**Afanas'eva, A. V.**; **Balakirskiĭ, V. B.**; **Bezzateev, S. V.**
**Private information retrieval protocol.** (Russian. English summary) Zbl 1472.68049
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:**

[1] Woodruff D., Yekhanin S., "A geometric approach to information-theoretic private information retrieval", SIAM J. Comput., 37:4 (2007), 1046-1056 · Zbl 1156.68019 · doi:10.1137/06065773X

[2] Chor B., Kushilevitz E., Goldreich O., Sudan M., "Private information retrieval", Proc. 36th Annu. IEEE Symp. on Foundations of Computer Science, 1995, 41-50 · Zbl 0938.68625 · doi:10.1109/SFCS.1995.492461

[3] Chor B., Gilboa N., "Computationally private information retrieval", 29th STOC, 1997, 304-313 · Zbl 0962.68054

[4] Kushilevitz E., Ostrovsky R., "Replication is not needed: Single database, computationally-private information retrieval", Proc. of the 38th Annu. IEEE Symp. on Foundations of Computer Science, 1997, 364-373· doi:10.1109/SFCS.1997.646125

[5] Ostrovsky R. et al., Method and apparatus for private information retrieval from a single electronic storage device, US Patent 6167392

[6] Cachin C., Micali S., Stadler M., "Computationally Private Information Retrieval with Polylogarithmic Communication", Proceedings of EUROCRYPT' 99, Lect. Notes Comput. Sci., 1592, 1999, 402-414 · Zbl 0932.68042 · doi:10.1007/3-540-48910-$X_28$

[7] Gentry C., Ramzan Z., "Single-database private information retrieval with constant communication rate", ICALP: Annu. Int. Colloq. on Automata, Languages and Programming, 2005, 803-815 · Zbl 1084.68043

[8] Ramzan et al., Method and apparatus for communication efficient private information retrieval and oblivious transfer, US Patent 8065332 B2

[9] Groth J., Kiayias A., Lipmaa H., "Multi-query computationally-private information retrieval with constant communication rate", Practice and Theory in Public Key Cryptography - PKC 2010, Lect. Notes Comput. Sci., 6056, 2010, 107-123 · Zbl 1279.94080 · doi:10.1007/978-3-642-13013-$7_7$

[10] Melchor C. A., Gaborit P., A lattice-based computationally-efficient private information retrieval protocol,

[11] Beimel A., Ishai Y., Kushilevitz E., "General constructions for information-theoretic private information retrieval", J. Comput. Syst. Sci., 71 (2005), 213-247 · Zbl 1076.68027 · doi:10.1016/j.jcss.2005.03.002

[12] Beimel A., Ishai Y., Kushilevitz E., Raymond J., "Breaking the \(O(n^{1/(2k-1)})\) barrier for information-theoretic private information retrieval", 43rd IEEE Symposium on Foundations of Computer Science (FOCS), 2002, 261-270· doi:10.1109/SFCS.2002.1181949

[13] Yekhanin S., "Locally decodable codes", Foundations and Trends in Theoretical Computer Science, 7:1 (2011), 1-117 · Zbl 1271.94031

[14] Mak-Vilyams F. Dzh., Sloen N. Dzh., Teoriya kodov, ispravlyayuschikh oshibki, Svyaz, M., 1979

[15] Landau E., Handbuch der Lehre yon der Verteilung der Primzahlen, v. 1, Reprinted in 1953 by Chelsea Publishing Co., New York, Teubner, Leipzig, 1909

[16] Rosser J. B., Schoenfeld L., "Approximate formulas for some functions of prime numbers", Illinois J. Math., 6:1 (1962), 64-94 · Zbl 0122.05001

[17] Shennon K., Raboty po teorii informatsii i kibernetike, Inostr. lit., M., 1963