

Cryptology ePrint Archive: Report 2013/003

On Formal Expressions of BRW-polynomials

Guillermo Morales-Luna

Abstract: Algebraic expressions of the Bernstein-Rabin-Winograd-polynomials, when defined over the field of the rational numbers, are obtained by recursion.

Category / Keywords: cryptographic protocols / authentication codes, hash functions, identification protocols

Date: received 3 Jan 2013

Contact author: gmorales at cs cinvestav mx

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

Version: 20130105:135706 ([All versions of this report](#))

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

[[Cryptology ePrint archive](#)]