Two-Round Secure Multiparty Computation
Minimizing Public Key Operations

Sanjam Garg    Peihan Miao    Akshayaram Srinivasan

Berkeley
What did we achieve?
Two-Round Secure Multiparty Computation
Minimizing Public Key Operations

Sanjam Garg Peihan Miao Akshayaram Srinivasan
Secure Multiparty Computation (MPC)

Only $y$ is revealed.

$f(x_1, x_2, x_3, x_4, x_5)$
What does **Two-Round** mean?

The MPC protocol has two rounds.
Two-Round MPC
Two-Round MPC
Why is round complexity important?
Why is round complexity important?

~200ms
Why not one round?

Because it’s impossible! [HLP’11]
Two-Round MPC?

- [Yao’86, GMW’87]: any function, round = depth of $C$
- [BMR’90]: constant rounds
- 2 rounds from various assumptions
  - Indistinguishability Obfuscation (iO) [GGHR’14]
  - Witness Encryption [GLS’15]
  - Learning With Errors (LWE) [MW’16, BP’16, PS’16]
  - Bilinear Maps [GS’17]
  - 2-Round Oblivious Transfer (OT) [BL’18, GS’18]
- 2-round MPC $\iff$ 2-round OT
Can we implement it?
Yes, but it’s too slow...

Why?
Too many public key operations...

Why is it bad?
Because public key operation is VERY slow!
• Symmetric key operations (AES) ~100M/sec
• Public (asymmetric) key operations ~10K/sec
Our Main Result

• 2-round MPC from 2-round OT (minimal assumption)

• State of the art: \( \text{poly}(n, \lambda, |C|) \) OTs (public key operations)

• We improve it to: \( \text{poly}(n, \lambda) \) OTs (public key operations) + \( \text{poly}(n, \lambda, |C|) \) symmetric key operations
  • Semi-honest from 2-round semi-honest OT
  • Malicious from 2-round malicious OT in the CRS model
How did we achieve it?
How to reduce OTs (public key operations)?

OT extension!

- poly$(n, \lambda, |C|)$ OTs
- Minimize public key operations

2-round OT extension?

Yes! [Beaver’96]
How to reduce OTs (public key operations)?

2-round OT extension!

- poly\((n, \lambda, |C|)\) OTs
- Minimize public key operations

2-round MPC with poly\((n, \lambda, |C|)\) OTs

Combine?

No!

Why?

Yes! [Beaver’96]
2-round MPC with $\text{poly}(n, \lambda, |C|)$ OTs

Combine? No!

Why?

2-round OT extension?
2-round MPC with $\text{poly}(n, \lambda, |C|)$ OTs

- $\text{poly}(n, \lambda, |C|)$ OTs
- Special properties needed from OTs

Combine?

No!

Why?

How to solve it?

2-round OT extension?

- $\text{poly}(n, \lambda, |C|)$ OTs
- Special properties needed from OTs
2-round MPC with $\text{poly}(n, \lambda, |C|)$ OTs

Combine?
No!

Why?

How to solve it?

2-round OT extension?
2-round MPC with \(\text{poly}(n, \lambda, |C|)\) OTs

Combine?  
\[\checkmark\text{poly}(n, \lambda, |C|)\) OTs\]  
\[\checkmark\text{Weakened special properties needed from OTs}\]

No!

Why?

How to solve it?

2-round OT extension?

\[\checkmark\text{poly}(n, \lambda, |C|)\) OTs\]  
\[\checkmark\text{Weakened special properties needed from OTs}\]
Technical Overview (semi-honest)

• Building blocks
  • Yao’s garbled circuit (symmetric key)
  • two-round OT (public key)

• Two-Round MPC [BL’18, GS’18]
  • What are the special properties needed from OT?
  • Why are they needed?

• Two-Round OT Extension [Beaver’96]
  • Why not satisfying the special properties needed from OT?

• How to solve the problems?
Technical Overview (semi-honest)

• Building blocks
  • Yao’s garbled circuit (symmetric key)
  • two-round OT (public key)

• Two-Round MPC [BL’18, GS’18]
  • What are the special properties needed from OT?
  • Why are they needed?

• Two-Round OT Extension [Beaver’96]
  • Why not satisfying the special properties needed from OT?

