ZKBoo / ZKB++

Kevin Pretterhofer

Graz, January 16, 2020

Multi-Party Computation (MPC)

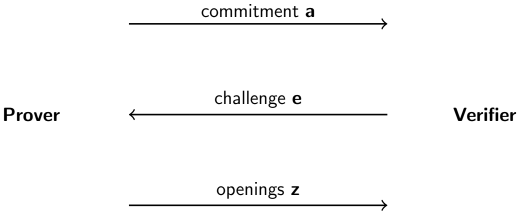
- Consider function: $f(\mathbf{x}) = \mathbf{y}$
  - $\mathbf{x} = \{\mathbf{x_1}, \mathbf{x_2}, ..., \mathbf{x_n}\}$
- Consider n players: $P_1, P_2, ..., P_n$
  - P_i holds secret value $\mathbf{x_i}$
- Players jointly compute $f(\mathbf{x})$
  - without revealing secret value $\mathbf{x_i}$

Zero-Knowledge Proofs

- Let L be a NP-language, with witness relation R, s.t. $L = \{x \mid \exists w : R(x, w) = 1\}$
- Let P be the prover and V be the verifier
- P wants to convince V that $x \in L$ and even more that P knows w
  - Completeness
  - Soundness
  - Zero-Knowledge

Sigma Protocols

- Interactive 3-move protocol
- Properties:
  - Complete
  - Special Soundness
  - Special honest-verifier ZK
- Can be made non-interactive: Fiat-Shamir heruistics [FS]



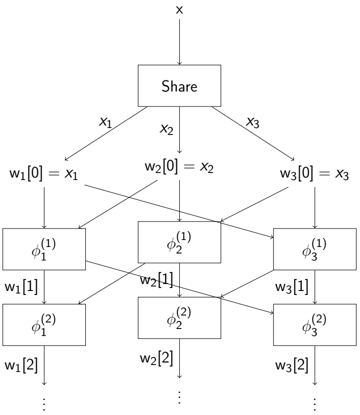
ZKBoo [GMO]

Introduction

- Zero-Knowledge proof system
  - Tailored for boolean circuits
- "MPC-in-the-head"-pardigm [Ish+]

(2,3)-decomposition

- Considering $y = \phi(x)$
  - Share
  - $\bigcup_{j=1}^{N}\{\phi_1^{(j)}, \phi_2^{(j)}, \phi_3^{(j)}\}$
  - $\mathrm{Output}_1, \mathrm{Output}_2, \mathrm{Output}_3$
  - Rec
- Correctness
- (2)-Privacy



The protocol Π_ϕ^* to evaluate ϕ

1. Sample random tapes $\mathbf{k}_1, \mathbf{k}_2, \mathbf{k}_3$
2. $(\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3) \leftarrow \mathrm{Share}(\mathbf{x}, \mathbf{k}_1, \mathbf{k}_2, \mathbf{k}_3)$
3. Let $\mathbf{w}_1, \mathbf{w}_2, \mathbf{w}_3$ be vector with $N + 1$ entries
4. Initialize $\mathbf{w}_i[0]$ with $\mathbf{x}_i$ for all $i \in [3]$
5.
6. For $j = 1...N$ compute:
   For $i = 1, 2, 3$ compute:
   $\mathbf{w}_i[j] =$
   $\phi_i^{(j)}((\mathbf{w}_m[0..j-1], \mathbf{k}_m)_{m \in \{i, i+1\}})$
7. Compute $\mathbf{y}_i = \mathrm{Output}_i(\mathbf{w}_i, \mathbf{k}_i)$ for $i \in \{1, 2, 3\}$
8. Compute $\mathbf{y} = \mathrm{Rec}(\mathbf{y}_1, \mathbf{y}_2, \mathbf{y}_3)$

