Highly Efficient Actively Secure Two-Party Computation with *One-Bit Advantage Bound*

Yi Liu[1] Junzuo Lai[1] Peng Yang[2] Anjia Yang[1] Qi Wang[3] Siu-Ming Yiu[2] Jian Weng[1]

1. Jinan University 2. The University of Hong Kong 3. Southern University of Science and Technology

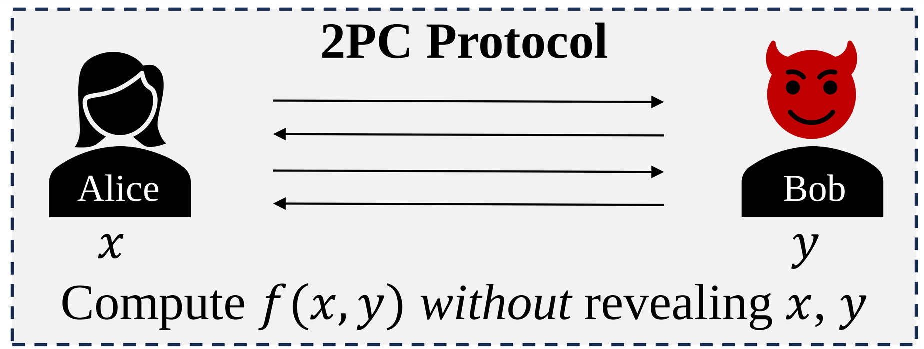
IEEE S&P 2025

Introduction

Secure two-party computation (2PC) allows two mutually distrusting parties to securely evaluate a public function on their private inputs.

Weak — Security — Strong

Passive Security
(a.k.a. *Semi-Honest* Security)
Adversaries *follow* the protocol, but *try to learn information*



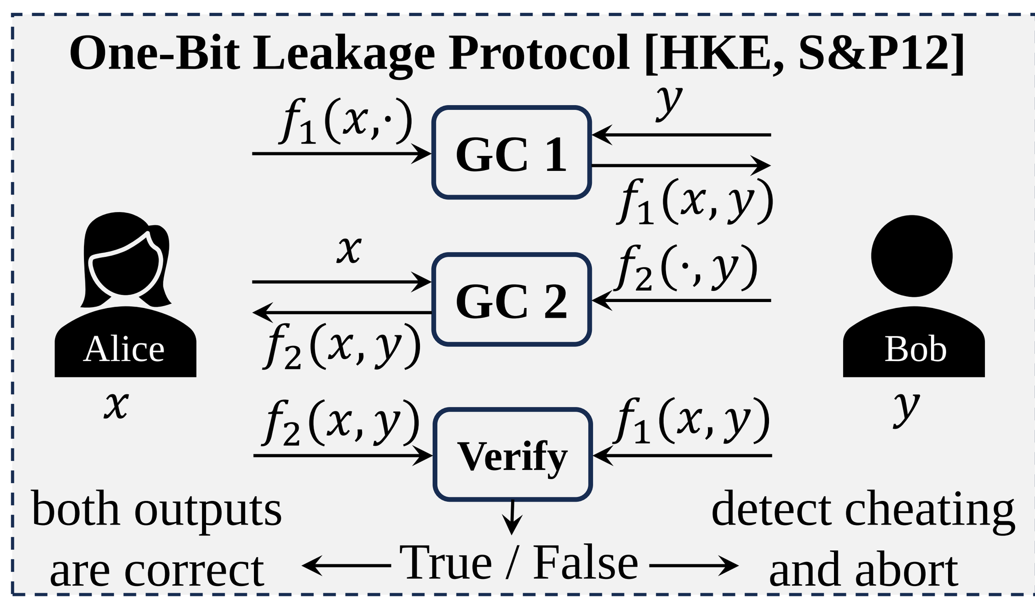
Active Security
(a.k.a. *Malicious* Security)
Adversaries may *deviate* from the protocol *arbitrarily*

