# Script for Eurocrypt 2023 Talk

## Page 1

Thanks for the introduction. I am Hongrui, and I am happy to present our recent progress on improving the communication complexity of constant-round maliciously secure 2 party computation. This is a joint work with Xiao Wang, Kang Yang, and Yu Yu.

## Page 2

### View 1

To begin with, we recall the progress on the optimization of garbled circuits. Ever since the Yao’s proposal in the 80s, there has been continuous effort improving the efficiency of the garbling scheme, and that translates to the respective progress in constant-round semi-honest 2PC, which is essentially .

### View 2

A natural question is how to boost semi-honest GC-based 2PC into malicious security, where we allow arbitrary deviation from the protocol. The state-of-the-art technique is authenticated garbling and it’s proposed by Wang et al. in CCS2017. The basic idea is to authenticate the garbling process using message authentication code, or MAC. And to generate such MACs we will need an input-independent preprocessing protocol. The online phase is essentially semi-honest GC evaluation plus consistency checking.

### View 3

In the original WRK17, the preprocessing functionality is instantiated via an optimized TinyOT protocol while in a subsequent paper by the same group of authors an online protocol matching the communication complexity of semi-honest half-gates was proposed.

### View 4

Afterwards, generating OT-like correlations has been significantly improved by numerous pseudorandom correlation generators based on Learning Parity with Noise. In particular, they allow generating such triples using sublinear communication and linear computation. A natural idea is to try to optimize the preprocessing protocol for authenticated garbling using PCGs. Dittmer et al. studied that idea in Crypto 2022 and achieved bits per AND gate in the correlated OT hybrid model and bits per AND gate in the multiplication triple hybrid model. The improvement is significant compared to previous TinyOT-style protocols, but we can see there is still a gap between the semi-honest world and the malicious world.

### View 5

A natural question is can we bridge such a gap?

## Page 3

Here we list the main contributions of our work in this table. In this work we manage to achieve essentially the same one-way communication as semi-honest half-gates, and as for total communication we achieve about 34% improvement over previous state-of-the-art. Since one-way communication is more relevant in the full-duplex network, and hence the title “Actively Secure Half-Gates with Minimum Overhead under Duplex Networks”. Now let me try to convey to you the essential ideas of this work for the rest of this talk.

## Page 4

### View 1

Let’s start by recalling the garbling notations in the good-old semi-honest GC-based circuit evaluation protocol. In this scheme the garbler first prepares random mask and labels for each wire, subject to the constraint that the 0-label and 1-label on each wire XOR to a fixed random string. We use small lambda for wire masks and capital lambda for the masked wire values. The garbler first sends the garbled truth tables for each AND gate to the evaluator, which can be done even before the specific inputs are known.

### View 2

Then the garbler sends the labels and masked wire values to the evaluator, specifically since Bob’s inputs need to be protected, we need to use oblivious transfer for his input labels.

### View 3

Now the evaluator uses the input information to evaluate the circuit topologically. For each AND gate the garbler decrypts the table entry that corresponds to its masked input values, and gets the output wire label. Typically, the masked output wire value is acquired by extracting the least significant bit of the output label, but any other position suffices.

### View 4

Since