Succinct Vector Commitments from Lattices

5 April, 2023

Introduction

Outline

Formally defined by Dario Catalano and Dario Fiore [CF13].

Syntax:

- Setup$(1^\lambda, 1^\ell)$: Output crs.
- Commit$(\vec{x}, crs)$: Output commitment $\vec{c}$ to $\vec{x}$ and state st.
- Open$(crs, \vec{c}, \vec{x}, i)$: Output opening π_i at index i.
- Verify$(crs, \vec{c}, i, x_i, \pi)$: Check (x_i, π) is valid opening at index i.

Vector Commitment

Properties:

- Correctness. If $\vec{c} = Com(\vec{x}, crs)$ and $\pi = Open(crs, \vec{c}, \vec{x}, i)$ then $Verify(crs, \vec{c}, i, x_i, \pi) = 1$.
- Binding. Hard to find $x \neq x', \pi, \pi'$ s.t $Verify(crs, \vec{c}, i, x_i, \pi) = Verify(crs, \vec{c}, i, x_i', \pi') = 1$.
- Hiding. Commitments and openings do not reveal anything about the vector.

Outline

General Vector Commitment Framework

crs: $A_1, A_2, ..., A_\ell \in \mathbb{Z}_q^{m \times n}$ and $\vec{t}_1, \vec{t}_2, ..., \vec{t}_\ell \in \mathbb{Z}_q^n$ and $\{A_i^{-1}(\vec{t}_j)\}_{j \neq i}$.

Commit: For $\vec{x} = (x_1, x_2, ..., x_\ell)$, commitment is $\vec{c} = \sum_{i \in [\ell]} x_i \vec{t}_i$.

Opening at index i: A short vector $\vec{v}_i$ s.t $\vec{c} = A_i \vec{v}_i + x_i \vec{t}_i$

where $\vec{v}_i = \sum_{j \neq i} x_j A_i^{-1}(\vec{t}_j)$.

Verification: Check $\|\vec{v}_i\|$ is small and $\vec{c} = A_i \vec{v}_i + x_i \vec{t}_i$.

Outline

Previous Works and Current Contribution from Lattices

Previous works ([PPS21], [ACL$^+$22]):

- Can only commit $\vec{x} \in \{0, 1\}^\ell$.
- In addition, the hiding property of [PPS21] is not proven.

This work [WW22]:

- Can commit any $\vec{x} \in \mathbb{Z}_{\boldsymbol{q}}^\ell$.
- Hiding property is formally proven.

Preliminaries

Outline

SIS Assumption. Given $A \xleftarrow{\$} \mathbb{Z}_q^{m \times n}$, find $\vec{u} \in \mathbb{Z}_q^m$ s.t

$$\begin{cases} A\vec{u} = \vec{0}, \\ \|\vec{u}\| \text{ is small.} \end{cases}$$

ISIS Assumption. Given $A \xleftarrow{\$} \mathbb{Z}_q^{m \times n}$ and $\vec{t} \xleftarrow{\$} \mathbb{Z}_q^n$, find $\vec{u} \in \mathbb{Z}_q^m$ s.t

$$\begin{cases} A\vec{u} = \vec{t}, \\ \|\vec{u}\| \text{ is small.} \end{cases}$$

Outline

Gadget Matrices

For integers n and q,

$$G_n = I_n \otimes \vec{g}^T = \begin{bmatrix} \vec{g} & & & \\ & \vec{g} & & \\ & & \ddots & \\ & & & \vec{g} \end{bmatrix} \in \mathbb{Z}_q^{n \times m'} \text{ is the gadget matrix,}$$

where $\vec{g} = (1, 2, 4, ..., 2^{\lceil log(q) \rceil})$ and $m' = n(\lceil log(q) \rceil + 1)$.

Gadget Trapdoors

There are efficient algorithms with the following syntax [MP12]:

- TrapGen$(1^n, q, m)$: Output (A, R) s.t $AR = G$ and $\|R\|$ is small. The distribution of A is statistically close to the uniform distribution.
- SamplePre$(A, R, \vec{v}, s)$: Output $\vec{u}$ s.t $A\vec{u} = \vec{v}$. If $AR = G$, the distribution of $\vec{u}$ is statistically close to $A^{-1}(\vec{v})$.

Outline

The Basis-Augmented SIS (BASIS) Assumption

<u>Sample$(1^\lambda, A)$:</u>

Sample $i^* \xleftarrow{\$} [\ell], A_i \xleftarrow{\$} \mathbb{Z}_q^{(n+1)\times m}\ \forall i \neq i^*, \vec{a} \xleftarrow{\$} \mathbb{Z}_q^m$ and $A_{i^*} = \begin{bmatrix} \vec{a}^T \\ A \end{bmatrix}$.