Fast — Efficiency — Slow

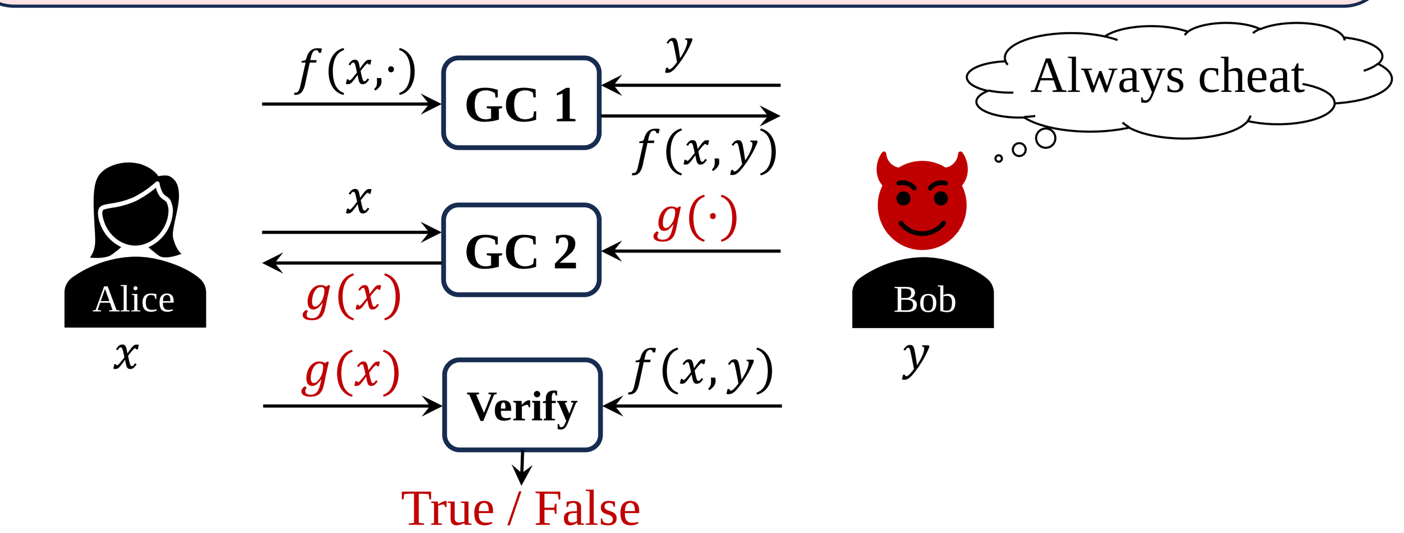
We seek to narrow the efficiency gap between actively and passively secure 2PC protocols.

Motivation

The notion of ***active security with one-bit leakage*** offers a promising approach to bridging the efficiency gap between passive and active security in garbled circuit (GC)-based 2PC.



Fairness Problem: **0** bits vs ***n*+1** bits, encourage cheating



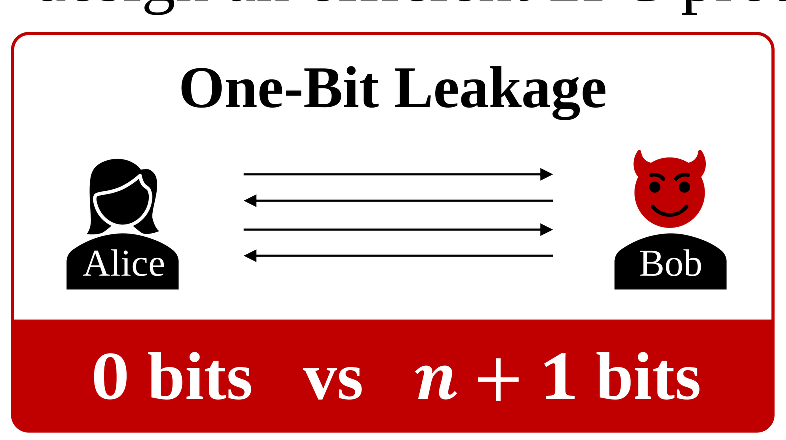
- Achieve **active security**
- But adversaries may learn **at most one additional bit of information**

