Afanas'eva, A. V.; Balakirskiĭ, V. B.; Bezzateev, S. V.
Private information retrieval protocol. (Russian. English summary) Zbl 07397144
Mat. Vopr. Kriptografii 6, No. 4, 5-21 (2015)

Summary: A new computationally efficient private information retrieval protocol is proposed. It is based on coset properties of Galois groups of the field GF($q$) finite extensions. The proposed protocol has communication complexity slightly worse than the best known schemes based on locally decodable codes and it may be constructed for any system parameters (as opposed to codes). In comparison with similar solutions based on polynomials the computational complexity of our method is smaller which is important especially for servers processing multiple requests from multiple users.

MSC:
68P20 Information storage and retrieval of data
94A60 Cryptography

Keywords:
private information retrieval protocol; polynomial interpolation; coset; Galois groups; finite fields

Full Text: DOI MNR

References:

This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original
paper as accurately as possible without claiming the completeness or perfect precision of the matching.