots, x^n\mathcal{P}), G_i = x^i G, x \leftarrow \mathbb{Z}_p$$

- **Example 3:** Structured Setup, $n = 2^\mu$ (multilinear monomials of μ variables)

  $$\mathsf{ck} = \vec{G} = (\mathcal{P}, x_1\mathcal{P}, x_2\mathcal{P}, \ldots, x_\mu\mathcal{P}, x_1x_2\mathcal{P}, \ldots, x_1x_2\ldots x_\mu\mathcal{P})$$

$(\mathbb{G}, +)$ group of prime order p.

- **Example 1:** Uniform Key, transparent setup, $\mathcal{D}_n = \mathcal{U}_n$.

  ck $= \vec{G} = (G_1, \ldots, G_n)$, G_i uniformly and independently chosen from $\mathbb{G}$

  Binding Ex1: DLOG Assumption $\overset{tight}{\Longrightarrow} \mathcal{U}_n -$ FINDREP ($\Longleftarrow$ is trivial).

- **Example 2:** Structured Setup (powers of trapdoor)

$$\text{ck} = \vec{G} = (\mathcal{P}, x\mathcal{P}, \ldots, x^n\mathcal{P}), G_i = x^i G, x \leftarrow \mathbb{Z}_p$$

- **Example 3:** Structured Setup, $n = 2^\mu$ (multilinear monomials of μ variables)

$$\text{ck} = \vec{G} = (\mathcal{P}, x_1\mathcal{P}, x_2\mathcal{P}, \ldots, x_\mu\mathcal{P}, x_1x_2\mathcal{P}, \ldots, x_1x_2\ldots x_\mu\mathcal{P})$$

  Binding Ex 2,3 : $n -$ DLOG $\overset{tight}{\Longrightarrow} \mathcal{D}_n -$ FINDREP.

$n -$ DLOG Assumption : $\quad \Pr\left(x \leftarrow \mathcal{A}(\mathcal{P}, x\mathcal{P}, \ldots, x^n\mathcal{P}) \mid x \leftarrow \mathbb{Z}_p^*\right) \approx 0$

$(\mathbb{G}, +)$ group of prime order p.

- **Example 1:** Uniform Key, transparent setup, $\mathcal{D}_n = \mathcal{U}_n$.

  ck $= \vec{G} = (G_1, \ldots, G_n)$, G_i uniformly and independently chosen from $\mathbb{G}$

- **Example 2:** Structured Setup (powers of trapdoor)

$$\text{ck} = \vec{G} = (\mathcal{P}, x\mathcal{P}, \ldots, x^n\mathcal{P}), G_i = x^i G, x \leftarrow \mathbb{Z}_p$$

- **Example 3:** Structured Setup, $n = 2^\mu$ (multilinear monomials of μ variables)

$$\text{ck} = \vec{G} = (\mathcal{P}, x_1\mathcal{P}, x_2\mathcal{P}, \ldots, x_\mu\mathcal{P}, x_1x_2\mathcal{P}, \ldots, x_1x_2\ldots x_\mu\mathcal{P})$$

1) Uniform Key: weaker assumptions!

$(\mathbb{G}, +)$ group of prime order p.

- **Example 1:** Uniform Key, transparent setup, $\mathcal{D}_n = \mathcal{U}_n$.

  ck $= \vec{G} = (G_1, \ldots, G_n)$, G_i uniformly and independently chosen from $\mathbb{G}$

- **Example 2:** Structured Setup (powers of trapdoor)

$$\text{ck} = \vec{G} = (\mathcal{P}, x\mathcal{P}, \ldots, x^n\mathcal{P}), G_i = x^i G, x \leftarrow \mathbb{Z}_p$$

- **Example 3:** Structured Setup, $n = 2^\mu$ (multilinear monomials of μ variables)

$$\text{ck} = \vec{G} = (\mathcal{P}, x_1\mathcal{P}, x_2\mathcal{P}, \ldots, x_\mu\mathcal{P}, x_1x_2\mathcal{P}, \ldots, x_1x_2\ldots x_\mu\mathcal{P})$$

1) Uniform Key: weaker assumptions!
2) Uniform Key: Trapdoors unknown to any party through oblivious sampling, $H : \{0,1\}^* \rightarrow \mathbb{G}$
3) Functionality ?