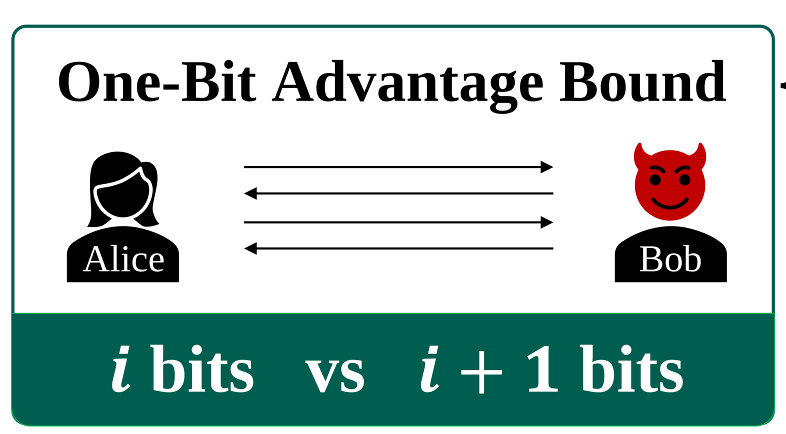
- The honest party cannot learn $f(x,y)$ (*i.e.*, learn 0 bits)
- The adversary learns $n+1$ bits about x
  - output $f(x,y)$
  - whether $g(x) = f(x,y)$

How can we provide an effective solution to the fairness problem in one-bit-leakage protocols?

Contributions

We propose active security with ***one-bit advantage bound*** and design an efficient 2PC protocol to address the fairness issue.





New Model

Formal Definition
Adjustable Advantage
- k-Bit Advantage Bound: i vs $i+k$ bits

New Protocol

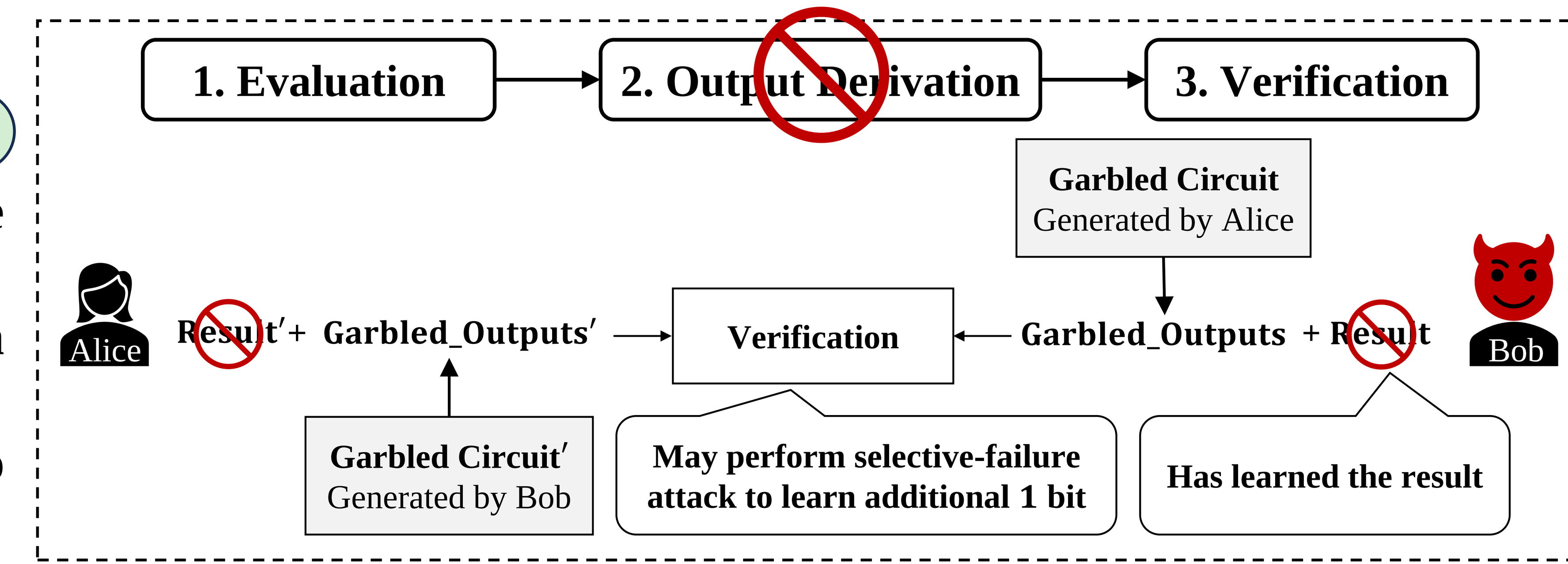
Fully Compatible with SOTA Garbling
- Three-Halves [RR21], Half-Gates [ZRE15]

Performance ≈ Passive 2PC

Key Insights

Start Point: The one-bit leakage protocol

To prevent either party from learning the output *before* verification
- We **remove the output derivation phase**;
- We **redesign the verification phase** to *work solely with garbled outputs*.