The Linear Decomposition

- Share$(\mathbf{x}; k_1, k_2, k_3)$ samples random $\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3$ s.t. $\mathbf{x} = \mathbf{x}_1 + \mathbf{x}_2 + \mathbf{x}_3$
- $\bigcup_{j=1}^{N} \{\phi_1^{(j)}, \phi_2^{(j)}, \phi_3^{(j)}\}$:
  - unary "add α":
    $\mathbf{w}_i[c] = \begin{cases} \mathbf{w}_i[a] + \alpha, & \text{if } i = 1 \\ \mathbf{w}_i[a] & \text{otherwise.} \end{cases}$
  - unary "mult α":
    $\mathbf{w}_i[c] = \alpha \cdot \mathbf{w}_i[a]$
  - binary addition:
    $\mathbf{w}_i[c] = (\mathbf{w_i}[a] + \mathbf{w_i}[b])$
  - binary multiplication:
    $\mathbf{w}_i[c] = \mathbf{w}_i[a] \cdot \mathbf{w}_i[b] + \mathbf{w}_{i+1}[a] \cdot \mathbf{w}_i[b] + \mathbf{w}_i[a] \cdot \mathbf{w}_{i+1}[b] + R_i(c) - R_{i+1}(c)$
- Output$_i(\mathbf{w}_i, \mathbf{k}_i)$ selects shares of the output wires
- Rec$(\mathbf{y}_1, \mathbf{y}_2, \mathbf{y}_3)$ outputs $\mathbf{y} = \mathbf{y}_1 + \mathbf{y}_2 + \mathbf{y}_3$

The ZKBoo Protocol

1. Prover runs Π^*_ϕ and obtain $\mathbf{w}_i$ and $\mathbf{y}_i$ for all i
2. Commit to $\mathbf{c}_i = \text{Com}(\mathbf{k}_i, \mathbf{w}_i)$ for all i
3. Send $\mathbf{a} = (\mathbf{y}_1, \mathbf{y}_2, \mathbf{y}_3, \mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3)$
4. Verifier chooses $\mathbf{e} \in [3]$ and sends to prover
5. Prover opens $\mathbf{c}_e, \mathbf{c}_{e+1}$ revealing $\mathbf{z} = (\mathbf{k}_e, \mathbf{w}_e, \mathbf{k}_{e+1}, \mathbf{w}_{e+1})$
6. Verifier checks: $\text{Rec}(\mathbf{y}_1, \mathbf{y}_2, \mathbf{y}_3) \neq \mathbf{y}$, reject
7. If $\exists i \in \{e, e+1\}$ s.t. $\mathbf{y}_i \neq \text{Output}_i(\mathbf{w}_i)$, reject
8. If $\exists j$ s.t. $\mathbf{w}_e[j] \neq \phi_e^{(j)}(\mathbf{w}_e, \mathbf{w}_{e+1}, \mathbf{k}_e, \mathbf{k}_{e+1})$, reject
9. Accept

ZKB++ [Cha+]

Optimizations

- Not including input shares
- Not including commitments
- No additional randomness for commitments
- Not including the output shares
- Not including View_e

Thank you for your attention!

Bibliography I

[Cha+] Melissa Chase et al. **Post-Quantum Zero-Knowledge and Signatures from Symmetric-Key Primitives**. Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, CCS 2017, Dallas, TX, USA, October 30 - November 03, 2017.

[FS] Amos Fiat and Adi Shamir. **How to Prove Yourself: Practical Solutions to Identification and Signature Problems**. Advances in Cryptology - CRYPTO '86, Santa Barbara, California, USA, 1986, Proceedings.

Bibliography II

[GMO] Irene Giacomelli, Jesper Madsen, and Claudio Orlandi. **ZKBoo: Faster Zero-Knowledge for Boolean Circuits**. 25th USENIX Security Symposium, USENIX Security 16, Austin, TX, USA, August 10-12, 2016.

[Ish+] Yuval Ishai et al. **Zero-knowledge from secure multiparty computation**. Proceedings of the 39th Annual ACM Symposium on Theory of Computing, San Diego, California, USA, June 11-13, 2007.