{tag}

{/tag}

International Journal of Computer Applications

Volume 54 - Number 15

Year of Publication: 2012

Authors:

P. Anuradha Kameswari

R. Chaya Kumari

10.5120/8639-2054

{bibtex}pxc3882054.bib{/bibtex}

Abstract

In this paper, two cryptosystems are constructed using the fact that Rédei rational functions are permutation polynomials and exploiting the multiplicative properties of Rédei rational functions and the inverse property of Dickson polynomial extended to Rédei rational functions. The encryptions are based on evaluating Rédei rational functions with the values connected to the solutions of the Pell's equation in . The connection between these evaluations and the convergents of solutions of Pell's equation are used in the construction of the second cryptosystem.

References

- A. K. Bhandari, The public key cryptography. Proceedings of the advanced instructional workshop on Algebraic number theory, HBA (2003)287-301.
- J. Buchmann, Introduction to cryptography , Springer-Verlag 2001.
- W. S. Chou, The factorization Dickson polynomials over finite fields, Finite fields Appl. 3,1997.
- S. D. Cohen, Dickson permutations in Number-theoritic and Algebraic methods in

computer science. Moscow, 1993.

- M. Fried-R. Lidl, On Dickson Polynomials And Rédei Function, Contributions to general algebra 5, Proceedings of the Salzburg conferene, Mai29-june1,1986.
- Hans Lausch and Wilfried Nobauer, Algebra of Polynomials, North Holland publishing company-1973.
- M. jacobson, W. Hugh, Solving the pell equation, CMS Books in mathematics, canadian mathematical society, 2009.
- F. Lemmermeyer, Higher descent on Pellconics. III. The first 2-descent, available on http://arxiv. org/abs/math/0311310v1,2003.
- Lenstra H. W Jr. Solving the pell equation. Notice of AMS v. 49 no. 2 186-192 (2002).
- Neal Koblitz, A course in number theory and cryptography. ISBN 3-578071-8,SPIN 10893308 .
- Nobauer Wilfried, Uber Permutationspolynome und Permutationsfunktionen fur Primzahlpotenzen.
- Rudolf Lidl and Winfried B. Muller, Permutation polynomials in RSA cryptosystems, Springer-Verlag(1998).
- Sahadeo Padhye, A Public key cryptosystem based on pell equation.
- Stefano Barbero, Umberto Cerruti and Nadir Murru, Solving the Pell Equation via Rédei rational functions.
- Wilfried B. Muller and Rupert Nobauer, Cryptanalysis of the dickson scheme.

Index Terms

Computer Science Applied Mathematics

Keywords

Pell conics Redei Rational function Permutation Polynomial Cryptosystem