Observation: Exploit label structures of garbling schemes with point-and-permute and free-XOR techniques for verification

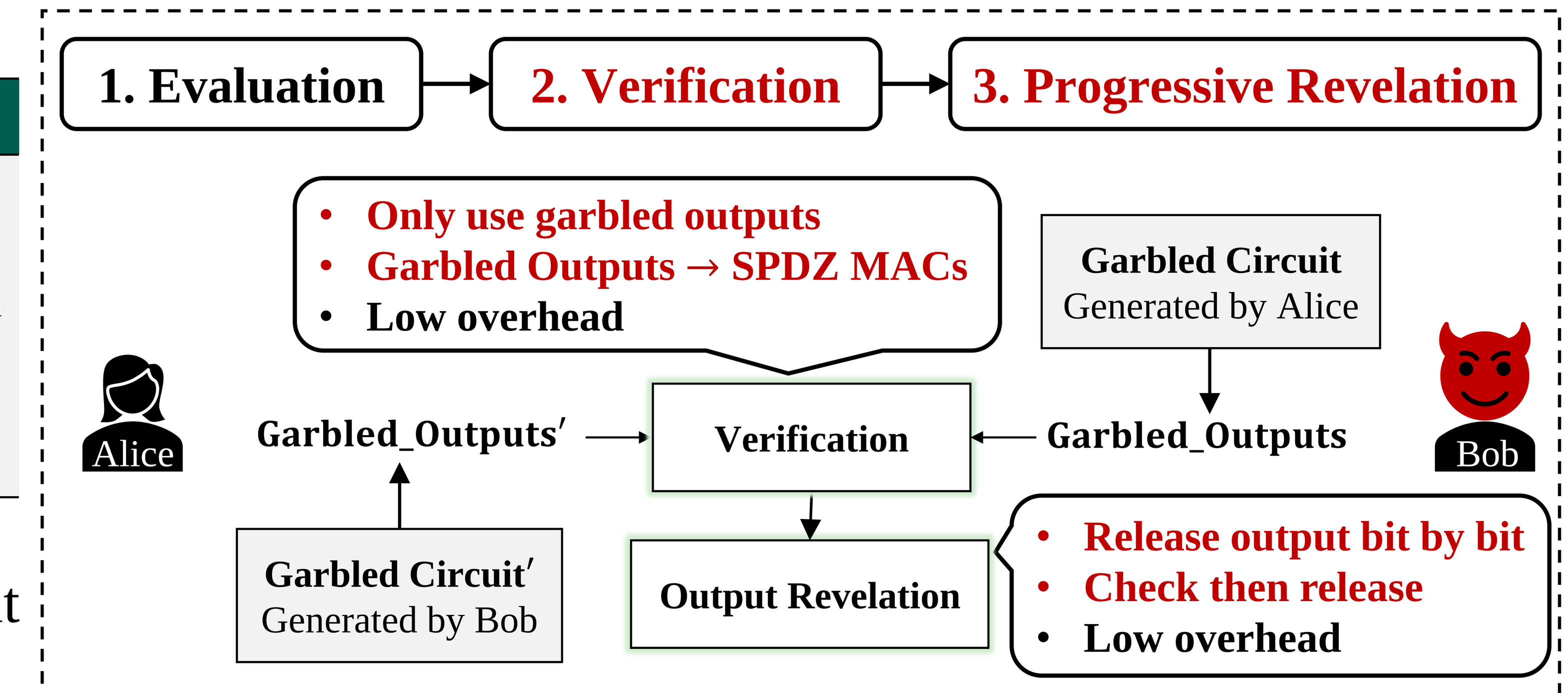
Within the garbled outputs, for a wire w, we have

