Zero-Knowledge Proofs for Committed Symmetric Boolean Functions

SAN LING, **KHOA NGUYEN**, **DUONG HIEU PHAN**, **HANH TANG** AND **HUAXIONG WANG**

NANYANG TECHNOLOGICAL UNIVERSITY, SINGAPORE

LTCI, TELECOM PARIS, INSTITUT POLYTECHNIQUE DE PARIS, FRANCE

Overview

- Introduction
- Backgrounds
- Technique for Evaluating Symmetric Boolean Functions in Zero-Knowledge
- Zero-Knowledge Proof for Symmetric Boolean Functions

Introduction

Previous Works and Motivation

- Previous works. Most existing works focus on ZKP for correct evaluation of **private input** (encrypted or committed) from a **publicly known function**.
- Our setting. ZKP for correct evaluation of **private symmetric Boolean functions** on **private inputs**.
- Possible applications. Policy-based anonymous authentication, privacy-preserving access controls for encrypted databases, accountable function evaluations, …

Symmetric Boolean Functions

- An n-ary symmetric Boolean function $f: \{0,1\}^n \to \{0,1\}$ is represented by

$$\boldsymbol{v} = \boldsymbol{v}(f) = (v_0, v_1, \dots, v_n) \in \{0,1\}^{n+1}.$$

- On input $\boldsymbol{x} \in \{0,1\}^n$, $f(\boldsymbol{x})$ returns v_w where $w = \mathrm{weight}(\boldsymbol{x})$.
- 2^{n+1} different symmetric Boolean functions.
- Examples.

1. Threshold functions: $\mathrm{T}_k(\boldsymbol{x}) = 1 \Leftrightarrow \mathrm{weight}(\boldsymbol{x}) \geq k$.
2. Parity functions: $\mathrm{PAR}(\boldsymbol{x}) = 1 \Leftrightarrow \mathrm{weight}(\boldsymbol{x})$ is odd.
3. Sorting functions: $\mathrm{SORT}(\boldsymbol{x}) = \left(T_1(\boldsymbol{x}), T_2(\boldsymbol{x}), \dots, T_n(\boldsymbol{x})\right)$.

Problem Statement

- Given a public bit b and commitments to $\boldsymbol{x} \in \{0,1\}^n$ and f as follows:

$$\boldsymbol{c}_x = \mathrm{Com}_{ck}(\boldsymbol{x}; \rho_x) \text{ and } \boldsymbol{c}_f = \mathrm{Com}_{ck}\big(\boldsymbol{v}(f); \rho_f\big).$$

- Construct ZK proof for knowledge of $\boldsymbol{x}$ and $\boldsymbol{v}(f)$ such that $f(\boldsymbol{x}) = b$.
- Common inputs. $ck, \boldsymbol{c}_x, \boldsymbol{c}_f$ and b.
- Prover's inputs. $\boldsymbol{x}, \boldsymbol{v}(f)$, commitment randomness ρ_x, ρ_f.
- Relation

$$R_{\mathrm{sym}} = \big\{\big(ck, \boldsymbol{c}_x, \boldsymbol{c}_f, b\big); \boldsymbol{x}, \boldsymbol{v}(f), \rho_x, \rho_f \ : \ \boldsymbol{c}_x = \mathrm{Com}_{ck}(\boldsymbol{x}; \rho_x), \boldsymbol{c}_f = \mathrm{Com}_{ck}\big(\boldsymbol{v}(f); \rho_f\big), f(\boldsymbol{x}) = b\big\}.$$

Backgrounds

LPN-Based Commitments [JKPT12]

- n: the bit-length of message.
- Commitment key $(\boldsymbol{A}_{1,x}, \boldsymbol{A}_2) \in \{0,1\}^{\kappa \times n} \times \{0,1\}^{\kappa \times s}$.
- To commit n-bit message $\boldsymbol{x}$, compute

$$\boldsymbol{c}_x = \boldsymbol{A}_{1,x} \cdot \boldsymbol{x} \oplus \boldsymbol{A}_2 \cdot \boldsymbol{s}_x \oplus \boldsymbol{e}_x$$

where $\boldsymbol{s}_x \xleftarrow{\$} \{0,1\}^s$ and $\boldsymbol{e}_x$ is sampled from appropriate Bernoulli distribution.

