Cryptology ePrint Archive: Report 2011/509

Policy-Enhanced Private Set Intersection: Sharing Information While Enforcing Privacy Policies

Emil Stefanov and Elaine Shi and Dawn Song

Abstract: Companies, organizations, and individuals often wish to share information to realize valuable social and economic goals. Unfortunately, privacy concerns often stand in the way of such information sharing and exchange.

This paper proposes a novel cryptographic paradigm called Policy-Enhanced Private Set Intersection (PPSI), allowing two parties to share information while enforcing the desired privacy policies. Our constructions require minimal additional overhead over traditional Private Set Intersection (PSI) protocols, and yet we can handle rich policy semantics previously not possible with traditional PSI and Authorized Private Set Intersection (APSI) protocols. Our scheme involves running a standard PSI protocol over carefully crafted encodings of elements formed as part of a challenge-response mechanism. The structure of these encodings resembles techniques used for aggregating BLS signatures in bilinear groups. We prove that our scheme is secure in the malicious model, under the CBDH assumption, the random oracle model, and the assumption that the underlying PSI protocol is secure against malicious adversaries.

Category / Keywords: cryptographic protocols / authorized private set intersection; multiple authorities; rich

Date: received 16 Sep 2011

Contact author: emil at berkeley edu

Available formats: PDF | BibTeX Citation

Version: 20110918:024650 (All versions of this report)

Discussion forum: Show discussion | Start new discussion

[Cryptology ePrint archive]