	Alice's Values	Bob's Values	Notations
GC Generated by Alice	$\Delta_A, L_{w,0}, \lambda_w$	$\hat{z}_w, L_{w,\hat{z}_w}$	• Δ_A, Δ_B: global key • $\hat{z}_w, \hat{z}'_w$: masked bit • λ_w, λ'_w: point-permute bit • $L_{w,b}, L'_{w,b}$: labels for w with masked bit $b \in \{0,1\}$ Actual bit $z_w = \lambda_w \oplus \hat{z}_w$, $z'_w = \lambda'_w \oplus \hat{z}'_w$ Evaluators only see masked bit
GC′ Generated by Bob	$\hat{z}'_w, L'_{w,\hat{z}'_w}$	$\Delta_B, L'_{w,0}, \lambda'_w$	

If computed correctly, it holds that:

$$\lambda_w \oplus \hat{z}_w = \hat{z}'_w \oplus \lambda'_w = z_w (= z'_w) \longrightarrow \text{actual bit}$$

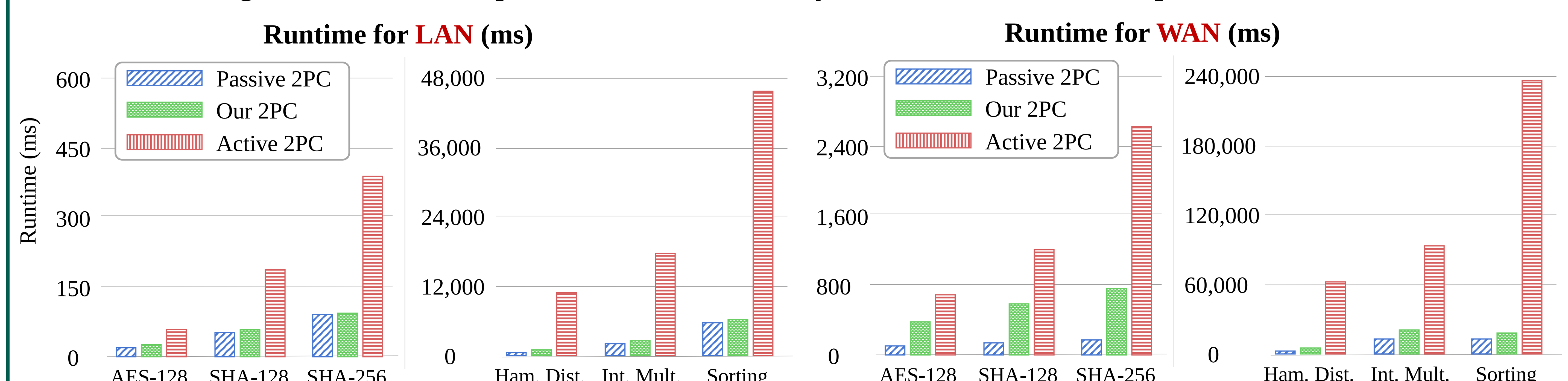
$$\left.\begin{aligned}(L_{w,0} \oplus \lambda_w \Delta_A) \oplus (L_{w,\hat{z}_w}) &= z_w \Delta_A \\ (L'_{w,\hat{z}'_w}) \oplus (L'_{w,0} \oplus \lambda'_w \Delta_B) &= z_w \Delta_B\end{aligned}\right\} \quad z_w\Delta_A \oplus z_w\Delta_B = z_w\Delta \text{ constitutes the corresponding } \textbf{SPDZ MAC}$$



Our approach: extending the principles behind the verification and opening of **SPDZ-style authenticated secret sharing** to support garbled output verification and progressive output revelation.

Performance

Our protocol attains runtime performance comparable to that of passively secure GC-based 2PC protocols, while exhibiting a 6.9 ~ 10.6× improvement over actively secure GC-based 2PC protocols.



To ensure a fair comparison, the experiment does not take into account the output progressive revelation, which is also of low cost.

References and QR Code for Our Paper (ePrint: 2025/614)

[HKE12] Huang Y, Katz J, Evans D. *Quid-pro-quo-tocols: Strengthening semi-honest protocols with dual execution*[C]//IEEE S&P 2012.
[ZRE15] Zahur S, Rosulek M, Evans D. *Two halves make a whole: Reducing data transfer in garbled circuits using half gates*[C]//EUROCRYPT 2015.
[RR21] Rosulek M, Roy L. *Three halves make a whole? Beating the half-gates lower bound for garbled circuits*[C]//CRYPTO 2021.