A New Public Key Cryptography Algorithm Using Chaotic Systems and Hyperelliptic Curves.

Rodrigo Abarzúa, Ivan Jirón, Miguel Alfaro, Ismael Soto.
Departamento de Ingeniería Industrial.
Universidad de Santiago de Chile.
Av. Ecuador 3769, Santiago.
CHILE.

roabarzua@gmail.com, ivanjiron.araya@gmail.com, malfaro@lauca.usach.cl, ismael.soto@gmail.com.

Abstract
The aim of this paper is to make a contribution to the development of the new stronger cryptographic algorithm using chaotic systems and hyperelliptic curve. In this context, the Diffie-Hellman scheme is implemented with chaotic systems and ElGamal scheme is constructed with hyperelliptic curves. Furthermore, the complexity algorithm is determined for proposed algorithm. Also, this algorithm is compared with other system and BER v/s SNR curves are obtain in developed experiments.

Key-Words: -Chaos, -Synchronization of Chaotic Systems, -Hyperelliptic Curves.

1 Introduction

Modern telecommunication networks, and especially Internet and Mobile-phone networks, have tremendously extended the limits and possibilities of communications and information transmissions. Associated with this rapid development, there is a growing demand of cryptographic techniques, which has spurred a great deal of intensive research activities in the study of cryptography [2], [3]. Since 1990s, many research have noticed that there exists and interesting relationship between chaos and cryptography, many properties of chaotic systems have their corresponding counterparts in traditional cryptosystems.

There exist two main approaches of designing chaos-based cryptosystems: analog and digital. Most analog chaos-based cryptosystems are secure communication schemes designed for noisy channels based on the technique of chaos synchronization [4]. Chaos synchronization is a technique developed since 1990. Roughly speaking, it means that two identical dynamical systems, starting from different initial conditions, can be synchronized by common external signal which is coupled to the two systems [5]. It has been shown that even chaotic systems can be synchronized although the correlation between the external signal and the common dynamics still remains chaotic [5], [6], [7]. This phenomenon has been applied to private key: If two partner A and B want to exchange a secret message, A adds its message to a synchronized signal while B obtains it. Of course, A and B need a common secret (private key), namely, the algorithm and the parameters of the used identical chaotic systems.

Other side Hyperelliptic curves to be used in cryptosystems of public key [8]. This curve form a special class of algebraic curves. The most important algebraic structure is given by a quotient group called Jacobian, of the hyperelliptic curve over a finite field, this quotient group was suggested by Neal Koblitz for an cryptosystems of public key.[8], [9].

The represented idea is the following: If two partners A and B want to exchange a secret message. Of course, A and B, need a common secret key, they are obtained. Given a hyperelliptic curves C, the [10] Diffie-Hellman algorithm is used for private key generating β, this is to transforms a parameter of the chaotic system. The synchronization of chaotic systems is implemented using a common external signal [4], two identical dynamical systems the A (Master system) and B (Slave system) are synchronized and γ parameter is obtained. Then, a new type of private key is produced (β, γ), where β is generated on an Abelian Jacobian group of the hyperelliptic curves Diffie-Hellman algorithm and γ it is generated on synchronization of chaotic systems.
2 Basic Concepts

When a system presents an erratic behavior, random and sensible to the initial conditions, we say that the system has a dynamic chaotic. (Hilborn, R. [11])

2.1 Chaos

Let us consider an interval $I = [a, b] \subset \mathbb{R}$ $f : I \to I$ is function continuous [12].

Definition 1. The forward orbit of $x \in I$ is the set points

$$\text{Orby}(x) = \{x, f(x), \ldots, f^k(x), \ldots\}$$

with $f^k = f \circ \cdots \circ f$ ($k$-times) it denotes to $k$-ésima iteration of $f$.

Definition 2. The point $x_0 \in I$ is a fixed point $f$ if $f(x_0) = x_0$. The point $x$ is a period point of periodic $n$ if $f^n(x_0) = x_0$ and $f^j(x_0) \neq x_0$ for $0 < j < n$.

