Benoît Libert
Zama

April 16, 2024

Vector Commitments with Proofs of Smallness: Short Range Proofs and More

PKC 2024 - Sydney

ZAMA

Outline

Vector Commitments: Applications and Prior Work

VC with Short Proofs of Smallness

- Building Block: Short Proof of Binarity

Applications

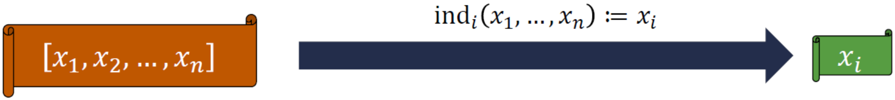
- Constant-size Range Proofs
- Short Proofs for RLWE Ciphertexts

Vector Commitments

Let a vector $(x_1, \ldots, x_n) \in R^n$ over a ring R. A commitment

$$C = Com(x_1, \ldots, x_n)$$

can be **concisely** opened to x_i for any $i \in [n]$



- $|C|$ and $|openings|$ should have size $O(\lambda \cdot \mathrm{polylog}(n))$
- **Applications:**
  - Zero-knowledge databases with short proofs (Catalano *et al.*, Eurocrypt'08; L.-Yung, TCC'10)
  - Verifiable data streaming [KSS+16], authenticated dictonaries [TXN20], cryptocurrencies [TAB+20], blockchain transactions [GRWZ20]

Prior Work on VCs (non-exhaustive)

- Folklore with $O(\log n)$-size openings via Merkle trees and CRHF
- Constructions with $O(1)$-size openings
  - From pairings and q-type assumptions (L.-Yung, TCC'10; Kate *et al.*, AC'10)
  - From CDH and hidden order groups (Catalano-Fiore, PKC'13; Boneh-Bünz-Fisch; Crypto'19)
  - From lattices (Peikert *et al.*, TCC'21; Albrecht *et al.*, Crypto'22; Wee-Wu, EC'23; ...,...)
- Over rings from compressed Σ-protocols (Attema *et al.*, TCC'22)
- Extensions
  - Functional commitments for linear functions (L.-Ramanna-Yung, ICALP'16) and beyond (de Castro-Peikert, EC'23; Wee-Wu, EC'23)
  - Subvector openings (Lai-Malavolta, Crypto'19)
  - Proof aggregation (Gorbunov et al., CCS'20; Campanelli *et al.*, AC'20)

Contributions: Short Proofs of Smallness for Committed Vectors

- Direct $O(1)$-size proofs that a committed $\vec{x} = (x_1, \ldots, x_n)$ is small:
  - $\vec{x} \in \{0, 1\}^n$ using 2 group elements
  - $\|\vec{x}\|_\infty \leq B$ using 3 group elements
  - $\|\vec{x}\|_2 \leq B$ using 6 group elements
  - $\vec{x}$ has small Hamming weight using 4 group elements
- **Applications:** short proofs (only 3 group elements) showing
  - (Batched) range membership: $\forall i \in [n] : x_i \in [-B_i, B_i]$
  - Validity of RLWE/FHE ciphertexts, plaintext (in)equalities, plaintext Hamming weight

Building Block: Short Proof of Binarity

Builds on vector commitments (L.-Yung, TCC'10):

- Uses a structured

$$crs = \left(g,\ \{g_i = g^{(\alpha^i)}\}_{i \in [2n] \setminus \{n+1\}},\ \{\hat{g}_i = \hat{g}^{(\alpha^i)}\}_{i \in [n]} \right)$$

- Commitment to $\vec{x} \in \mathbb{Z}_p^n$

$$C = g^{\gamma} \cdot \prod_{i=1}^{n} g_i^{x_i} = g^{\gamma + \sum_{i=1}^{n} x_i \cdot (\alpha^i)}$$

  is opened at position $i \in [n]$ by revealing $\pi_i \in \mathbb{G}$ s.t.

$$e(C, \hat{g}_{n+1-i}) = e(g_1, \hat{g}_n)^{x_i} \cdot e(\pi_i, \hat{g})$$

- Extends to prove $\langle \vec{x}, \vec{y} \rangle = z$ for public $\vec{y}, z \in \mathbb{Z}_p$

$$e(C, \prod_{i=1}^{n} \hat{g}_{n+1-i}^{y_i}) = e(g_1, \hat{g}_n)^{\langle \vec{x}, \vec{y} \rangle} \cdot e(\prod_{i=1}^{n} \pi_i^{y_i}, \hat{g})$$