Bulletproofs

Bulletproofs

BP is an Inner Product Argument

- $(\mathbb{G}, +)$ group of prime order p. $\vec{G}, \vec{H} \in \mathbb{G}^n$ commitment keys;
- <u>Statement:</u>

$$\begin{cases} C \in \mathbb{G} \text{ is a commitment to } \vec{a} \text{ with key } \vec{G} \\ \text{ and} \\ D \in \mathbb{G} \text{ is a commitment to } \vec{b} \text{ with key } \vec{H} \\ \text{ and} \\ \sigma \in \mathbb{Z}_p \text{ is the inner product of committed values } \vec{a}, \vec{b}. \end{cases} \quad \textbf{i.e.} \quad \begin{cases} C = < \vec{a}, \vec{G} > \\ \text{ and} \\ D = < \vec{b}, \vec{H} > \\ \text{ and} \\ \sigma = < \vec{a}, \vec{b} > . \end{cases}$$

Witness: $\vec{a}, \vec{b}$.

Bulletproofs

BP is an Inner Product Argument

- $(\mathbb{G}, +)$ group of prime order p. $\vec{G}, \vec{H} \in \mathbb{G}^n$ commitment keys;
- Statement:

$$\begin{cases} C \in \mathbb{G} \text{ is a commitment to } \vec{a} \text{ with key } \vec{G} \\ \text{and} \\ D \in \mathbb{G} \text{ is a commitment to } \vec{b} \text{ with key } \vec{H} \\ \text{and} \\ \sigma \in \mathbb{Z}_p \text{ is the inner product of committed values } \vec{a}, \vec{b}. \end{cases} \quad \textbf{i.e.} \quad \begin{cases} C = < \vec{a}, \vec{G} > \\ \text{and} \\ D = < \vec{b}, \vec{H} > \\ \text{and} \\ \sigma = < \vec{a}, \vec{b} > . \end{cases}$$

  Witness: $\vec{a}, \vec{b}$.

- Recursive Strategy: Reduce to a randomized statement of half the size:

$$\begin{cases} C' = < \vec{a}', \vec{G}' > \\ \text{and} \\ D' = < \vec{b}', \vec{H}' > \\ \text{and} \\ \sigma' = < \vec{a}', \vec{b}' >, \end{cases}$$

  $\vec{a}', \vec{b}' \in \mathbb{Z}_p^{n/2}$, $\vec{G}', \vec{H}' \in \mathbb{G}_p^{n/2}$. Repeat until length 1, then open and check.

Bulletproofs Recursive Strategy I

Simple Facts

- **Simple Fact 1:** $\vec{a} = (\vec{a}_L, \vec{a}_R)$, $\vec{G} = (\vec{G}_L, \vec{G}_R)$,

$$C = < \vec{a}, \vec{G} > = < \vec{a}_L, \vec{G}_L > + < \vec{a}_R, \vec{G}_R > .$$

- **Simple Fact 1:** $\vec{a} = (\vec{a}_L, \vec{a}_R)$, $\vec{G} = (\vec{G}_L, \vec{G}_R)$,

$$C = <\vec{a}, \vec{G}> = <\vec{a}_L, \vec{G}_L> + <\vec{a}_R, \vec{G}_R> .$$

- **Simple Fact 2:** Let $\alpha \in \mathbb{R}$,

$$\text{If } \begin{cases} \vec{a}' = \vec{a}_L + \alpha \vec{a}_R \\ \vec{G}' = \vec{G}_L + \alpha^{-1} \vec{G}_R \end{cases} \quad \text{then } <\vec{a}', \vec{G}'> = C + \alpha C_{RL} + \alpha^{-1} C_{LR}$$

Proof:

$$<\vec{a}', \vec{G}'> = <\vec{a}_L, \vec{G}_L> + \alpha\alpha^{-1} <\vec{a}_R, \vec{G}_R> + \alpha <\vec{a}_R, \vec{G}_L> + \alpha^{-1} <\vec{a}_L, \vec{G}_R>$$

- **Simple Fact 1:** $\vec{a} = (\vec{a}_L, \vec{a}_R)$, $\vec{G} = (\vec{G}_L, \vec{G}_R)$,

$$C = <\vec{a}, \vec{G}> = <\vec{a}_L, \vec{G}_L> + <\vec{a}_R, \vec{G}_R>.$$

- **Simple Fact 2:** Let $\alpha \in \mathbb{R}$,

$$\text{If } \begin{cases} \vec{a}' = \vec{a}_L + \alpha \vec{a}_R \\ \vec{G}' = \vec{G}_L + \alpha^{-1} \vec{G}_R \end{cases} \quad \text{then } <\vec{a}', \vec{G}'> = C + \alpha C_{RL} + \alpha^{-1} C_{LR}$$

