New Directions in Multivariate Public Key Cryptography

Raymond Heindl, Clemson University

Date of Award
5-2009

Document Type
Dissertation

Degree Name
Doctor of Philosophy (PhD)

Legacy Department
Mathematical Science

Advisor
Gao, Shuhong

Committee Member
Maharaj , Hiren

Committee Member
Matthews , Gretchen

Committee Member
Xue , Hui

Abstract
Most public key cryptosystems used in practice are based on integer factorization or discrete logarithms (in finite fields or elliptic curves). However, these systems suffer from two potential drawbacks. First, they must use large keys to maintain security, resulting in decreased efficiency. Second, if large enough quantum computers can be built, Shor's algorithm will render them completely insecure.

Multivariate public key cryptosystems (MPKC) are one possible alternative. MPKC makes use of the fact that solving multivariate polynomial systems over a finite field is an NP-complete problem, for which it is not known whether there is a polynomial algorithm on quantum computers.

The main goal of this work is to show how to use new mathematical structures, specifically polynomial identities from algebraic geometry, to construct new multivariate public key cryptosystems. We begin with a basic overview of MPKC and present several significant cryptosystems that have been proposed. We also examine in detail some of the most powerful attacks against MPKCs.

We propose a new framework for constructing multivariate public key cryptosystems and consider several strategies for constructing polynomial identities that can be utilized by the framework. In particular, we have discovered several new families of polynomial identities. Finally, we propose our new cryptosystem and give parameters for which it is secure against known attacks on MPKCs.

Recommended Citation
Heindl, Raymond, "New Directions in Multivariate Public Key Cryptography" (2009). All Dissertations. 368.

https://tigerprints.clemson.edu/all_dissertations/368

New Directions in Cryptography. WHITFIELD. Invited Paper

DIFFIE AND MARTIN E. HELLMAN Public key distribution systems offer a different ap-proach to eliminating the need for a secure key distribution channel. In such a system, two users who wish to exchange a key communicate back and forth until they arrive at a key in common. A third party eavesdropping on this ex-change must find it computationally infeasible to compute the key from the information overheard, A possible solu-tion to the public key distribution problem is given in Section III, and Merkle [l] has a partial solution of a dif-ferent form. We now suggest a new public key distribution system which has several advantages. First, it requires only one "key" to be exchanged. PDF | A multivariate public key cryptosystem (MPKCs for short) have a set of (usually) quadratic polynomials over a finite field as its public map. Its main security assumption is backed by the NP-hardness of the problem to solve nonlinear equations over a finite field. This family...
Public Key Cryptography in the last two decades. Some constructions are not as secure as was claimed initially, but others are still viable. The paper gives an overview of multivariate public key cryptography and discusses the current status of the research in this area. Based cryptography provide an even wider variety of new candidates for post-quantum cryptography. Some specific proposals have been broken.