Construction of permutation polynomials and its application in Biometric authentication

Gurgen Khachatryan
AUA
Yerevan, Armenia
e-mail: gurgenkh@aua.am

Melsik Kyureghyan
IIAP
Yerevan, Armenia
e-mail: melsik@ipia.sci.am

Sergey Abrahamyan
IIAP
Yerevan, Armenia
e-mail: serj.abrahamyan@gmail.com

ABSTRACT
In this paper a construction method of permutation polynomials is developed. It is also shown how permutation polynomials can be used in Biometric authentication.

Keywords
Permutation polynomials, Biometrics, Authentication technology.

1. INTRODUCTION
Let F_q be a finite field with q elements, where q is a prime or power prime. A polynomial $f \in F_q[x]$ is called a permutation polynomial of F_q if $f(x) = a$ has one solution in F_q for every a in F_q. Permutation polynomials have been an interesting subject of study in the area of finite fields for many years. Particularly permutation polynomials have many important applications in coding theory [1], cryptography [3], and combinatorial design theory.

In section 2 a new method of construction of permutation polynomial is introduced. In section 3 how to use permutation polynomials for biometric authentication is demonstrated.

2. NEW CONSTRUCTION OF PERMUTATION POLYNOMIALS
Let's introduce some notations and definitions:

Let $F_q = F_{p^s}$ be a finite field of characteristic p.

For every permutation polynomial $f(x)$ over F_q, there exists a unique polynomial, $f^{-1}(x)$ over F_q such that $f(f^{-1}(x)) = (f^{-1}(f(x)) = x$ called the compositional inverse of $f(x)$.

Definition 1.A polynomial $F(x)$ is called a permutation polynomial of F_{q^n} if the mapping F is a permutation of F_{q^n}.

Definition 2.1.A polynomial of the form

$$L(x) = \sum_{i=0}^{n} a_i x^{q^i}$$

with coefficients in an extension field F_{q^n} of F_q is called a q-polynomial or linearized polynomial over F_{q^n}.

Theorem 2.2[2, Theorem 7.9]. Let F_q be a finite field of characteristic p. Then the polynomial

$$L(x) = \sum_{i=0}^{n} a_i x^{p^i} \in F_q$$

is a permutation polynomial of F_q if and only if $L(x)$ has one root 0 in F_q.

Theorem 2.3[4]. Let

$$f(x) = \sum_{u=0}^{n} a_u x^u \in F_q[x]$$

and $F(x)$ be its linearized q-associate. Then the polynomial $f(x)$ is a primitive polynomial over F_q if and only if the polynomial

$$x^{-1}F(x) = \sum_{u=0}^{n} a_u x^{q^u-1}$$

is irreducible over F_q.

Based on theorem 2.3 we propose a new construction method of permutation polynomials over F_q.

Let $f(x) = \sum_{u=0}^{n} a_u x^u \in F_{q^s}[x]$ be a primitive polynomial. In accordance to Theorem 2.3 we can say that polynomial

$$x^{-1}L(x) = \sum_{u=0}^{n} a_u x^{2^u-1}$$

is a irreducible polynomial. Hence $L(x) = \sum_{u=0}^{n} a_u x^{q^u}$ has one 0 root. And by Theorem 2.1 $L(x)$ is a permutation polynomial F_{2^s}.

As such given the primitive polynomial

$$f(x) = \sum_{u=0}^{n} a_u x^u$$

it is possible to construct $L(x) = \sum_{u=0}^{n} a_u x^{q^u}$ and $L(x)$ will be a permutation polynomial.

We define the weight of polynomial $f(x)$ as a number of non-zero terms of polynomial. Our target is to construct one way permutation polynomials: i.e. permutation polynomials which inverse is unknown.

Our preliminary analysis shows that the construction of inverse polynomial of $L(x)$ is a difficult problem when the weight of $L(x)$ is greater than or equal to seven. As such, having primitive polynomial of weight greater than or equal to seven is sufficient to construct one way permutation polynomial with weight greater than or equal to seven.

3. AN APPLICATION OF PERMUTATION POLYNOMIALS IN BIOMETRIC AUTHENTICATION SCHEMES

Construction of Permutation polynomials described above in fact provides a method of construction collision free one way function. This fact can be used in biometric authentication schemes as follows: Biometric information b in many cases can be considered as an element of $GF(2^n)$. Evaluation of the Permutation polynomial over biometric information b $f(b)$ can be considered as an encoded image of b and it is assumed that it would be computationally infeasible having $f(b)$ to get b. As such $f(b)$ can be considered as a reference template for the biometric information b. When using an application based on biometrics, first a reference template is generated from the biometric sample provided in the enrolment phase for later use. In the authentication phase, a new biometric sample is acquired and compared with the reference template. Hence, the application requires this reference template for a successful authentication and therefore it needs to be stored. Usually we store reference template in a centralized database. Storing unprotected biometric reference template in centralized database for each application increases the privacy risk a since we are storing as a reference encoded image of b by using permutation polynomials that risk can be ignored.

4. ACKNOWLEDGEMENT

This research has been carried out within the project "Ap-plication of Security to Biometrics and Communica-tions" sponsored by the Volkswagen Foundation.

REFERENCES

[1] Y. Laigle-Chapuy, Permutation polynomials and applications to coding theory, Finite Fields, Appl.13 (2007), 58–70.

[2] R. Lidl, Niederreiter, Finite Fields, Addison Wesley, reading, MA, 1983.

[3] J. Schwenk, K. Huber,Public key encryption and digital signatures based on permutation polynomials, Electron, Lett.34 (1998), 759–760.

[4] N. Zeirler, Linear recurring sequens, J.Soc.Ind.Appl.Math.7,(1959), 31–48.