Encrypted Fast Covariance Intersection on the Cloud Without Leaking Weights

Marko Ristic[1] and Benjamin Noack[1]

***Abstract*— Abstract**

I. Introduction

II. Problem Statement

III. Preliminaries

A. Fast Covariance Intersection

B. Paillier Encryption Scheme

C. Integer Encoding for Homomorphic Encryption

IV. Encrypted Fast Covariance Intersection

V. Security Analysis

VI. Simulation and Results

VII. Conclusion

[1] Marko Ristic and Benjamin Noack are with the Autonomous Multisensor Systems Group (AMS), Institute for Intelligent Cooperating Systems (ICS), Otto von Guericke University (OVGU), Magdeburg, Germany {marko.ristic, benjamin.noack}@ovgu.de