Observation 1. If $x_0 \in I$ is a period point periodic $n \geq 1$, then is a fixed point of $f^n$.

Example 1. The identity map $id(x) = x$ fixes all points in $\mathbb{R}$, whereas the map $f(x) = -x$ fixes the origin, while all other points have period $2$.

Example 2. The map $f(x) = x^3$ has $0, 1$ and $-1$ as fixed points and no other periodic points. The map $P(x) = x^2 - 1$ has fixed at $(1 \pm \sqrt{5})/2$, while the points $0$ and $-1$ lie on a periodic orbit of period $2$.

Observation 2. If $x_0 \in I$ is a point fixed $f$, will say that $x_0$ is:

1. attractor if $|f'(x_0)| < 1$.
2. repulsor if $|f'(x_0)| > 1$.
3. indifferent if $|f'(x_0)| = 1$.
4. superattractor de $f$ if $f'(x_0) = 0$ (it is to say a point I critic of $f$).

There are many possible definitions of chaos, ranging from measure theoretic notions of randomness in ergodic theory to the topological approach we will adopt here.

Definition 3. If $f : I \to I$ is said topologically transitive, or simply transitive, if for any pair of open sets nonempty $U, V \subset I$, there exists $k > 0$ so that $f^k(U) \cap V \neq \emptyset$.

The following theorem characterizes the transitive of simple form.

Theorem 1. If $I \subset \mathbb{R}$ a close interval and $f : I \to I$, then $f$ is transitive if and single if it has it orbits dense.

Definition 4. If $I \subset \mathbb{R}$ $y' : I \to I$. We say $f$ that it has sensitive dependency to its initial conditions if it exists $\epsilon > 0$ so that for nobody $x_0 \in I$ and any extended interval $U \subset I$ containing $x_0$, it exists $y_0 \in U$ and $k \in \mathbb{N}$ so that $|f^k(x_0) - f^k(y_0)| \geq \epsilon$.

With all the previous concepts we can give a formal definition of chaos

Definition 5. If $I = [a, b] \subset \mathbb{R}$. We say that an application $f : I \to I$, if chaotic is

1. $f$ es transitive.
2. The set of the points periodic of $f$ is dense in $I$.
3. $f$ has sensitive dependency to the initial conditions.

The following theorems characterizes the formal chaotic systems.

Theorem 2. (M. Vellekoop 1994) If $f : I \to I$ a application continuous in $I \subset \mathbb{R}$ it is an interval, not necessarily finite. If $f$ transitive, then the periodic orbit set of $f$ is in $I$, then $f$ es chaotic.

Theorem 3. (J. Banks 1992) If $I \subset \mathbb{R}$ an interval and $f : I \to I$ a continuous map. If $f$ is transitive and the set of orbit periodic of $f$ is dense in $I$, then it has sensitive dependency to the initial conditions.

Theorem 4. If $I \subset \mathbb{R}$ a interval open $f : I \to I$ a continuous map. Let us suppose that for any pair of close intervals $U \cap V$ content in $I$, a positive whole number exists $n$ so that $f^n(U) \supset V$, then $f$ in chaotic if $I$.

Example 3. The map $F_4(x) = 4x(1 - x)$ is chaotic in $I = [0, 1]$.

2.2 Synchronization of Chaotic Systems

In the 1990 L. M. Pecora y T. L. Carroll published [5] an unexpected result. Two chaotic dynamical systems were to prove synchronization that begin with different initial conditions.

In which it follows we will give to a general concept of the result [4]:

Given to two dynamic systems with initial different, denominated masterful system from the system 1 which excites to enslaved denominated system 2 by a signal.

Then to demonstrated that system 2 follows system 1 asymptotic.

