



All



ADVANCED SEARCH

Conferences > 2014 IEEE International Confe...

# A New Public Key Encryption System Based on Permutation Polynomials

Publisher: IEEE

Cite This

Cite This

PDF

Gurgen Khachatryan ; Melsik Kyureghyan All Authors

1 Paper Citation

164 Full Text Views



Export to Collabratec

Alerts

Manage Content Alerts

Add to Citation Alerts

### More Like This

Modular multiplication in the residue number system with application to massively-parallel public-key cryptography systems

Conference Record of the Thirty-Fourth Asilomar Conference on Signals, Systems and Computers (Cat. No.00CH37154) Published: 2000

Topological Public-Key Cryptography Based On Graph Image-Labelings For Information Security

2020 IEEE International Conference on Information Technology, Big Data and Artificial Intelligence (ICIBA) Published: 2020

Show More

## Abstract

### Document Sections

- I. Introduction
- II. New construction method of permutation polynomials
- III. New public key encryption and signature scheme based on permutation polynomials
- IV. White box implementation of polynomial evaluation
- V. Security analysis of the proposed system

Show Full Outline

Downl PDF

**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  $P(\xi) \bmod g(x)$  where  $g(x)$  is a secret primitive polynomial,  $\xi$  is the secret number such that  $(\xi, 2n-1) = 1$  and  $P(\xi) = P_i(x)$  is declared to be a public polynomial for encryption. A public key encryption of given  $m(x)$  is the evaluation of polynomial  $P_i(x)$  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

Authors

**Date of Conference:** 11-14 March 2014 **INSPEC Accession Number:** 14615295

References

**Date Added to IEEE Xplore:** 22 September 2014 **DOI:** 10.1109/IC2E.2014.52

Citations

**Electronic ISBN:**978-1-4799-3766-0 **Publisher:** IEEE

Keywords

**Conference Location:** Boston, MA, USA

Metrics

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  $f(x) = r$  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.

Sign in to Continue Reading

Authors

References

Citations

Keywords

Metrics

#### IEEE Personal Account

CHANGE USERNAME/PASSWORD

#### Purchase Details

PAYMENT OPTIONS

VIEW PURCHASED DOCUMENTS

#### Profile Information

COMMUNICATIONS PREFERENCES

PROFESSION AND EDUCATION

TECHNICAL INTERESTS

#### Need Help?

US & CANADA: +1 800 678 4333

WORLDWIDE: +1 732 981 0060

CONTACT & SUPPORT

#### Follow



About IEEE Xplore | Contact Us | Help | Accessibility | Terms of Use | Nondiscrimination Policy | Sitemap | Privacy & Opting Out of Cookies

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

© Copyright 2021 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions.

#### IEEE Account

» Change Username/Password

» Update Address

#### Purchase Details

» Payment Options

» Order History

» View Purchased Documents

#### Profile Information

» Communications Preferences

» Profession and Education

» Technical Interests

#### Need Help?

» US & Canada: +1 800 678 4333

» Worldwide: +1 732 981 0060

» Contact & Support

About IEEE Xplore | Contact Us | Help | Accessibility | Terms of Use | Nondiscrimination Policy | Sitemap | Privacy & Opting Out of Cookies

A not-for-profit organization, IEEE is the world's largest technical professional organization dedicated to advancing technology for the benefit of humanity.

© Copyright 2021 IEEE - All rights reserved. Use of this web site signifies your agreement to the terms and conditions.