Value collision multi party computing via multiple graph topologies

Péter Hudoba, Péter Burcsi

Eötvös Loránd University, Department of Computer Algebra
peter.hudoba@inf.elte.hu, bupe@inf.elte.hu

Abstract

Keywords: multi party computation, socialist millionaire problem, graph

In computer science, there is a need for protocols that determine the equality of secrets. A motivating example is when we want to know whether we have unique identifiers in a network. Formally, we have n actors, all of them have their own secrets, and we want to determine if is there a collision between their values without revealing the secrets themselves to the others.

If we consider the two-participant scenario, there are efficient solutions the security of which depend on the hardness of the discrete logarithm problem, but these approaches ususally only consider the two-participant case. General constructions exist that prove the existence of a secure multi-party computation for several participants, but we would like to construct a scheme that is more efficient in terms of computation and communication.

In previous work, we suggested multiple approaches to achieve a general protocol. One of the approaches is based on additive secret sharing. Every participant splits their secret into multiple fragments and shares it by some other actors in the network, determined by a graph pattern.

In this talk we investigate this specific approach and talk about possible graph patterns and their comparison.

Acknowledgement

Péter Hudoba was supported by EFOP-3.6.3-VEKOP-16-2017-00001: Talent Management in Autonomous Vehicle Control Technologies | The Project is supported by the Hungarian Government and co-financed by the European Social Fund.

Péter Burcsi has been supported by the European Union, co-financed by the European Social Fund (EFOP-3.6.2-16-2017-00013, Thematic Fundamental Research Collaborations Grounding Innovation in Informatics and Infocommunications).

References

[1] Hudoba, P.; Burcsi, P., Multi party computation motivated by the birthday problem, *Acta Cybernetica*, 2019, 24.1: 29-41.