<u>Proof:</u>

$$<\vec{a}', \vec{G}'> = <\vec{a}_L, \vec{G}_L> + \alpha\alpha^{-1} <\vec{a}_R, \vec{G}_R> + \alpha <\vec{a}_R, \vec{G}_L> + \alpha^{-1} <\vec{a}_L, \vec{G}_R>$$

Bulletproofs Recursive Strategy I

Simple Facts

- **Simple Fact 1:** $\vec{a} = (\vec{a}_L, \vec{a}_R)$, $\vec{G} = (\vec{G}_L, \vec{G}_R)$,

$$C = <\vec{a}, \vec{G}> = <\vec{a}_L, \vec{G}_L> + <\vec{a}_R, \vec{G}_R> .$$

- **Simple Fact 2:** Let $\alpha \in \mathbb{R}$,

$$\text{If } \begin{cases} \vec{a}' = \vec{a}_L + \alpha \vec{a}_R \\ \vec{G}' = \vec{G}_L + \alpha^{-1} \vec{G}_R \end{cases} \quad \text{then } <\vec{a}', \vec{G}'> = C + \alpha C_{RL} + \alpha^{-1} C_{LR}$$

- **Simple Fact 3:** Let $\alpha \in \mathbb{R}$, $C = <\vec{a}, \vec{G}>$, $D = <\vec{H}, \vec{b}>$, $\sigma = <a, b>$.

$$\text{If } \begin{cases} \vec{a}' = \vec{a}_L + \alpha \vec{a}_R \\ \vec{H}' = \vec{H}_L' + \alpha \vec{H}_R \\ \vec{G}' = \vec{G}_L + \alpha^{-1} \vec{G}_R \\ \vec{b}' = \vec{b}_L + \alpha^{-1} \vec{b}_R \end{cases} \quad \text{then: } \begin{cases} <\vec{a}', \vec{G}'> = C + \alpha C_{RL} + \alpha^{-1} C_{LR} = \vec{C}' \\ <\vec{H}', \vec{b}'> = D + \alpha D_{RL} + \alpha^{-1} D_{LR} = \vec{D}' \\ <a', b'> = \sigma + \alpha \sigma_{RL} + \alpha^{-1} \sigma_{LR} = \sigma' \end{cases}$$

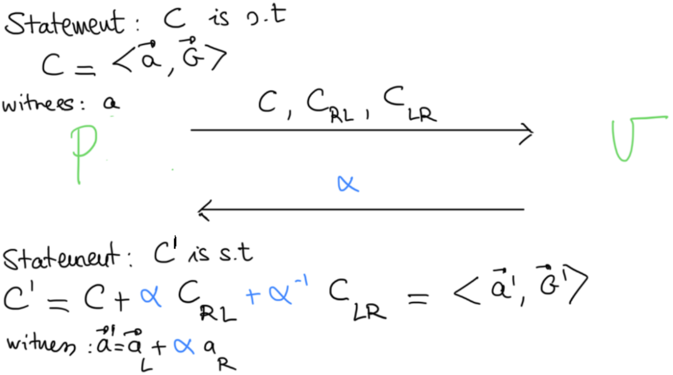
Bulletproofs Recursive Strategy II

Split and Combine: From Commitments Size n to Commitments size $n/2$

- **Simple Fact 2:** Let $\alpha \in \mathbb{R}$,

$$\text{If} \begin{cases} \vec{a}' = \vec{a}_L + \alpha \vec{a}_R \\ \vec{G}' = \vec{G}_L + \alpha^{-1} \vec{G}_R \end{cases} \quad \text{then} \quad < \vec{a}', \vec{G}' >= C + \alpha C_{RL} + \alpha^{-1} C_{LR}$$

Split and Combine Protocol:



Bulletproofs Full Protocol

$$C = \langle (a_0, a_1, a_2, a_3), (G_0, G_1, G_2, G_3) \rangle, \quad (a_0,a_1,a_2,a_3) \in \mathbb{Z}_p^4, \quad (G_0,G_1,G_2,G_3) \in \mathbb{G}^4$$

$$C_{LR} = \langle (a_0, a_1), (G_2, G_3) \rangle$$

$$C_{RL} = \langle (a_2, a_3), (G_0, G_1) \rangle$$

$$\xrightarrow{\quad C_{LR},\ C_{RL} \quad}$$

$$\vec{a}^{(1)} = \vec{a}_L + \alpha_1 \vec{a}_R \in \mathbb{Z}_p^2$$

$$\vec{G}^{(1)} = \vec{G}_L + \alpha_1^{-1} \vec{G}_R \in \mathbb{G}^2$$

$$\xleftarrow{\quad \alpha_1 \quad} \qquad C^{(1)} = C + \alpha_1 C_{RL} + \alpha_1^{-1} C_{LR}$$

$$C_{LR}^{(1)} = \langle a_0^{(1)}, G_1^{(1)} \rangle$$

$$C_{RL}^{(1)} = \langle a_1^{(1)}, G_0^{(1)} \rangle$$

$$\xrightarrow{\quad C_{LR}^{(1)},\ C_{RL}^{(1)} \quad}$$

$$\xleftarrow{\quad \alpha_2 \quad} \qquad C^{(2)} = C^{(1)} + \alpha_2 C_{RL}^{(1)} + \alpha_2^{-1} C_{LR}^{(1)}$$

$$\vec{a}^{(2)} = \vec{a}_L^{(1)} + \alpha_2 \vec{a}_R^{(1)} \in \mathbb{Z}_p$$

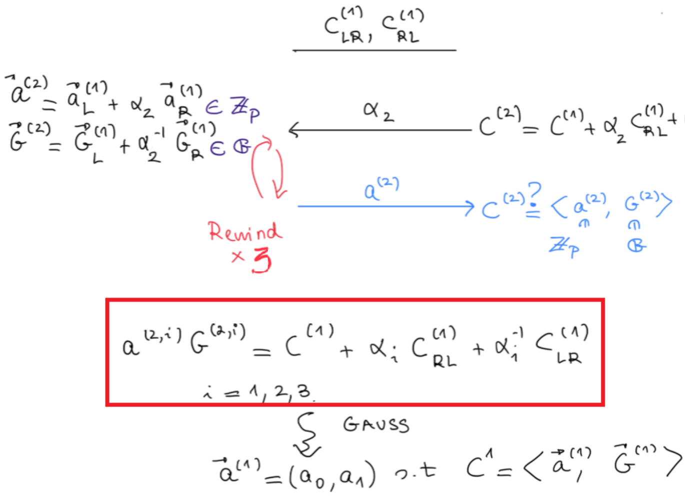
$$\vec{G}^{(2)} = \vec{G}_L^{(1)} + \alpha_2^{-1} \vec{G}_R^{(1)} \in \mathbb{G}$$

$$\xrightarrow{\quad a^{(2)},\ G^{(2)} \quad} \quad C^{(2)} \stackrel{?}{=} \langle a^{(2)}, G^{(2)} \rangle \wedge G^{(2)} \text{ is CORRECT}, \quad a^{(2)} \in \mathbb{Z}_p,\ G^{(2)} \in \mathbb{G}$$

Bulletproofs: Soundness

Algebraic Reductions of Knowledge

- Idea: if adversary knows opening for $C^{(i+1)}$ w.r.t to key $\vec{G}^{(i+1)}$, then it knows an opening for $C^{(i)}$ w.r.t to key $\vec{G}^{(i)}$.



Polynomial Commitments in DLOG Groups

Polynomial commitments from BP

- $C \leftarrow \mathsf{PolyCommit}(\mathsf{ck} \in \mathbb{G}^n, \vec{a} \in \mathbb{Z}_p^n)$:

$$\begin{cases} \mathsf{ck} = \vec{G} = (G_1, \ldots, G_n) \\ (a_1, \ldots, a_n) \in \mathbb{Z}_p^n \end{cases} \longrightarrow \qquad C = < \vec{a}, \vec{G} > = \sum_{i=1}^{n} a_i G_i$$

- $\pi, f(s) \leftarrow \mathsf{PolyCommitOpen}(\mathsf{ck} \in \mathbb{G}^n, \vec{c} \in \mathbb{Z}_p^n, s \in \mathbb{Z}_p)$: if $\vec{a}$ are the coefficients of polynomial $f(X)$, return $f(s)$, and short proof of correct opening π.