- Similarly, to commit $(n+1)$-bit vector $\boldsymbol{v} = \boldsymbol{v}(f)$, use commitment key $\left(\boldsymbol{A}_{1,f}, \boldsymbol{A}_2\right)$ and compute

$$\boldsymbol{c}_f = \boldsymbol{A}_{1,f} \cdot \boldsymbol{v} \oplus \boldsymbol{A}_2 \cdot \boldsymbol{s}_f \oplus \boldsymbol{e}_f.$$

Stern-Like Σ-Protocol [LLMNW16]

- Stern-like Σ-protocol aims to show the knowledge of secret vector $\boldsymbol{w} = (\boldsymbol{w}_1 \| \boldsymbol{w}_2)$ satisfying

$$\boldsymbol{M}_1 \cdot \boldsymbol{w}_1 \oplus \boldsymbol{M}_2 \cdot \boldsymbol{w}_2 = \boldsymbol{u} \qquad \text{and} \qquad \boldsymbol{w}_1 \in \mathrm{VALID}$$

for some public matrices $\boldsymbol{M}_1, \boldsymbol{M}_2$, public vector $\boldsymbol{u}$ and set VALID containing $\boldsymbol{w}_1$.

- Relation

$$R_{\text{abstract}} = \{(\boldsymbol{M}_1, \boldsymbol{M}_2, \boldsymbol{u}); \boldsymbol{w}_1, \boldsymbol{w}_2 \ : \ \boldsymbol{M}_1 \cdot \boldsymbol{w}_1 \oplus \boldsymbol{M}_2 \cdot \boldsymbol{w}_2 = \boldsymbol{u} \wedge \boldsymbol{w}_1 \in \mathrm{VALID}\}$$

- Stern-like ZK Proof of Knowledge is constructable if there exists a set of permutations S satisfying

$$\begin{cases} \forall \varphi \in S: \boldsymbol{w} \in \mathrm{VALID} \Leftrightarrow \varphi(\boldsymbol{w}) \in \mathrm{VALID} \\ \text{If } \boldsymbol{w} \in \mathrm{VALID} \text{ and } \varphi \text{ is uniform in } S, \text{then } \varphi(\boldsymbol{w}) \text{ is uniform in } \mathrm{VALID}. \end{cases}$$

- Purpose. Reduce R_{sym} to R_{abstract}.

Recall. Stern-Like Technique for Valid Openings of LPN-Based Commitments

- Recall. $\boldsymbol{c}_x = \boldsymbol{A}_{1,x} \cdot \boldsymbol{x} \oplus \boldsymbol{A}_2 \cdot \boldsymbol{s}_x \oplus \boldsymbol{e}_x$ where $\boldsymbol{s}_x \xleftarrow{\$} \{0,1\}^s$ and $\boldsymbol{e}_x \in \{0,1\}^\kappa$ is sampled from appropriate Bernoulli distribution.
- With overwhelming probability, $\text{weight}(\boldsymbol{e}_x) \le t$ for some t.
- Extend $\boldsymbol{e}_x$ to $(\boldsymbol{e}_x \| \boldsymbol{e}'_x) \in \{0,1\}^{\kappa+t}$, where $\boldsymbol{e}'_x \in \{0,1\}^t$ such that $\text{weight}(\boldsymbol{e}_x \| \boldsymbol{e}'_x) = t$.
- Fact. $\text{weight}(\boldsymbol{e}_x) \le t \Leftrightarrow \exists \boldsymbol{e}'_x \in \{0,1\}^t$ s.t $\text{weight}(\boldsymbol{e}_x \| \boldsymbol{e}'_x) = t$.

$$\boldsymbol{c}_x = [\boldsymbol{I}_\kappa | \boldsymbol{0}^{\kappa \times t}] \cdot (\boldsymbol{e}_x \| \boldsymbol{e}'_x) \oplus [\boldsymbol{A}_{1,x} | \boldsymbol{A}_2] \cdot (\boldsymbol{x} \| \boldsymbol{s}_x) \text{ and } \text{weight}(\boldsymbol{e}_x \| \boldsymbol{e}'_x) = t.$$

- Define $\text{VALID}_{\text{LPN}} = \{\boldsymbol{w} \in \{0,1\}^{\kappa+t} \colon \text{weight}(\boldsymbol{w}) = t\}$.
- Reducible to R_{abstract} by defining set of permutations to be symmetric group over $\kappa + t$ elements.