Example 4. Given the dynamic system of Lorenz (Masterful)

$$x'_1 = \alpha(y_1 - x_1)$$
$$y'_1 = \beta x_1 - y_1 - x_1 z_1$$
$$z'_1 = x_1 y_1 - \gamma z_1$$
We defined the dynamic system of Lorenz (Enslaved) dice by:

\[
\begin{align*}
    x_2' &= \alpha(y_2 - x_2) \\
    y_2' &= \beta x_1 - y_2 - x_1 z_2 \\
    z_2' &= x_1 y_2 - \gamma z_2
\end{align*}
\]

To demonstrated that \( y_1 = y_2; \ z_1 = z_2 \) which denominates synchronization of the systems masterful and enslaved. Where \((\beta, \gamma)\) secret key.

2.3 Hyperelliptic Curves

Another one of the technics used in Cryptography are the fields generated on the hyperelliptic curves. In 1989 N. Koblitz [8] create a cryptography system based on this mechanism is based on solving a problem mathematically hard call the problem of the discreet logarithm in a finite group \( G \).

To been able to demonstrate that one curves hyperelliptic \( C \) on a finite field \( K \) she is safe must satisfy [13]:

1. Arithmetic in the underlying finite field \( K \) should be efficient to implement; finite fields of characteristic 2 appear to be the most attractive choice.

2. The order of Jacobiano \( J(K) \) of \( C \), denoted by \( \sharp J(K) \), should be divisible by a large prime number. Given the current state of computer technology, a security requirement is that \( \sharp J(K) \) es divisible by a prime number \( r \) of at least 45 decimal digits. In addition, to avoid the reduction attack of Frey and R"uck [14] which reduces the logarithm problem in \( J(K) \) to the logarithm problem in an extension of \( K = \mathbb{F}_q \), \( r \) should not divide \( q^k - 1 \) for all small \( k \) for which the discrete logarithm problem in \( \mathbb{F}_q^k \) es feasible (\( 1 \leq k \leq 2000/(\log_2 q) \) surfaces)

3 Study Case

The hyperelliptic curve \[2\]

\[ C : v^2 + uv = u^5 + 5u^4 + 6u^2 + u + 3 \]

over the field \( F_7 = \{0, 1, 2, 3, 4, 5, 6\} \) with genus \( g = 2 \).

Using a theorem of characterization of the divisor of a hyperelliptic curve it is obtained

\[ a(u) = u^4 + 2u^2 + 4 \quad b(u) = 6u^3 + 4u^2 + 3u + 2, \]

These polynomials we can represent them clearly like the vectors

\[ a = [1, 0, 2, 0, 4] \quad b = [0, 6, 4, 3, 2] \]

and these vectors we can mapping in \( \mathbb{R} \) whit

\[ \varphi(a, b) \geq 28 \]

where chaos for Lorenz is known that it exists, example \( \beta = 28 \) parameters secret. Given the dynamical system of Lorenz(Master) the A whit three parameters of the system \( \alpha, \beta, \gamma \).

\[
\begin{align*}
    x_1' &= \alpha(y_1 - x_1) \\
    y_1' &= \beta x_1 - y_1 - x_1 z_1 \\
    z_1' &= x_1 y_1 - \gamma z_1
\end{align*}
\]

the defined enslavedodynamical system like the B.

\[
\begin{align*}
    x_2' &= \alpha(y_2 - x_2) \\
    y_2' &= \beta x_1 - y_2 - x_1 z_2 \\
    z_2' &= x_1 y_2 - \gamma z_2
\end{align*}
\]

To demonstrated that \( y_1 = y_2; \ z_1 = z_2 \) which denominates synchronization of the master and enslaved systems. It is to say B obtained the parameter. Then, a new type of private key is produced \((\beta, \gamma)\), where \( \beta \) is generated on an Abelian Jacobian group of the hyperelliptic curves Diffie-Hellman algorithm and \( \gamma \) it is generated on synchronization of chaotic systems.

4 References


**Acknowledgements** The authors would like to thank pbct/conicyt act 11/04 - Chile for their financial support.