Output $B = \begin{bmatrix} A_1 & & & & -G_{n+1} \\ & A_2 & & & -G_{n+1} \\ & & \ddots & & \vdots \\ & & & A_n & -G_{n+1} \end{bmatrix}$ and $aux = i^*$.

<u>BASIS Assumption:</u>

Given A, $B \leftarrow \text{Sample}(1^\lambda, A)$ and the trapdoor $T \leftarrow B^{-1}(G)$, the SIS problem w.r.t A is still hard to solve.

Succinct Vector Commitment from SIS

Intuition

From previous works for binary vectors:

For binding at position 1, expect $\vec{c} = x_1 \vec{t_1} + \vec{a_1}$ for public non-zero $\vec{t_1}$ and $\vec{a}_1$.

Suppose there are $\vec{a}_1, \vec{a}'_1$ s.t $\vec{c} = 1 \cdot \vec{t_1} + \vec{a_1} = 0 \cdot \vec{t_1} + \vec{a}'_1$. Then, we have $\vec{t_1} = \vec{a}'_1 - \vec{a}_1$.

If $\vec{a_1} = A_1 \vec{v_1}$ and $\vec{a}'_1 = A_1 \vec{v}'_1$ for some vector $\vec{v_1}$ and $\vec{v}'_1$, then we have $\vec{t_1} = A_1(\vec{v}'_1 - \vec{v}_1)$.

Restricting $\vec{v_1}$ and $\vec{v}'_1$ to have small norm, then we have the ISIS solution, which is hard to find.

Intuition

Replacing $\vec{t}_1$ with $\vec{e}_1 = (1, 0, ..., 0)$, then $(x_1 - x_1')\vec{e}_1 = A_1(\vec{v}_1 - \vec{v}_1')$. This becomes the SIS problem by removing the first row of A

$\Rightarrow$ Can commit for any $\vec{x} \in \mathbb{Z}_q^\ell$.

Generalizing for all i, we require $\vec{c} = x_i\vec{e}_1 + A_i\vec{v}_i$ for all $i \in [\ell]$.

In their work, the authors want $\vec{c} = G\vec{c}'$ where $\vec{c}'$ has small norm for security analysis.

These relations can be expressed by a linear system:

$$\begin{bmatrix} A_1 & & & & -G \\ & A_2 & & & -G \\ & & \ddots & & \vdots \\ & & & A_\ell & -G \end{bmatrix} \cdot \begin{bmatrix} \vec{v}_1 \\ \vec{v}_2 \\ \vdots \\ \vec{v}_\ell \\ \vec{c}' \end{bmatrix} = \begin{bmatrix} -x_1\vec{e}_1 \\ -x_2\vec{e}_1 \\ \vdots \\ -x_\ell\vec{e}_1 \end{bmatrix} \qquad (1)$$

Intuition

To commit $\vec{x} = (x_1, x_2, ..., x_\ell)$, let $B_\ell = \begin{bmatrix} A_1 & & & & -G \\ & A_2 & & & -G \\ & & \ddots & & \vdots \\ & & & A_\ell & -G \end{bmatrix}$.

Sample a vector $\begin{bmatrix} \vec{v}_1 \\ \vec{v}_2 \\ \vdots \\ \vec{v}_\ell \\ \vec{c}' \end{bmatrix}$ of small norm that satisfies (1).

This yields a commitment $\vec{c} = G\vec{c}'$ and openings $\vec{v}_1, \vec{v}_2, ..., \vec{v}_\ell$.

Vector Commitment from SIS

<u>$\text{Setup}(1^\lambda, 1^\ell)$:</u>

Sample $(A_i, R_i) \leftarrow \text{TrapGen}(1^\lambda, q, m)$ for all $i \in [\ell]$.

$$\text{Let } B = \begin{bmatrix} A_1 & & & & -G \\ & A_2 & & & -G \\ & & \ddots & & \vdots \\ & & & A_\ell & -G \end{bmatrix} \in \mathbb{Z}_q^{n\ell \times (\ell m + m')}$$

$$\text{and } R = \begin{bmatrix} \text{diag}(R_1, R_2, \ldots, R_\ell) \\ 0^{m' \times \ell m'} \end{bmatrix} \in \mathbb{Z}_q^{(\ell m + m') \times \ell m'}$$

Sample $T \leftarrow \mathit{SamplePre}(B_\ell, R, G_{n\ell}, s_0)$.

Output $\mathit{crs} = (A_1, A_2, \ldots, A_\ell, T)$.

Vector Commitment from SIS

$\underline{\mathrm{Com}(\vec{x}, crs = (A_1, A_2, \ldots, A_\ell, T)) :}$

$$\text{Sample } \begin{bmatrix} \vec{v}_1 \\ \vec{v}_2 \\ \vdots \\ \vec{v}_\ell \\ \vec{c}' \end{bmatrix} = \mathrm{SamplePre}(B_\ell, T, -\vec{x} \otimes \vec{e}_1, s_1)$$

where $\vec{e}_1 = (1, 0, ..., 0) \in \mathbb{Z}_q^\ell$.