Technique for Evaluating Symmetric Boolean Functions in ZK

ZKP for Symmetric Boolean Functions

- Prover needs to convince verifier that

$$\begin{cases} \boldsymbol{c}_x = \boldsymbol{A}_{1,x} \cdot \boldsymbol{x} \oplus \boldsymbol{A}_2 \cdot \boldsymbol{s}_x \oplus \boldsymbol{e}_x, \\ \boldsymbol{c}_f = \boldsymbol{A}_{1,f} \cdot \boldsymbol{v} \oplus \boldsymbol{A}_2 \cdot \boldsymbol{s}_f \oplus \boldsymbol{e}_f, \\ f(\boldsymbol{x}) = b \end{cases}$$

where $\boldsymbol{v} = \boldsymbol{v}(f)$.

- ZKP techniques for valid openings of commitments are available.
- How to simultaneously show that $f(\boldsymbol{x}) = b$?

Technique for Handling $f(\boldsymbol{x}) = b$

- Recall. $\boldsymbol{v} = \boldsymbol{v}(f) = (v_0, \dots, v_n)$ as f is a symmetric Boolean function.
- Define $w = \mathrm{weight}(\boldsymbol{x})$.
- Hence,

$$f(\boldsymbol{x}) = b \Leftrightarrow v_w = b.$$

- To extract v_w from $\boldsymbol{v}$, define $\boldsymbol{y} = \mathrm{U}(w) = (y_0, \dots, y_n) = (0, \dots, 0,1,0, \dots, 0)$ the w^{th} basis vector.
- Hence,

$$f(\boldsymbol{x}) = b \Leftrightarrow v_w = b \Leftrightarrow \langle \boldsymbol{v}, \boldsymbol{y} \rangle = b.$$

1. How to construct $\boldsymbol{y}$?
2. How to show that $\langle \boldsymbol{v}, \boldsymbol{y} \rangle = b$?

Constructing $\boldsymbol{y} = \mathrm{U}(w)$

- Recall. $\boldsymbol{x} \in \{0,1\}^n, \quad w = \mathrm{weight}(\boldsymbol{x}), \quad \boldsymbol{y} = \mathrm{U}(w) \in \{0,1\}^{n+1}$.
- Observation. Number of 0's in the right of 1 in $\boldsymbol{y}$ is equal to $n - w$.
- Example. $\boldsymbol{x} = (1,0,1,0,0,1,1) \in \{0,1\}^7 \Rightarrow \boldsymbol{y} = (0,0,0,0,1,0,0,0) \in \{0,1\}^8$.
- To show that $\boldsymbol{y}$ is well-formed, construct $\boldsymbol{z} \in \{0,1\}^{n+1}$ by inverting all 0's in the right of 1 in $\boldsymbol{y}$.
- Example. $\boldsymbol{y} = (0,0,0,0,1,0,0,0) \in \{0,1\}^8 \Rightarrow \boldsymbol{z} = (0,0,0,0,1,1,1,1) \in \{0,1\}^8$.
- Facts. By setting $\boldsymbol{z} = (z_0, \dots, z_n) \in \{0,1\}^8$, then

$$\boldsymbol{y} = \mathrm{U}(w) \Leftrightarrow \begin{cases} z_0 = y_0, \\ z_i = y_i \oplus z_{i-1} \ \forall i \in \{1, \dots, n\}, \\ \mathrm{weight}(\boldsymbol{y}) = 1 \\ \mathrm{weight}(\boldsymbol{z}) + \mathrm{weight}(\boldsymbol{x}) = n + 1. \end{cases}$$

