Cryptology ePrint Archive: Report 2011/122

Secure Multi-Party Sorting and Applications

Kristj{\'a}n Valur J{\'o}nsson and Gunnar Kreitz and Misbah Uddin

Abstract: Sorting is among the most fundamental and well-studied problems within computer science and a core step of many algorithms. In this article, we consider the problem of constructing a secure multi-party computing (MPC) protocol for sorting. Our protocol builds on previous work in the fields of MPC and sorting networks.

Apart from the immediate uses for sorting, our protocol can be used as a building-block in more complex algorithms. We present a weighted set intersection algorithm, where each party inputs a set of weighted elements and the output consists of the input elements with their weights summed. As a practical example, we apply our protocols in a network security setting for aggregation of security incident reports from multiple reporters, specifically to detect stealthy port scans in a distributed but privacy preserving manner. Both sorting and weighted set intersection use $\Ordo{n \log^2 n}$ comparisons in $\Ordo{\log^2 n}$ rounds with practical constants.

Our protocols can be built upon any secret sharing scheme supporting multiplication and addition. We have implemented and evaluated the performance of sorting on the Sharemind secure multi-party computation platform, demonstrating the real-world performance of our proposed protocols.

Category / Keywords: cryptographic protocols / Secure multi-party computation; Sorting; Aggregation; Cooperative anomaly detection

Date: received 10 Mar 2011, last revised 4 Nov 2011

Contact author: gkreitz at kth se

Available formats: PDF | BibTeX Citation

Note: Added more references to related work.

Version: 20111104:095651 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]