Cryptology ePrint Archive: Report 2011/200

Fair and Privacy-Preserving Multi-Party Protocols for Reconciling Ordered Input Sets (Extended version)

Georg Neugebauer and Ulrike Meyer and Susanne Wetzel

Abstract: In this paper, we introduce the first protocols for multi-party, privacy-preserving, fair reconciliation of ordered sets. Our contributions are twofold. First, we show that it is possible to extend the round-based construction for fair, two-party privacy-preserving reconciliation of ordered sets to multiple parties using a multi-party privacy-preserving set intersection protocol. Second, we propose new constructions for fair, multi-party, privacy-preserving reconciliation of ordered sets based on multiset operations. We prove that all our protocols are privacy-preserving in the semi-honest model. We furthermore provide a detailed performance analysis of our new protocols and show that the constructions based on multisets generally outperform the round-based approach.

Category / Keywords: cryptographic protocols / secure multi-party computation, reconciliation protocols, privacy

Publication Info: G. Neugebauer, U. Meyer, S. Wetzel: Fair and Privacy-Preserving Multi-Party Protocols for Reconciling Ordered Input Sets, 13th Information Security Conference (ISC), October 2010

Date: received 20 Apr 2011

Contact author: neugebauer at umic rwth-aachen de