Building Block: Short Proof of Binarity

Builds on vector commitments (L.-Yung, TCC'10):

- Uses a structured

$$crs = \Big(g,\ \{g_i = g^{(\alpha^i)}\}_{i \in [2n] \setminus \{n+1\}},\ \{\hat{g}_i = \hat{g}^{(\alpha^i)}\}_{i \in [n]} \Big)$$

- Commitment to $\vec{x} \in \mathbb{Z}_p^n$

$$C = g^{\gamma} \cdot \prod_{i=1}^{n} g_i^{x_i} = g^{\gamma + \sum_{i=1}^{n} x_i \cdot (\alpha^i)}$$

  is opened at position $i \in [n]$ by revealing $\pi_i \in \mathbb{G}$ s.t.

$$e(C, \hat{g}_{n+1-i}) = e(g_1, \hat{g}_n)^{x_i} \cdot e(\pi_i, \hat{g})$$

- Extends to prove $\langle \vec{x}, \vec{y} \rangle = z$ for public $\vec{y}, z \in \mathbb{Z}_p$

$$e\Big(C, \prod_{i=1}^{n} \hat{g}_{n+1-i}^{y_i}\Big) = e(g_1, \hat{g}_n)^{\langle \vec{x}, \vec{y} \rangle} \cdot e\Big(\prod_{i=1}^{n} \pi_i^{y_i}, \hat{g}\Big)$$

Short Proof of Binarity

- **Goal:** prove that $\hat{C} = \hat{g}^{\gamma + \sum_{i=1}^{n} x_i \cdot (\alpha^i)}$ commits to some $\vec{x} \in \{0,1\}^n$

- Prover shows that $\vec{y} = H(\hat{C}) \in \mathbb{Z}_p^n$ satisfies

$$\langle \vec{y} \circ (\vec{x} - \vec{1}), \vec{x} \rangle = \sum_{i=1}^{n} y_i \cdot \underbrace{x_i \cdot (x_i - 1)}_{=0} = 0$$

- **Idea:** Verifiably commit to $\vec{y} \circ \vec{x}$ (in reversed order) via

$$C_y = g^r \cdot \prod_{i=1}^{n} g_{n+1-i}^{x_i \cdot y_i} = g^{r + \sum_{i=1}^{n} x_i \cdot y_i \cdot (\alpha^{n+1-i})}$$

- Then, generate π_y s.t.

$$e\left(C_y \Big/ \prod_{i=1}^{n} g_{n+1-i}^{y_i}, \hat{C}\right) = e(g_1, \hat{g}_n)^{\overbrace{\langle \vec{y} \circ (\vec{x} - \vec{1}), \vec{x} \rangle}^{=0}} \cdot e(\pi_y, \hat{g})$$

Short Proof of Binarity

- **Goal:** prove that $\hat{C} = \hat{g}^{\gamma + \sum_{i=1}^{n} x_i \cdot (\alpha^i)}$ commits to some $\vec{x} \in \{0,1\}^n$
- Prover shows that $\vec{y} = H(\hat{C}) \in \mathbb{Z}_p^n$ satisfies

$$\langle \vec{y} \circ (\vec{x} - \vec{1}), \vec{x} \rangle = \sum_{i=1}^{n} y_i \cdot \underbrace{x_i \cdot (x_i - 1)}_{=0} = 0$$

- **Idea:** Verifiably commit to $\vec{y} \circ \vec{x}$ (in reversed order) via

$$C_y = g^r \cdot \prod_{i=1}^{n} g_{n+1-i}^{x_i \cdot y_i} = g^{r + \sum_{i=1}^{n} x_i \cdot y_i \cdot (\alpha^{n+1-i})}$$

- Then, generate π_y s.t.

$$e\left(C_y \Big/ \prod_{i=1}^{n} g_{n+1-i}^{y_i}, \hat{C}\right) = e(g_1, \hat{g}_n)^{\overbrace{\langle \vec{y} \circ (\vec{x} - \vec{1}), \vec{x} \rangle}^{=0}} \cdot e(\pi_y, \hat{g})$$

