

Cryptology ePrint Archive: Report 2011/595

Efficient Multi-Query C_{PIR} from Ring-LWE

Helger Lipmaa

Abstract: We propose an (n, m) -computationally-private information retrieval (C_{PIR}) protocol with rate $1 - o(1)$ and highly nontrivial (sublinear and data-dependent) server's computational complexity. For this, we note that an (n, m) -C_{PIR} protocol is equivalent to a secure function evaluation protocol that evaluates a secret function f on m different inputs. Thus, we first design an efficient multi-level circuit for f and then use the recent (ring-)LWE based fully-homomorphic encryption scheme by Brakerski, Gentry and Vaikuntanathan [cite {eprint2011:BrakerskiGV}] to evaluate the circuit in a private manner. Apart from the final result itself, several of our techniques may be of independent interest. This includes the construction of the circuit for f and the definition and construction of computational batch codes.

Category / Keywords: cryptographic protocols / Circuit complexity, compressed constant-weight codes, computational batch codes, C_{PIR}, parallel computation, ring-LWE

Date: received 25 Oct 2011, last revised 3 Nov 2011

Contact author: helger lipmaa at gmail com

Available formats: [PDF](#) | [BibTeX Citation](#)

Note: The rest of this paper is from Autumn 2010, but this version is based on the new eprint by Brakerski et al.

Version: 20111103:120540 ([All versions of this report](#))

Discussion forum: [Show discussion](#) | [Start new discussion](#)

[[Cryptology ePrint archive](#)]