Output commitment $\vec{c} = G\vec{c}' \in \mathbb{Z}_q^n$ and state $st = (\vec{v}_1, \vec{v}_2, ..., \vec{v}_\ell)$.

$\underline{\mathrm{Open}(crs, \vec{c}, \vec{x}, i) :}$ Output $\vec{v}_i$.

$\underline{\mathrm{Verify}(crs, \vec{c}, i, x_i, \pi) :}$ Check $\|\vec{v}_i\| \leq B$ and $\vec{c} = A_i\vec{v}_i + x_i e_1$

Outline

Linear Homomorphism

For $\vec{x}$ and $\vec{x}'$ with commitments $\vec{c}$ and $\vec{c}'$, observe that for all i:

$$\vec{c} + \vec{c}' = A_i(\vec{v}_i + \vec{v}_i') + (x_i + x_i')e_1.$$

Thus, the commitment to $\vec{x} + \vec{x}'$ is equal to $\vec{c} + \vec{c}'$, and the opening at index i is equal to $\vec{v}_i + \vec{v}_i'$.

Notice that the norm of the openings is increased (from B to $2B$).

$\Rightarrow$ Can only support a bounded number of additions.

Updatability

Given $(\vec{x}, \vec{c})$, suppose we want to update to $(\vec{x}', \vec{c}')$ s.t $\vec{x}'$ differ from $\vec{x}$ at exactly one position i.

Let $\vec{x}^* = \vec{x}' - \vec{x}$ and $\vec{c}^*$ be the commitment to $\vec{x}^*$, then $\vec{c} + \vec{c}^*$ is the commitment to $\vec{x}'$ and $\vec{v}_i + \vec{v}_i^*$ is the opening at position i of $\vec{x}'$.

We know that $\vec{x}^* = (0, 0, ..., x_i' - x_i, 0, .., 0)$.

Hence, the update step can be done without knowing the other positions of $\vec{x}$.

Once again, because of norm bound, we can only update a bounded number of times.

Outline

Application: Verkle Tree

Verkle Tree

- Introduced by John Kuszmaul [Kus18].
- Use commitment scheme instead of hashing.
- Recommended using KZG by Vitalik [But21].
  $\Rightarrow$ Not quantum secure.

Application: Verkle Tree

Idea worth trying: Replacing KZG with a lattice-based vector commitment for post-quantum security.

Limitations: Many restrictions for lattice based construction,

e.g., bounded norm forbids many updates,...

Thank You

[ACL+22] Martin R. Albrecht, Valerio Cini, Russell W. F. Lai, Giulio Malavolta, and Sri Aravinda Krishnan Thyagarajan.
Lattice-based snarks: Publicly verifiable, preprocessing, and recursively composable - (extended abstract).
In Yevgeniy Dodis and Thomas Shrimpton, editors, *Advances in Cryptology - CRYPTO 2022 - 42nd Annual International Cryptology Conference, CRYPTO 2022, Santa Barbara, CA, USA, August 15-18, 2022, Proceedings, Part II*, volume 13508 of *Lecture Notes in Computer Science*, pages 102–132. Springer, 2022.

[But21] Vitalik Buterin.
Verkle trees, 2021.

[CF13] Dario Catalano and Dario Fiore.
Vector commitments and their applications.
In Kaoru Kurosawa and Goichiro Hanaoka, editors, *Public-Key Cryptography - PKC 2013 - 16th International Conference on Practice and Theory in Public-Key Cryptography, Nara, Japan, February 26 - March 1, 2013. Proceedings*, volume 7778 of *Lecture Notes in Computer Science*, pages 55–72. Springer, 2013.

[Kus18] John Kuszmaul.
Verkle trees, 2018.

[MP12] Daniele Micciancio and Chris Peikert.
Trapdoors for lattices: Simpler, tighter, faster, smaller.
In David Pointcheval and Thomas Johansson, editors, *Advances in Cryptology - EUROCRYPT 2012 - 31st Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cambridge, UK, April 15-19, 2012. Proceedings*, volume 7237 of *Lecture Notes in Computer Science*, pages 700–718. Springer, 2012.

[PPS21] Chris Peikert, Zachary Pepin, and Chad Sharp.
Vector and functional commitments from lattices.
In Kobbi Nissim and Brent Waters, editors, *Theory of Cryptography - 19th International Conference, TCC 2021, Raleigh, NC, USA, November 8-11, 2021, Proceedings, Part III*, volume 13044 of *Lecture Notes in Computer Science*, pages 480–511. Springer, 2021.

[WW22] Hoeteck Wee and David J. Wu.
Succinct vector, polynomial, and functional commitments from lattices.
IACR Cryptol. ePrint Arch., page 1515, 2022.