Short Proof of Binarity

- **Goal:** prove that $\hat{C} = \hat{g}^{\gamma + \sum_{i=1}^{n} x_i \cdot (\alpha^i)}$ commits to some $\vec{x} \in \{0,1\}^n$
- Prover shows that $\vec{y} = H(\hat{C}) \in \mathbb{Z}_p^n$ satisfies

$$\left\langle \vec{y} \circ (\vec{x} - \vec{1}), \vec{x} \right\rangle = \sum_{i=1}^{n} y_i \cdot \underbrace{x_i \cdot (x_i - 1)}_{=0} = 0$$

- **Idea:** Verifiably commit to $\vec{y} \circ \vec{x}$ (in reversed order) via

$$C_y = g^r \cdot \prod_{i=1}^{n} g_{n+1-i}^{x_i \cdot y_i} = g^{r + \sum_{i=1}^{n} x_i \cdot y_i \cdot (\alpha^{n+1-i})}$$

- Then, generate π_y s.t.

$$e\left(C_y \Big/ \prod_{i=1}^{n} g_{n+1-i}^{y_i}, \hat{C}\right) = e(g_1, \hat{g}_n)^{\overbrace{\langle \vec{y} \circ (\vec{x} - \vec{1}), \vec{x} \rangle}^{=0}} \cdot e(\pi_y, \hat{g})$$

Short Proof of Binarity

- **Final step:** prove that

$$C_y = g^r \cdot \prod_{i=1}^{n} g_{n+1-i}^{x_i \cdot y_i}$$

is really a commitment to the reversed $\vec{y} \circ \vec{x}$ where

$$\hat{C} = \hat{g}^\gamma \cdot \prod_{i=1}^{n} g_i^{x_i}$$

- Can be done using one element $\pi_{eq} \in \mathbb{G}$ using proof aggregation as in PointProofs (Gorbunov et al., CCS'20)

- Further aggregation compresses π_y, π_{eq} into one $\pi \in \mathbb{G}$;

Final proof of binarity consists of $(C_y, \pi) \in \mathbb{G}^2$

Application 1: Range proofs

Problem: Given a commitment $C = g^v \cdot h^r$ to $v \in \mathbb{Z}$, prove that $v \in [0, 2^\ell - 1]$

- Standard technique: prove that $\exists v_i \in \{0, 1\}$ s.t. $v = \sum_{i=1}^{\ell} v_i \cdot 2^{i-1}$ (proof size $O(\lambda \cdot \ell)$ in the standard approach)
- BulletProofs (Bünz *et al.*, IEEE S&P 2018): proof size $O(\lambda \cdot \log \ell)$
- Existing solution (Boneh *et al.*, `https://hackmd.io/@dabo/B1U4kx8XI`) with proof size $O(1)$ (i.e., $O(\lambda)$ bits) using polynomial commitments

New construction with shorter proofs

- Proofs (live in $\hat{\mathbb{G}} \times \mathbb{G}^2$) as short as in SNARKs
- Proof of simulation-extractability in the AGM+ROM

Application 1: Range proofs

Problem: Given a commitment $C = g^v \cdot h^r$ to $v \in \mathbb{Z}$, prove that $v \in [0, 2^\ell - 1]$

- Standard technique: prove that $\exists v_i \in \{0, 1\}$ s.t. $v = \sum_{i=1}^{\ell} v_i \cdot 2^{i-1}$ (proof size $O(\lambda \cdot \ell)$ in the standard approach)
- BulletProofs (Bünz *et al.*, `IEEE S&P 2018`): proof size $O(\lambda \cdot \log \ell)$
- Existing solution (Boneh *et al.*, `https://hackmd.io/@dabo/B1U4kx8XI`) with proof size $O(1)$ (i.e., $O(\lambda)$ bits) using polynomial commitments

New construction with shorter proofs

- Proofs (live in $\hat{\mathbb{G}} \times \mathbb{G}^2$) as short as in SNARKs
- Proof of simulation-extractability in the AGM+ROM

PKC 2024

Application 1: Range proofs

Problem: Given a commitment $C = g^v \cdot h^r$ to $v \in \mathbb{Z}$, prove that $v \in [0, 2^\ell - 1]$