Showing $\langle \boldsymbol{v}, \boldsymbol{y} \rangle = b$

- Recall. $\boldsymbol{y} = (y_0, y_1, \dots, y_n) = \mathrm{U}(j) \in \{0,1\}^{n+1}$ and $\boldsymbol{v} = \boldsymbol{v}(f) = (v_0, v_1, \dots, v_n) \in \{0,1\}^{n+1}$.
- $\mathrm{ext}(\boldsymbol{y}) = (\boldsymbol{y}_0 \| \boldsymbol{y}_1 \| \dots \| \boldsymbol{y}_n) = (y_0, 0, y_1, 0, \dots, y_n, 0) \in \{0,1\}^{2n+2}$ where $\boldsymbol{y}_i = (y_i, 0)$.
- Observation. $\mathrm{weight}(\mathbf{y}_\mathrm{j}) = 1 \bmod 2$ and $\mathrm{weight}(\boldsymbol{y}_i) = 0 \bmod 2\ \forall i \neq j$.
- $\mathrm{enc}(\boldsymbol{v}) = (\boldsymbol{v}_0 \| \boldsymbol{v}_1 \| \dots \| \boldsymbol{v}_n) = (\overline{v}_0, v_0, \overline{v}_1, v_1, \dots, \overline{v}_n, v_n) \in \{0,1\}^{2n+2}$ where $\boldsymbol{v}_i = (\overline{v}_i, v_i)$.
- Observation. $\mathrm{weight}(\boldsymbol{v}_i) = 1 \bmod 2\ \forall i$.
- Define $\boldsymbol{b} = (\boldsymbol{b}_0 \| \boldsymbol{b}_1 \| \dots \| \boldsymbol{b}_n) = \mathrm{ext}(\boldsymbol{y}) \oplus \mathrm{enc}(\boldsymbol{v})$ where $\boldsymbol{b}_i = (b_i \oplus \overline{v}_i, v_i)$ s.t

$$\begin{cases} \mathrm{weight}(\boldsymbol{b}_j) = 0 \bmod 2, \\ \mathrm{weight}(\boldsymbol{b}_i) = 1 \bmod 2\ \forall i \neq j. \end{cases}$$

Showing $\langle \boldsymbol{v}, \boldsymbol{y} \rangle = b$ (continued)

- Define $\text{good}(b) = \{(\boldsymbol{b}'_0 \| \boldsymbol{b}'_1 \| \dots \| \boldsymbol{b}'_n) : \text{exits unique } j \text{ s.t } \boldsymbol{b}'_j = (b, b) \text{ and } \text{weight}(\boldsymbol{b}'_i) = 1\ \forall i \ \neq j\}$.

$$\text{ext}(\boldsymbol{y}) \oplus \text{enc}(\boldsymbol{v}) \in \text{good}(b) \Leftrightarrow \langle \boldsymbol{v}, \boldsymbol{y} \rangle = b.$$

- Now, assume that $\text{weight}(\boldsymbol{y})$ is unknown and $\boldsymbol{b} = \text{ext}(\boldsymbol{y}) \oplus \text{enc}(\boldsymbol{v}) \in \text{good}(b)$.
- $\boldsymbol{b} = (\boldsymbol{b}_0 \| \boldsymbol{b}_1 \| \dots \| \boldsymbol{b}_n) \in \text{good}(b) \Rightarrow \boldsymbol{b}_j = (b, b)$ for some unique j and $\text{weight}(\boldsymbol{b}_i) = 1\ \forall i \neq j$.
- $\text{enc}(\boldsymbol{v}) = (\boldsymbol{v}_0 \| \boldsymbol{v}_1 \| \dots \| \boldsymbol{v}_n) \Rightarrow \text{weight}(\boldsymbol{v}_i) = 1 \bmod 2\ \forall i$.

➢ $\text{ext}(\boldsymbol{y}) = (\boldsymbol{y}_0 \| \boldsymbol{y}_1 \| \dots \| \boldsymbol{y}_n) = \boldsymbol{b} \oplus \text{enc}(\boldsymbol{v}) \Rightarrow \text{weight}(\boldsymbol{y}_j) = 1$ and $\text{weight}(\boldsymbol{y}_i) = 0 \bmod 2\ \forall i \neq j$.

$$\left.\begin{array}{r} \boldsymbol{y}_j = (y_j, 0) \Rightarrow y_j = 1 \\ \forall i \neq j, \boldsymbol{y}_i = (y_i, 0) \Rightarrow y_i = 0 \end{array}\right\} \Rightarrow \boldsymbol{y} = (y_0, \dots, y_n) \text{ is a unit vector.}$$

