**Meenakshi Nagarajan**

# DUPLO: Unifying Cut-and-Choose for Garbler Circuits

**Research problem and its importance**

Secure two-party computation is a protocol which ensures two parties to communicate securely for their inputs on a random function. Yao's garbled circuit protocol helps in achieving the secure two party computation by distorting the random function which has to be designed as a Boolean circuit. Traditional cut and choose protocol applies randomized noise to the entire circuits at a macroscopic level which may allow adversaries to understand the arbitrary function. LEGO paradigm on garbled circuit introduces more random noise by adding more gates which improves privacy but compromises on computation cost in soldering circuits. This paper talks about developing an efficient method to cut down computation costs of evaluating garbled circuits by taking a centric approach between those two paradigms.

**Technical challenges of the problem**

There are two leading challenges in Cut and Choose two party computation. First challenge in normal Cut and choose method is the replication factor. Three times the number of sub components are replicated to preserve privacy which adds to computation cost in assembly. The Second challenge is in LEGO technique where the number of NAND gates generated to garble an identical functionality are huge. This NAND gate addition adds extra cost overhead in soldering on evaluation phase. Finding a common ground in cut and choose will help in evaluating the required circuits thereby saving computation time to obtain the resulting function.

**Proposed approach**

In this paper, they have adopted a methodology by generalizing C&C to unlock a new degree of freedom by having reduced to no impact on the number of subcomponents involved in replication factor. All critical computations are expressed in terms of moderate sized components which can still perform two party secure computations operating on varied different typed of arbitrary functions. In function-independent phase independent subroutines are analyzed and garbled. Cut and choose happens on the generated garbled functions across both parties. In function-dependent phase chosen garbled functions are soldered. In online phase inputs are applied upon the soldered functions to evaluate other party's results.

**Strengths of the approach**

- Real time integration with compiler Frigate.
- Increase in subcomponent size has reduced effect in computation using parallel processing
- Increases efficiency of multiple joint computation intensive functions like Mat-Mul, CMAC etc.
- Faster amortization time.

**Possible weaknesses**

- For reduced N-value, this approach provides similar results as compared to other GC cut and choose approaches.
- Scalability of larger systems are limited as functions are restricted in representation by combinatorial circuits.[1]

References

1. https://repository.library.northeastern.edu/files/neu:cj82rh04k/fulltext.pdf