- Standard technique: prove that $\exists v_i \in \{0,1\}$ s.t. $v = \sum_{i=1}^{\ell} v_i \cdot 2^{i-1}$ (proof size $O(\lambda \cdot \ell)$ in the standard approach)
- BulletProofs (Bünz *et al.*, `IEEE S&P 2018`): proof size $O(\lambda \cdot \log \ell)$
- Existing solution (Boneh *et al.*, `https://hackmd.io/@dabo/B1U4kx8XI`) with proof size $O(1)$ (i.e., $O(\lambda)$ bits) using polynomial commitments

New construction with shorter proofs

- Proofs (live in $\hat{\mathbb{G}} \times \mathbb{G}^2$) as short as in SNARKs
- Proof of simulation-extractability in the AGM+ROM

Range Proof: Intuition

Let a Pedersen commitment $\hat{C}_x = \hat{g}_1^x \cdot \hat{g}^r$ to $x \in [0, 2^\ell - 1]$,

- Let the binary representation $\vec{x} = (x_1, \ldots, x_\ell, 0, \ldots, 0)$ of x and compute

$$\hat{C} = \hat{g}^\gamma \cdot \prod_{i=1}^{\ell} \hat{g}_i^{x_i}$$

  with a proof of binarity (C_y, π_{bin})

- Prove knowledge of $x = \langle \vec{x}, (1, 2, \ldots, 2^{\ell-1}, \mathbf{0}^{n-\ell}) \rangle$, $\pi_x \in \mathbb{G}$ and $r \in \mathbb{Z}_p$ s.t.

$$e\Big(\prod_{i=1}^{\ell} g_{n+1-i}^{2^{i-1}}, \hat{C}\Big) = e(g_1, \hat{g}_n)^x \cdot e(\pi_x, \hat{g}) \quad \wedge \quad \hat{C}_x = \hat{g}_1^x \cdot \hat{g}^r$$

- Aggregating all π elements yields a proof $(\hat{C}, C_y, \pi)$ of 3 group elements

Range Proof: Intuition

Let a Pedersen commitment $\hat{C}_x = \hat{g}_1^x \cdot \hat{g}^r$ to $x \in [0, 2^\ell - 1]$,

- Let the binary representation $\vec{x} = (x_1, \ldots, x_\ell, 0, \ldots, 0)$ of x and compute

$$\hat{C} = \hat{g}^\gamma \cdot \prod_{i=1}^{\ell} \hat{g}_i^{x_i}$$

  with a proof of binarity (C_y, π_{bin})

- Prove knowledge of $x = \langle \vec{x}, (1, 2, \ldots, 2^{\ell-1}, \mathbf{0}^{n-\ell}) \rangle$, $\pi_x \in \mathbb{G}$ and $r \in \mathbb{Z}_p$ s.t.

$$e\Big(\prod_{i=1}^{\ell} g_{n+1-i}^{2^{i-1}}, \hat{C}\Big) = e(g_1, \hat{g}_n)^x \cdot e(\pi_x, \hat{g}) \qquad \wedge \qquad \hat{C}_x = \hat{g}_1^x \cdot \hat{g}^r$$

- Aggregating all π elements yields a proof $(\hat{C}, C_y, \pi)$ of 3 group elements

Range Proof: Security

Theorem

The scheme is **simulation-extractable** in the AGM+ROM under the $(2n, n)$-DLOG assumption: hardness of computing $\alpha \in \mathbb{Z}_p$ given

$$\left(g,\ \{g^{(\alpha^i)}\}_{i\in[2n]},\ \{\hat{g}^{(\alpha^i)}\}_{i\in[n]}\right)$$

- Reduction $\mathcal{B}$ simulates without using $g_{n+1} = g^{(\alpha^{n+1})}$

  $\Rightarrow$ AGM representation of $\mathcal{A}$'s proof $\pi^\star$ does not depend on g_{n+1}

- If extractor fails, $\mathcal{B}$ obtains another representation of $\pi^\star$ that *depends* on g_{n+1}

  $\Rightarrow$ reveals α as a root of a non-zero polynomial

- *Trapdoor-less* simulator programs random oracles as a function of previously-chosen aggregation coefficients