Polynomial commitments from BP

- $C \leftarrow \mathsf{PolyCommit}(\mathsf{ck} \in \mathbb{G}^n, \vec{a} \in \mathbb{Z}_p^n)$:

$$\begin{cases} \mathsf{ck} = \vec{G} = (G_1, \ldots, G_n) \\ (a_1, \ldots, a_n) \in \mathbb{Z}_p^n \end{cases} \longrightarrow \quad C = < \vec{a}, \vec{G} > = \sum_{i=1}^{n} a_i G_i$$

- $\pi, f(s) \leftarrow \mathsf{PolyCommitOpen}(\mathsf{ck} \in \mathbb{G}^n, \vec{c} \in \mathbb{Z}_p^n, s \in \mathbb{Z}_p)$: if $\vec{a}$ are the coefficients of polynomial $f(X)$, return $f(s)$, and short proof of correct opening π.

$$\begin{cases} C = \langle \vec{a}, \vec{G} \rangle \\ D = \langle \vec{H}, \vec{s} \rangle \\ f(s) = < \vec{a}, (1, s, s^2, \ldots, s^{n-1}) > \end{cases}$$

PolyCommitOpen Statement

Polynomial commitments from BP

- $C \leftarrow \text{PolyCommit}(\text{ck} \in \mathbb{G}^n, \vec{a} \in \mathbb{Z}_p^n)$:

$$\begin{cases} \text{ck} = \vec{G} = (G_1, \ldots, G_n) \\ (a_1, \ldots, a_n) \in \mathbb{Z}_p^n \end{cases} \longrightarrow \quad C =< \vec{a}, \vec{G} >= \sum_{i=1}^{n} a_i G_i$$

- $\pi, f(s) \leftarrow \text{PolyCommitOpen}(\text{ck} \in \mathbb{G}^n, \vec{c} \in \mathbb{Z}_p^n, s \in \mathbb{Z}_p)$: if $\vec{a}$ are the coefficients of polynomial $f(X)$, return $f(s)$,and short proof of correct opening π.

$$\begin{cases} C = \langle \vec{a}, \vec{G} \rangle \\ \sout{D = \langle \vec{H}, \vec{s} \rangle} \longrightarrow s \\ f(s) =< \vec{a}, (1, s, s^2, \ldots, s^{n-1}) > \end{cases}$$

PolyCommitOpen Statement

Bulletproofs: Efficiency

- Prover Complexity: $O(n)$
- Communication Complexity: $O(\log n)$.
- Verifier Complexity:

Bulletproofs: Efficiency

- Prover Complexity: $O(n)$
- Communication Complexity: $O(\log n)$.
- Verifier Complexity: $O(n)$

$$
\begin{aligned}
\vec{G} &= (G_0, G_1, G_2, G_3) \in \mathbb{G}^4 \\
\vec{G}^{(1)} &= (G_0 + \alpha_1^{-1} G_2, G_1 + \alpha_1^{-1} G_3) \in \mathbb{G}^2 \\
\vec{G}^{(2)} &= G_0 + \alpha_1^{-1} G_2 + \alpha_2^{-1} G_1 + \alpha_2^{-1}\alpha_1^{-1} G_3 \in \mathbb{G} \\
&= G_0 + \alpha_2^{-1} G_1 + \alpha_1^{-1} G_2 + \alpha_2^{-1}\alpha_1^{-1} G_3 \\
&= \langle \vec{G}, (1, \alpha_1^{-1}) \otimes (1, \alpha_2^{-1}) \rangle \\
&= \mathsf{PolyCommit}_{\vec{G}}(g)
\end{aligned}
$$

where $g(X) = (1 + \alpha_1^{-1} X^2)(1 + \alpha_2^{-1} X) = 1 + \alpha_2^{-1} X + \alpha_1^{-1} X^2 + \alpha_2^{-1}\alpha_1^{-1} X^3$.