• How to solve the problems?
Yao’s garbled circuit [Yao’86]

Security: Evaluation only reveals $C(x)$
Oblivious Transfer (OT) [Rab’81, EGL’85, BCR’86, Kil’88]

\(m_0, m_1\)  
\(\perp\)  
\(b\)  
\(m_b\)  

\(b\) is hidden to \(S\)  
\(m_{1-b}\) is hidden to \(R\)  

\(b \in \{0,1\}\)
Two-Round OT [AIR’01, NP’01, HK’12]

$b$ is hidden to $S$
$m_{1-b}$ is hidden to $R$

$b \in \{0, 1\}$
Technical Overview (semi-honest)

• Building blocks
  • Yao’s garbled circuit (symmetric key)
  • two-round OT (public key)

• Two-Round MPC [BL’18, GS’18]
  • What are the special properties needed from OT?
  • Why are they needed?

• Two-Round OT Extension [Beaver’96]
  • Why not satisfying the special properties needed from OT?

• How to solve the problems?
Two-Round MPC \([\text{BL’18, GS’18}]\)

\[
\begin{align*}
    m_0^1, m_1^1 & \rightarrow \text{Oblivious Transfer} \rightarrow b_1 \\
    m_0^2, m_1^2 & \rightarrow \text{Oblivious Transfer} \rightarrow b_2 \\
    \vdots & \\
    m_0^k, m_1^k & \rightarrow \text{Oblivious Transfer} \rightarrow b_k
\end{align*}
\]

\[k = \text{poly}(\lambda, |C|)\]
Two-Round MPC [BL’18, GS’18]

- Decryption secrets are known by Receiver before Round-2
- Decryption secrets are independent

Why?
Two-Round MPC \([\text{BL’18, GS’18}]\)

- Decryption secrets are known by Receiver before Round-2
- Decryption secrets are independent
Technical Overview (semi-honest)

• Building blocks
  • Yao’s garbled circuit (symmetric key)
  • two-round OT (public key)

• Two-Round MPC [BL’18, GS’18]
  • What are the special properties needed from OT?
  • Why are they needed?

• Two-Round OT Extension [Beaver’96]
  • Why not satisfying the special properties needed from OT?

• How to solve the problems?
OT Extension [Beaver’96]

\[ m_0^1, m_1^1 \]
\[ m_0^2, m_1^2 \]
\[ \vdots \]
\[ m_0^k, m_1^k \]

\[ h_0^1, h_1^1 \rightarrow \text{Oblivious Transfer} \rightarrow c_1 \rightarrow h_{c_1}^1 \]
\[ h_0^2, h_1^2 \rightarrow \text{Oblivious Transfer} \rightarrow c_2 \rightarrow h_{c_2}^2 \]
\[ \vdots \]
\[ h_0^\lambda, h_1^\lambda \rightarrow \text{Oblivious Transfer} \rightarrow c_\lambda \rightarrow h_{c_\lambda}^\lambda \]

\[ \lambda \]
\[ +\text{poly}(\lambda, |C|) \]
symmetric key operations

\[ b_1 \]
\[ b_2 \]
\[ \vdots \]
\[ b_k \]
Two-Round OT Extension [Beaver’96]

- Decryption secrets are known by Receiver before Round-2
- Decryption secrets are independent

Why?
Two-Round OT Extension [Beaver’96]

Decryption secrets are independent
2-round MPC with $\text{poly}(n, \lambda, |C|)$ OTs

- $\text{poly}(n, \lambda, |C|)$ OTs
- Special properties needed from OTs

How to solve it?

2-round OT extension?

- $\text{poly}(n, \lambda, |C|)$ OTs
- Special properties needed from OTs

Combine? Yes!

Why? No!
Two-Round OT Extension [Beaver’96]

- Decryption secrets are known by Receiver before Round-2
- Decryption secrets are independent
Decryption secrets are known by Receiver before Round-2

Decryption secrets are independent
Two-Round MPC [BL’18, GS’18]

Decryption secrets are hard-coded in the garbled circuits; So they should be known before Round 2!
Second Attempt: Weaken Special Properties

Decryption secrets are hard-coded in the garbled circuits; So they should be known before Round 2!

Weakened property: Decryption secrets can be computed and fed into the garbled circuits after Round-2.
Summary

• What did we achieve?
  • 2-round MPC from 2-round OT using $\text{poly}(n, \lambda)$ OTs (public key operations) + $\text{poly}(n, \lambda, |C|)$ symmetric key operations

• Combine 2-round MPC with 2-round OT extension
  • Mismatch in the special properties!
  • Weaken special properties and modify protocols

• More challenges and new tools in malicious setting
  • Somewhere Adaptive Garbled Circuit
  • Special Purpose Zero-Knowledge Proof
Future Work

• How to make it more practical?
  • Making black-box use of crypto operations?
  • Impossible for 2 rounds! [GMMM’18] talk tomorrow morning :)
  • Black-box but 3 rounds?
    • Combining with black-box OT extension [IKNP’03]

• Concrete optimization for implementation
Thanks!