Hong, Jeongdae; **Kim, Jung Woo**; **Kim, Jihye**; **Park, Kunsoo**; **Cheon, Jung Hee**
Constant-round privacy preserving multiset union. (English) Zbl 1310.94152
Bull. Korean Math. Soc. 50, No. 6, 1799-1816 (2013).

Summary: Privacy preserving multiset union (PPMU) protocol allows a set of parties, each with a multiset, to collaboratively compute a multiset union *secretly*, meaning that any information other than union is not revealed. We propose efficient PPMU protocols, using multiplicative homomorphic cryptosystem. The novelty of our protocol is to directly encrypt a polynomial by representing it by an element of an extension field. The resulting protocols consist of constant rounds and improve communication cost. We also prove the security of our protocol against malicious adversaries, in the random oracle model.

MSC:

94A60 Cryptography

Keywords:

privacy preserving multiset union; ElGamal on polynomials; homomorphic encryption

Full Text: DOI Link