- In summary.

$$\boldsymbol{b} = \text{ext}(\boldsymbol{y}) \oplus \text{enc}(\boldsymbol{v}) \in \text{good}(b) \Leftrightarrow \langle \boldsymbol{v}, \boldsymbol{y} \rangle = b \text{ and } \boldsymbol{y} \text{ is unit vector}$$

Putting pieces together

Theorem. $\boldsymbol{x} \in \{0,1\}^n, \boldsymbol{v} = \boldsymbol{v}(f) = (v_0, v_1, \dots, v_n), b \in \{0,1\}$, the following statements are equivalent:

i. $f(\boldsymbol{x}) = b$.

ii. There exists $b_0, b_1, \dots, b_n \in \{0,1\}$ and $\boldsymbol{z} = (z_0, z_1, \dots, z_n) \in \{0,1\}^{n+1}$ satisfying

$$\begin{cases} b_0 \oplus v_0 \oplus z_0 = 1, \\ b_i \oplus v_i \oplus z_i \oplus z_{i-1} = 1 \ \ \forall i \in \{1, \dots, n\}, \\ \mathrm{weight}(\boldsymbol{x}) + \mathrm{weight}(\boldsymbol{z}) = n + 1, \\ (b_0, v_0, \dots, b_n, v_n) \in \mathrm{good}(b). \end{cases}$$

ZKP for Symmetric Boolean Functions

ZKP for Symmetric Boolean Functions

Prover shows that $\exists \mathbf{e}'_x \in \{0,1\}^t, \boldsymbol{e}'_f \in \{0,1\}^t,\ b_0, b_1, \dots, b_n \in \{0,1\},\ \boldsymbol{z} = (z_0, z_1, \dots, z_n) \in \{0,1\}^{n+1}$ s.t

$$\begin{cases} \boldsymbol{c}_x = \boldsymbol{A}_{1,x} \cdot \boldsymbol{x} \oplus \boldsymbol{A}_2 \cdot \boldsymbol{s}_x \oplus [\boldsymbol{I}_\kappa | \mathbf{0}^{\kappa\times t}] \cdot (\boldsymbol{e}_x \| \boldsymbol{e}'_x), \\ \boldsymbol{c}_f = \boldsymbol{A}_{1,f} \cdot \boldsymbol{v} \oplus \boldsymbol{A}_2 \cdot \boldsymbol{s}_f \oplus [\boldsymbol{I}_\kappa | \mathbf{0}^{\kappa\times t}] \cdot (\boldsymbol{e}_f \| \boldsymbol{e}'_f), \\ b_0 \oplus v_0 \oplus z_0 = 1, \\ b_i \oplus v_i \oplus z_i \oplus z_{i-1} = 1 \ \ \forall i \in \{1, \dots, n\}, \\ \text{weight}(\boldsymbol{e}_x \| \boldsymbol{e}'_x) = \text{weight}(\boldsymbol{e}_f \| \boldsymbol{e}'_f) = t, \\ \text{weight}(\boldsymbol{x}) + \text{weight}(\boldsymbol{z}) = n+1, \\ (b_0, v_0, \dots, b_n, v_n) \in \text{good}(b). \end{cases} \Leftrightarrow$$

$$\begin{cases} \boldsymbol{c}_x = \boldsymbol{A}_{1,x} \cdot \boldsymbol{x} \oplus \boldsymbol{A}_2 \cdot \boldsymbol{s}_x \oplus [\boldsymbol{I}_\kappa | \mathbf{0}^{\kappa\times t}] \cdot (\boldsymbol{e}_x \| \boldsymbol{e}'_x), \\ \boldsymbol{c}_f = \boldsymbol{A}_{1,f} \cdot \boldsymbol{v} \oplus \boldsymbol{A}_2 \cdot \boldsymbol{s}_f \oplus [\boldsymbol{I}_\kappa | \mathbf{0}^{\kappa\times t}] \cdot (\boldsymbol{e}_f \| \boldsymbol{e}'_f), \\ b_0 \oplus v_0 \oplus z_0 = 1, \\ b_i \oplus v_i \oplus z_i \oplus z_{i-1} = 1 \ \ \forall i \in \{1, \dots, n\}, \end{cases}$$

and

$$\begin{cases} \text{weight}(\boldsymbol{e}_x \| \boldsymbol{e}'_x) = \text{weight}(\boldsymbol{e}_f \| \boldsymbol{e}'_f) = t, \\ \text{weight}(\boldsymbol{x}) + \text{weight}(\boldsymbol{z}) = n+1, \\ (b_0, v_0, \dots, b_n, v_n) \in \text{good}(b). \end{cases}$$