Range Proof: Comparisons

	CRS size	Proof size	Prover cost	Verifier cost
[BFGW20] + [KZG10]	$(4n+2) \times \lvert\mathbb{G}\rvert + 4 \times \lvert\hat{\mathbb{G}}\rvert$	$3 \times \lvert\mathbb{G}\rvert + 4 \times \lvert\mathbb{Z}_p\rvert$	$5n \exp_{\mathbb{G}}$	$3\mathrm{P} + 4\exp_{\hat{\mathbb{G}}}$
Groth16	$3\lvert\mathcal{C}\rvert \times \lvert\mathbb{G}\rvert$ $\lvert\mathcal{C}\rvert \times \lvert\hat{\mathbb{G}}\rvert$	$1 \times \lvert\hat{\mathbb{G}}\rvert + 2 \times \lvert\mathbb{G}\rvert$	$4\lvert\mathcal{C}\rvert \exp_{\mathbb{G}}$ $\lvert\mathcal{C}\rvert \exp_{\hat{\mathbb{G}}}$	$3\mathrm{P} + O(1)\exp_{\hat{\mathbb{G}}}$
New scheme	$2n \times \lvert\mathbb{G}\rvert$ $n \times \lvert\hat{\mathbb{G}}\rvert$	$1 \times \lvert\hat{\mathbb{G}}\rvert + 2 \times \lvert\mathbb{G}\rvert$	$3n \exp_{\mathbb{G}}$ $n \text{ mult}_{\hat{\mathbb{G}}}$	$4\mathrm{P} + 2n \exp_{\mathbb{G}}$ $n \exp_{\hat{\mathbb{G}}}$

Figure: Comparison among constant-size range proofs

- Groth16 and BFGW+KZG have $O(1)$ verification time
- We have the same proof size as Groth16 with the smallest prover cost

[BFGW20] D. Boneh, B. Fisch, A. Gabizon, Z. Williamson. *A simple range proof from polynomial commitments*. `https://hackmd.io/@dabo/B1U4kx8XI`

[KZG10] A. Kate, G. Zaverucha, I. Goldberg. *Constant-size commitments to polynomials and their applications*. Asiacrypt'10

Application 2: Lattice Statements

Problem: Let $R = \mathbb{Z}[X]/(X^d + 1)$ and $R_q = R/(qR)$ for a modulus q

For public $\vec{t}, \vec{a}_1, ..., \vec{a}_M \in R_q^N$, prove knowledge of $s_1, ..., s_M \in R$ s.t.

$$\sum_{i=1}^{M} \vec{a}_i \cdot s_i = \vec{t} \mod q$$

with $\|s_i\|_\infty \leq B_i \quad \forall i \in [M]$

- Allows proving (R)LWE relations (including validity of FHE ciphertexts)
- Can be handled in different ways:
  - MPC-in-the-head [IKOS07], Fiat-Shamir-with-Abort [Lyu09], Stern-like protocols [LNSW13]
  - In the discrete-log setting: via zk-SNARKs [Gro16] or directly [dLS19]

Short Proofs for RLWE Ciphertexts

Idea (del Pino-Lyubashevsky-Seiler; PKC'19): consider the statement over $\mathbb{Z}[X]/(X^d+1)$

$$\sum_{i=1}^{M} \vec{a}_i \cdot s_i = \underbrace{\vec{t}}_{\text{remainder}} + \underbrace{\vec{r}}_{\text{quotient}} \cdot q \mod (X^d+1)$$

with $\|s_i\|_\infty \leq B_i$ and $\|\vec{r}\|_\infty \leq \frac{d \cdot M}{2} \cdot \max_i (B_i)$

- Commit to $\big((s_1, \ldots, s_M) \mid \vec{r}\big)$ in a DLOG-hard group $\mathbb{G}$ of order $p \gg q$
- Prove that $\|s_i\|_\infty \ll p$ and $\|\vec{r}\|_\infty \ll p$
- Prove that

$$\sum_{i=1}^{M} \vec{a}_i \cdot s_i = \vec{t} + \vec{r} \cdot q \mod (p, X^d+1)$$

