A New Public Key Encryption System Based on Permutation Polynomials

Publisher: IEEE

Gurgen Khachatrian ; Melsik Kyureghyan **All Authors**

Abstract: In this paper a new public key encryption and digital signature system based on permutation polynomials is developed. The permutation polynomial P(x) is replaced by P(xi)... **View more**

Metadata

Abstract:
In this paper a new public key encryption and digital signature system based on permutation polynomials is developed. The permutation polynomial P(x) is replaced by P(xi) mod g(x) where g(x) is a secret primitive polynomial, i is the secret number such that (i, 2n-1) =1 and P(xi) = Pi(x) is declared to be a public polynomial for encryption. A public key encryption of given m(x) is the evaluation of polynomial Pi(x) at point m(x) where the result of evaluation is calculated via so called White box reduction, which does not reveal the underlying secret polynomial g(x). It is shown that for the new system to achieve a comparable security with conventional public key systems based on either Discrete logarithm or Integer factorization problems, substantially less processing length n is required resulting in a significant acceleration of public key operations.

Published in: 2014 IEEE International Conference on Cloud Engineering

Date of Conference: 11-14 March 2014

Date Added to IEEE *Xplore*: 22 September 2014

Electronic ISBN:978-1-4799-3766-0

INSPEC Accession Number: 14615295

DOI: 10.1109/IC2E.2014.52

Publisher: IEEE

Conference Location: Boston, MA, USA

Contents

More Like This

I. Introduction

Let $GF(q)$ be the finite field with q elements, where q is a prime or power of a prime. A polynomial f(x) over $GF(q)$ is called a permutation polynomial if an equation $\mathrm{f(x)} = \mathrm{r}$ for any $r \in GF(q)$ has only one root in $GF(q)$. Permutation polynomials have been studied intensively in the past (see for example [1]–[4]) and have important applications in coding theory [1] and cryptography [3]. In this paper we will introduce a new class of permutation polynomials and will show how they can be used to design a public key system. Public-key cryptography started in 1976 with the publication of pioneering work of Diffie and Hellman [5] in which DH key exchange was presented, and in 1978 with another fundamental work by Rivest, Shamir and Adleman [6], called RSA crypto system. DH key exchange is based on discrete logarithm problem (DLP) and RSA is based on integer factorization problem. The current state of the art requires that public modulus size must be 2048 bits. Another important development for public key cryptosystems was the invention of Elliptic curve cryptosystems [7] which are also based on DLP problem, but require significantly less number of modular size, but more complex operations.

Authors
References
Citations
Keywords
Metrics