Mr NISC from LWE: _Multiparty Reusable Non-Interactive Secure Computation_

Fabrice Benhamouda  
(Algorand Foundation)

Joint work with  
Aayush Jain (UCLA, NTT),  
Ilan Komargodski (Hebrew University, NTT),  
Rachel Lin (University of Washington)
mrNISC: Multiparty Reusable Non-Interactive Secure Computation

Public study $f$

$f(x_1)$, but learn nothing else

Public study $f'$

$f'(x_1)$

Public study $f''$

$f''(x_4)$
mrNISC: Multiparty Reusable Non-Interactive Secure Computation

Public study $f$

$f(x_1, x_2, x_3)$

Insecure: [FK94, IK97]
Leakage of residual function
mrNISC: Multiparty Reusable Non-Interactive Secure Computation

Solution:
Require commitments $\hat{x}_i$ (and secret state $s_i$)
mrNISC: Multiparty Reusable Non-Interactive Secure Computation

- Input encoding / commitment: \((\hat{x}_i, s_i) \leftarrow \text{Com}(x_i)\)
- Computation: \(\alpha_i \leftarrow \text{Encode}(f, \{\hat{x}_j\}, s_i)\) \((j \in S, \text{chosen set of inputs/parties})\)
- Output: \(y \leftarrow \text{Eval}(f, \{\hat{x}_j\}, \{\alpha_j\})\)

- Correctness with dynamic parties joining
- Simulation security:
  - Semi-honest adversary, static corruptions, dishonest majority
Another View of mrNISC

mrNISC

= 2-round MPC with

reusable first round & dynamic set of parties

Round 1 = broadcast commitments $\hat{\chi}_i$

Round 2 = broadcast computation encodings $\alpha_i$
Comparison with Previous Reusable 2-round MPC

<table>
<thead>
<tr>
<th></th>
<th>Setup</th>
<th>Assumptions</th>
<th>Reusable?</th>
<th>Dynamic set of parties?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Obfuscation</td>
<td>No setup</td>
<td>iO</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>Witness Encryption</td>
<td>No setup</td>
<td>Witness Encryption</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>Multi-key FHE</td>
<td>No setup</td>
<td>LWE</td>
<td>✅</td>
<td>❌</td>
</tr>
<tr>
<td>Homomorphic Secret</td>
<td>No setup</td>
<td>DDH</td>
<td>✅</td>
<td>❌</td>
</tr>
<tr>
<td>Secret Sharing</td>
<td>No setup</td>
<td>SXDH</td>
<td>✅</td>
<td>✅</td>
</tr>
<tr>
<td>This work</td>
<td>No setup</td>
<td>LWE</td>
<td>✅</td>
<td>✅</td>
</tr>
</tbody>
</table>
Our Contributions

• Definition of **Reusable Functional OT**
  • mrNISC with 2 parties for specific functionality

• LWE \(\rightarrow\) **Reusable Functional OT** \(\rightarrow\) mrNISC

• Applications
  • Multi-Key FHE \(\rightarrow\) Threshold Multi-Key FHE
    • For NC1, first polynomial-modulus threshold multi-key FHE
Construction Overview

[GGHR14] Obfuscation mrNISC


[This work] LWE Garbled Circuits + Reusable Functional OT mrNISC
Overview

- [GGHR14] Compress $L$-round MPC to 2 rounds using iO
  - Round 1: commitment of input
  - Round 2: obfuscation of

\[
\begin{align*}
\text{Input: previous messages in } L\text{-round MPC} \\
+ \ldots \\
\text{Output: next message + } \ldots
\end{align*}
\]

- [GLS15] Replace iO by witness encryption + garbled circuit

\[
\begin{align*}
\text{Input: previous messages in } L\text{-round MPC} \\
\text{Output: message + } \ldots
\end{align*}
\]

Allow to compute the garbled circuit labels
Overview of Construction from iO
[GGHR14...]  
L-round MPC

For each party $P_i$:

Round 1: broadcast $m_i^1 = \text{Next}(x_i, r_i)$
Round 2: broadcast $m_i^2 = \text{Next}(x_i, r_i, \bar{m}^{<2})$

... 

Round L: broadcast $m_i^L = \text{Next}(x_i, r_i, \bar{m}^{<L})$

Output: $y = \text{Output}({\bar{m}})$
Overview of Construction from iO

[GGHR14...]

Round Compression

For each party $P_i$:

Round 1: broadcast $c_i = \text{Commit}(x_i, r_i)$

Round 2: broadcast $m_i^1 = \text{Next}(x_i, r_i)$

+ obfuscation of

$\vdots$

Correct: local evaluation of MPC

Insecure: leakage of residual function

---

Input: $\overline{m}^{<2}, \{\pi_j^1\}$
Abort if any proof $\pi_j^1$ invalid
Output: $m_i^2 = \text{Next}(x_i, r_i, \overline{m}^{<2}) + \text{proof } \pi_i^2$

---

Input: $\overline{m}^{<L}, \{\pi_j^{L-1}\}$
Abort if any proof $\pi_j^{L-1}$ invalid
Output: $m_i^L = \text{Next}(x_i, r_i, \overline{m}^{<L})$
Construction from Reusable Functional OT

**Simplification:** 1-bit message

**Goal:** Anyone can compute this message

**Input:** Bob’s round-(r-1) message $b$

**Output:** Alice’s round-r message + ...

**Labels:** $(\ell_0, \ell_1) = g_1(K_1)$
Reusable Functional OT from LWE

- Goal: 2rNISC for
  - Alice’s input = $x_1$, Bob’s input = $x_2$
  - Output: $y = (b, \ell_b)$ with $(\ell_0, \ell_1) = g_1(x_1)$ and $b = g_2(x_2)$

- Bob commits to $x_2$ using fully homomorphic commitment:
  \[
  \hat{x}_2 = \text{Com}(x_2) \quad \Rightarrow \quad C_{g_2} = \text{Com}(g_2(x_2))
  \]
  \[
  x_2 = (A, A R + x_2 G) \quad \Rightarrow \quad C_{g_2} = A R_{g_2} + (1 - b) G
  \]

  - $\alpha_1$: Alice encrypts $\ell_\beta$ for $\beta = 0, 1$
    - can be decrypted with ZK proof “$C_{g_2} = \text{Com}(\beta)$”

  - $\alpha_2$: Bob provides ZK proof that $C_{g_2} = \text{Com}(b)$

  Can use GSW commitments!

  Ideas from [GVW15] and [BD18]
Conclusion

• Definition of Reusable Functional OT
  • mrNISC with 2 parties for specific functionality

• LWE $\rightarrow$ Reusable Functional OT $\rightarrow$ mrNISC

• Applications
  • Multi-Key FHE $\rightarrow$ Threshold Multi-Key FHE
    • For NC1, first polynomial-modulus threshold multi-key FHE
Thank You