Short Proofs for RLWE Ciphertexts

- Rewrite the statement as a linear relation with binary witness

$$\underbrace{\left[\, \tilde{\mathbf{A}}_1 \;\; \ldots \;\; \tilde{\mathbf{A}}_M \;\middle|\; -q \cdot \left(\mathbf{I} \otimes (1,2,4,\ldots)\right) \right]}_{\triangleq\, \tilde{\mathbf{A}}} \cdot \underbrace{\begin{bmatrix} \vec{s}_1 \\ \vdots \\ \vec{s}_M \\ \hline \vec{r}_1 \\ \vdots \\ \vec{r}_N \end{bmatrix}}_{\triangleq\, \tilde{\mathbf{w}}} = \tilde{\mathbf{t}} \mod p, \tag{1}$$

- Prove that a committed $\tilde{\mathbf{w}} \in \{0,1\}^n$ is binary and satisfies (1)
- (1) is turned into an inner product relation $\langle \vec{\theta}^\top \cdot \tilde{\mathbf{A}}, \tilde{\mathbf{w}} \rangle = \vec{\theta}^\top \cdot \tilde{\mathbf{t}} \mod p$ for a random $\vec{\theta}$

  ($\vec{\theta}^\top \cdot \tilde{\mathbf{A}}$ computable in $O(d \cdot \log d)$ time when $\{\tilde{\mathbf{A}}_i\}_{i=1}^M$ are structured)

Short Proofs for RLWE Ciphertexts

- Aggregation yields a proof $(\hat{C}, C_y, \pi) \in \hat{\mathbb{G}} \times \mathbb{G}^2$ satisfying

$$e(\pi, \hat{g}) = e\Big(\underbrace{C_y{}^{\delta_y} \cdot \prod_{i=1}^{n} g_{n+1-i}^{(\delta_{eq}\cdot t_i - \delta_y)\cdot y_i + \delta_\theta \cdot \vec{a}_\theta[i]}}_{\triangleq\, C_h}, \hat{C}\Big) \cdot e\Big(C_y{}^{\delta_{eq}}, \underbrace{\prod_{i=1}^{n} \hat{g}_i^{t_i}}_{\triangleq\, \hat{C}_t}\Big)^{-1} \cdot e(g_1, \hat{g}_n)^{-t_\theta \cdot \delta_\theta},$$

- Verifier **V** computes $O(n)$ exponentiations where $n = |\tilde{\mathbf{w}}|$

- Tradeoff with $O(1)$ exponentiations for **V** and proofs in $(\hat{\mathbb{G}} \times \mathbb{G}^2)^2$:
  - Prover **P** computes C_h and $\hat{C}_t$ as KZG commitments
  - Then generates KZG evaluation proofs on a random point (cf. Schwartz-Zippel)

V only computes $2n$ field multiplications

Comparison with SNARKs

Proving validity of an [LPR10] ciphertext with $q \approx 2^{64}$ and $d = 1024$

- **Shortest SNARKs** (Groth; EC'16): weak simulation-extractability (AGM), arithmetic circuit with 150, 000 R1CS constraints
  - Structured CRS of 50116 KB
  - **P** computes $\approx 1,300,000$ exponentiations in $\mathbb{G}$ (assuming exponentiations in $\hat{\mathbb{G}}$ are 3x as expensive as in $\mathbb{G}$)
  - **V** computes ≈ 4096 exponentiations
- **New solution:** simulation-extractability in the AGM+ROM
  - Structured CRS of 25000 KB
  - **P** computes 900, 000 exponentiations in $\mathbb{G}$; **V** computes 8 exp. in $\mathbb{G}$
  - Can prove other statements without changing the CRS
  - Implem. on BLS12-381 curves for proving validity of (Joye, CT-RSA'24) with $n \approx 65000$: **P** runs in 3.9s (on laptop using 12 cores), **V** in 50ms

Summary

- Direct constructions of VC with concise proofs of smallness:
  - Binarity, low norm, or low Hamming weight
  - Security proofs in the AGM+ROM

- **Applications:**
  - Range proofs with $O(1)$-size proofs (3 group elements)
  - Short proofs for RLWE ciphertexts
    - Proofs made of 3 group elements, but $O(n)$ exponentiations to verify
    - Proofs containing 6 group elements, but $O(1)$ exponentiations to verify

  Under integration in Zama's fhEVM

Questions?