Gage MPC: Bypassing Residual Function Leakage for Non-Interactive MPC

Ghada Almashaqbeh\textsuperscript{1} Fabrice Benhamouda\textsuperscript{2} Seungwook Han\textsuperscript{3} Daniel Jaroslawicz\textsuperscript{3} Tal Malkin\textsuperscript{3} Alex Nicita\textsuperscript{3} Tal Rabin\textsuperscript{4,2} Abhishek Shah\textsuperscript{3} Eran Tromer\textsuperscript{3,5}

\textsuperscript{1}UConn, \textsuperscript{2}Algorand, \textsuperscript{3}Columbia, \textsuperscript{4}UPenn, \textsuperscript{5}Tel-Aviv University

PETS 2021
NIMPC — Auction

The winner is ...

\[ f(x_0, x_1, ..., x_N) \]
NIMPC — Auction

Trusted Setup [BGIKMP14, BKR17]

\[ f(m_0, m_1, \ldots, m_N) \]

The winner is ...
Leakage of the *Residual Function* is inherent. Evaluator and say $P_0$ can compute $f(\bullet, m_1, \ldots, m_N)$.
Leakage of the \textit{Residual Function} is inherent. Evaluator and say $P_0$ can compute $f(\bullet, m_1, \ldots, m_N)$.

Robustness to collusion. Only the residual function is leaked!
Leakage of the *Residual Function* is inherent.
Evaluator and say $P_0$ can compute $f(\bullet, m_1, \ldots, m_N)$.

Robustness to collusion.
Only the residual function is leaked!

Setup assumptions.
Leakage of the *Residual Function* is inherent.
Evaluator and say $P_0$ can compute $f(\bullet, m_1, \ldots, m_N)$.

Robustness to collusion.
Only the residual function is leaked!

Setup assumptions.

Avoid such limitations??!
MPC and Blockchain

- **Gen I.** A blockchain implements a broadcast channel.
**Gen I.** A blockchain implements a broadcast channel.

**Gen II.** Payments are incorporated into MPC.
MPC and Blockchain

- **Gen I.** A blockchain implements a broadcast channel.

- **Gen II.** Payments are incorporated into MPC.

- **Gen III.** *This work; Gage MPC!* Smart contracts and miners are active participants in MPC.
A monetary assumption. An honest party can put a collateral of value much higher than what an adversary can expend on computation.
A monetary assumption. An honest party can put a collateral of value much higher than what an adversary can expend on computation.
Eliminate the leakage of the residual function.
On Circumventing the Lower Bounds

- Eliminate the leakage of the residual function.
- Eliminate setup assumptions.
  - A PKI or pre-shared correlated randomness.
  - The need for a dedicated online evaluator.
On Circumventing the Lower Bounds

- Eliminate the leakage of the residual function.
- Eliminate setup assumptions.
  - A PKI or pre-shared correlated randomness.
  - The need for a dedicated online evaluator.

Gage MPC guarantees short term security!
Gage MPC: Our Construction

- Time Capsules
- Zero Knowledge Proofs
- POTC
- Collateral
- LD-MPC (Yao-based)
- GaTC

Gage MPC
Simply commit to a value that can be opened after expending a pre-specified amount of computation.

E.g., $h(s)$ where $s \leftarrow \{0, 1\}^{\lambda^*}$
Instead of announcing the decommitment itself (i.e., s), prove in zero knowledge that the decommitment has been found.
Bundle several POTCs together, and utilize a smart contract to provide a monetary incentive to open the intended POTC.
A generalization of Garbled Circuits that is robust to the exposure of additional labels.
Our Construction — Label Driven MPC (LD-MPC)

Conventional Yao; Exposure of any additional label compromise input privacy.

LD-MPC = Error Correcting Codes + Yao
Combines LD-MPC with GaTC. Simplest case; Only the input of $P_0$ is private.
- $P_0$ prepares a garbled circuit, GaTCs for input labels for $P_1, \ldots, P_N$, and a controller smart contract.
- $P_1, \ldots, P_N$ submit their inputs.
- Either $P_0$ will come back and open the corresponding labels, or bounty hunters will do.
- Smart contract evaluates the circuit over the labels and record the output.
The private input versions support only two party computation.
Conclusion

Main Result — Gage MPC

NIMPC for \( f \) leaking \( R \) and requiring \( TS \rightarrow \) NIMPC with no \( R \) and \( TS \)

Gen III of MPC + blockchain

Side Result

Several new primitives (POTC, GaTC, and LD-MPC) that could be of independent interest.

A proof-of-concept implementation in Ethereum-like blockchain.
Thank you!

Questions?