Accumulators

Bulletproofs: Efficiency

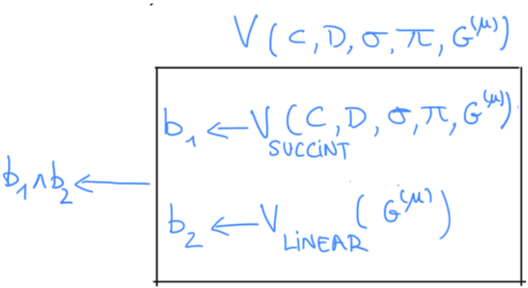
- Prover Complexity: $O(n)$
- Communication Complexity: $O(\log_2 n)$.
- Verifier Complexity: $O(n)$ IT'S A SAD, SAD, WORLD

More generally, if $n = 2^\mu$,

$$\vec{G}^{(\mu)} = \langle \vec{G}, \bigotimes (1, \alpha_i^{-1}) \rangle = \text{PolyCommit}_{\vec{G}}(\vec{c})$$

where $g(X) = \prod_{i=1}^{\mu} (1 + \alpha_{\mu+1-i}^{-1} X^{2^{i-1}})$.

Bulletproofs: Split Verifiers



- Except with probability d/p, if $s \leftarrow \mathbb{Z}_p$ is chosen independently of $G^{(\mu)}$,

$$G^{(\mu)} \text{ is correct } \iff G^{(\mu)} \text{ opens to } g(s) = \prod_{i=1}^{\mu} (1 + \alpha_{\mu+1-i}^{-1} s^{2^{i-1}})$$

Bulletproofs: Amortizing Linear Verifiers

(Atomic) Accumulator Intuition

- Suppose we want to prove a sequence of inner product statements...

CLAIM 1: $(C_1, D_1, \sigma_1) \in \mathcal{R}_{IP}$

PROOF 1: $\pi_1, G_1^{(\mu)}$

$$1 \stackrel{?}{=} V_{\text{SUCCINCT}}(C_1, D_1, \sigma_1, \pi_1, G_1^{(\mu)})$$

$$s_1 \leftarrow \mathbb{Z}_p$$

CLAIM 1': PolyCommit $(G_1^{(\mu)})$ opens to

$$g(s_1) = \prod (1 + \alpha_{\mu+1-i} \, s_1^{2^{i-1}})$$

CLAIM 2: $(C_2, D_2, \sigma_2) \in \mathcal{R}_{IP} \wedge (G_1^{(\mu)}, g(s_1)) \in \mathcal{R}_{PC}$

PROOF: $\pi_2, G_2^{(\mu)}$

⋮

Bulletproofs: Amortizing Linear Verifiers

(Atomic) Accumulator Intuition

- Suppose we want to prove a sequence of inner product statements...

CLAIM 1: $(C_1, D_1, \sigma_1) \in \mathcal{R}_{IP}$

PROOF 1: $\pi_1, G_1^{(\mu)}$

$$1 \stackrel{?}{=} V_{\text{SUCCINCT}}(C_1, D_1, \sigma_1, \pi_1, G_1^{(\mu)})$$

$$s_1 \leftarrow \mathbb{Z}_p$$

CLAIM 1': $\text{PolyCommit}(G_1^{(\mu)})$ opens to

$$g(s_1) = \prod (1 + \alpha_{\mu+1-i} \, s_1^{2^{i-1}})$$

CLAIM 2: $(C_2, D_2, \sigma_2) \in \mathcal{R}_{IP} \wedge (G_1^{(\mu)}, g(s_1)) \in \mathcal{R}_{PC}$

PROOF: $\pi_2, G_2^{(\mu)}$

⋮

The linear verification "delayed" or accumulated in a fresh running instance

References

1. J. Bootle, A.Cerulli, P. Chaidos, J.Groth, C.Petit: Efficient Zero-Knowledge Arguments for Arithmetic Circuits in the Discrete Log Setting. EUROCRYPT 2016.
2. B. Bünz, J. Bootle, D. Boneh, A. Poelstra, P. Wuille, G. Maxwell: Bulletproofs: Short Proofs for Confidential Transactions and More. IEEE Symposium on Security and Privacy 2018.
3. S. Bowe, J. Grigg, D. Hopwood: Halo: Recursive Proof Composition without a Trusted Setup. IACR Cryptol. ePrint Arch. 2019: 1021 (2019)
4. B. Bünz, A. Chiesa, P. Mishra, N. Spooner: Recursive Proof Composition from Accumulation Schemes. TCC (2) 2020: 1-18
5. J. Bootle, A. Chiesa, K. Sotiraki: Sumcheck Arguments and Their Applications. CRYPTO (1) 2021: 742-773