ZKP for Symmetric Boolean Functions

Prover shows that $\exists \mathbf{e}'_x \in \{0,1\}^t, \boldsymbol{e}'_f \in \{0,1\}^t,\ b_0, b_1, \dots, b_n \in \{0,1\},\ \boldsymbol{z} = (z_0, z_1, \dots, z_n) \in \{0,1\}^{n+1}$ s.t

$$\begin{cases} \boldsymbol{c}_x = \boldsymbol{A}_{1,x} \cdot \boldsymbol{x} \oplus \boldsymbol{A}_2 \cdot \boldsymbol{s}_x \oplus [\boldsymbol{I}_\kappa | \boldsymbol{0}^{\kappa\times t}] \cdot (\boldsymbol{e}_x \| \boldsymbol{e}'_x), \\ \boldsymbol{c}_f = \boldsymbol{A}_{1,f} \cdot \boldsymbol{v} \oplus \boldsymbol{A}_2 \cdot \boldsymbol{s}_f \oplus [\boldsymbol{I}_\kappa | \boldsymbol{0}^{\kappa\times t}] \cdot (\boldsymbol{e}_f \| \boldsymbol{e}'_f), \\ b_0 \oplus v_0 \oplus z_0 = 1, \\ b_i \oplus v_i \oplus z_i \oplus z_{i-1} = 1 \ \ \forall i \in \{1, \dots, n\}, \end{cases}$$

and

$$\begin{cases} \mathrm{weight}(\boldsymbol{e}_x \| \boldsymbol{e}'_x) = \mathrm{weight}(\boldsymbol{e}_f \| \boldsymbol{e}'_f) = t, \\ \mathrm{weight}(\boldsymbol{x}) + \mathrm{weight}(\boldsymbol{z}) = n + 1, \\ (b_0, v_0, \dots, b_n, v_n) \in \mathrm{good}(b). \end{cases}$$

$\Rightarrow$

$$\mathrm{VALID}_{\mathrm{SYM}} = B(\kappa + t, t) \| B(\kappa + t, t) \| B(2n + 1, n + 1) \| \mathrm{good}(b)$$

Possible to construct set of permutations S_{SYM}

Secret $\boldsymbol{w}_1 = (\boldsymbol{e}_x \| \boldsymbol{e}'_x \| \boldsymbol{e}_f \| \boldsymbol{e}'_f \| \boldsymbol{x} \| \boldsymbol{z} \| \boldsymbol{b}) \in \mathrm{VALID}_{\mathrm{SYM}}$,

Secret $\boldsymbol{w}_2 = (\boldsymbol{s}_x \| \boldsymbol{s}_f)$,

By linear algebra, define public $\boldsymbol{M}_1, \boldsymbol{M}_2, \boldsymbol{u}$ satisfying

$$\boldsymbol{M}_1 \cdot \boldsymbol{w}_1 \oplus \boldsymbol{M}_2 \cdot \boldsymbol{w}_2 = \boldsymbol{u}$$

where $\boldsymbol{u} = (\boldsymbol{c}_x \| \boldsymbol{c}_f \| \boldsymbol{1}^{n+1})$.

$\Rightarrow$ Reducible to R_{abstract}.

Thank you!
Q&A

References

[JKPT12] A. Jain, S. Krenn, K. Pietrzak, and A. Tentes. Commitments and efficient zero-knowledge proofs from learning parity with noise. In *ASIACRYPT 2012*, volume 7658 of *LNCS*, pages 663–680. Springer, 2012.

[LLMNW16] B. Libert, S. Ling, F. Mouhartem, K. Nguyen, and H. Wang. Signature schemes with efficient protocols and dynamic group signatures from lattice assumptions. In *ASIACRYPT 2016*, volume 10032 of *LNCS*, pages 373–403, 2016.