International Journal of Cryptology Research 1(2): 149-163 (2009)

AA_{β}-Cryptosystem: A Chaos Based Public Key Cryptosystem

[1]M.R.K. Ariffin and [2]N.A. Abu
[1]Al-Kindi Cryptography Research Laboratory,
Laboratory of Theoretical Studies,
Institute for Mathematical Research,
Universiti Putra Malaysia, 43400 UPM, Serdang, Selangor, Malaysia
[2] Department of Computer Systems and Communication,
Faculty of Information and Communication Technology,
Universiti Teknikal Malaysia Melaka,
76109 Durian Tunggal, Melaka, Malaysia
E-mail: [1]rezal@math.upm.edu.my, [2]nura@utem.edu.my

ABSTRACT

We describe the AA_{β}-cryptosystem, a new public key cryptosystem that is built by utilizing the classical one-way chaotic beta-transformation mapping given by $f_{\beta} = \beta x (\mathrm{mod}\ 1)$. The AA_{β}-cryptosystem represents its private keys as a vector $\overrightarrow{dA}$ and uses the parallelogram law to prove that encryption and decryption does indeed occur. The mathematical hard problem for this system is likely to be harder than the classical Discrete Log Problem and to some extent probably equal or slightly better than the Elliptic Curve Discrete Log Problem (ECDLP). With the correct choice of α, β and generator point $X(0)$, the generator point $X(0)$ when iterated via the AA_{β} function will have an order (i.e. period/cycle) of 2^{k-1} where k is the length of the private key. Because of this fact, the AA_{β}-Cryptosystem maybe more secure than the Elliptic Curve Cryptosystem (ECC).

Keywords: beta-transformation, chaotic map, asymmetric cryptography

INTRODUCTION

Noise like and deterministic features of chaotic maps make it a good mathematical candidate to be utilized as a cryptosystem. Since the 1990's attempts have been made to design cryptosystems that are based on chaotic maps. The work by Alvarez and Li [1] describes a comparison table between chaos and cryptographic properties. We list back the properties here.

TABLE 1

No.	Chaotic property	Cryptographic property	Description
1.	Ergodicity.	Confusion.	The output has the same distribution for any input.
2.	Sensitivity to initial conditions / control parameter.	Diffusion with a small change in the plaintext / secret key.	A small deviation in the input can cause a large change at the output.
3.	Mixing property.	Diffusion with a small change in one plain-block of the whole plaintext.	A small deviation in the local area can cause a large change in the whole space.
4.	Deterministic dynamics.	Deterministic pseudo – randomness.	A deterministic process can cause a random-like (pseudo-random) behavior.
5.	Structure complexity.	Algorithm (attack) complexity.	A simple process has a very high complexity.

Other characteristics that make chaotic maps an excellent candidate for cryptosystems are that initial distance between 2 arbitrary points will increase after n iterations (we will discuss more about this in section 2) and that the periodic points of a chaotic map f are repelling. That is, if a trajectory $x(k)$ happens to come close to a periodic cycle for some k, it will separate from it for indices greater than k.

Most cryptosystems that are designed by utilizing the chaotic maps are symmetric. Their characteristics that are sensitive to initial conditions and their spreading out of trajectories over the whole interval seems to be a model that satisfies the classic Shannon requirements of confusion and diffusion, which are fundamental in designing symmetric cryptosystems . Among techniques that are notable in designing symmetric cryptosystem based on chaotic maps are the Masuda and Aihara technique [10] which discritizes a chaotic map. The Yi, Tan and Siew technique [16] that re-defines the chaotic map and the Baptista cryptosystem [2], [3], [12], [13] that utilizes the ergodic property of a chaotic map.

Attempts have also been made to design asymmetric cryptosystems based on chaotic maps. Notable designs are by Kocarev and Tasev, which is based on the Chebyshev polynomials [8]. However, it has been cryptanalyzed by Bergamo [4]. In 2004 Kocarev, proposed an RSA-like encryption algorithm– based on torus automorphisms and is claimed to be as secure as RSA [9]. In 2005 Klein et al. designed a key-exchange protocol that comprises two parties with chaotic dynamics that are mutually coupled

and undergo a synchronization process [6]. In 2005 Bose utilized multiple chaotic systems and a set of linear maps for key exchange [5]; and it has been cryptanalyzed by Wang et.al [15] and Zhang [17]. Tenny and Tsimring used distributed nonlinear dynamics for designing a public-key encryption scheme [14]. They adopted synchronization of chaos but could not put forward a realistic example.

It is important in attempting to design an asymmetric cryptosystem based on chaotic maps to include discussions regarding additional advantages over current asymmetric cryptosystems based on number theoretic principles. A formal hard mathematical problem must be stated in order for further research to justify the claim. Another integral part of discussion is the minimum key size needed for the asymmetric cryptosystem to be secure. Key size is an important element of discussion to make the asymmetric cryptosystem based on chaotic maps under scrutiny relevant in terms of implementation. Much has been said about the advantages of the Elliptic Curve Cryptosystem (ECC) that employs a key at minimum length of 160-bits. Introduced by Koblitz [7], the small key length makes it advantageous over RSA (which needs keys with a minimum length of 1024-bits) when attempting to deploy security on an environment with limited processing power, storage space and power consumption.

In this paper, we propose an asymmetric cryptosystem based on the chaotic beta-transformation. In section 2, we discuss the Lyapunov Exponent which describes chaos for a given map. In section 3 we will describe the beta transformation and some underlying mathematical results related to it. In section 4, we describe the AA_β cryptosystem on the continuum $(0,1)$. We also describe the underlying hard mathematical problem which forms the basis of this asymmetric cryptosystem. The reader will also be able to observe the simplicity of the mathematical operations involved in the cryptosystem. Simplicity of the encryption and decryption operation should have overwhelming impacts on the performance of this cryptosystem when implemented. In section 5, we show that the AA_β function under minimum conditions is a one-to-one function. Finally, in section 6 we conclude the paper.

THE LYAPUNOV EXPONENT

Let us observe 2 arbitrary points x_0 and $x_0 + \Delta x_0$. These 2 points will generate an orbit based on a mapping or a system of mappings. We will assume that the orbit will take a function which utilizes time as its parameter. If we take one of the points to be the reference point, the divergence between

those 2 points could also be assumed as a function which utilizes time as its parameter.

The Lyapunov Exponent given by

$$\lambda = \lim_{\substack{t\to\infty \\ \Delta x_0 \to 0}} \frac{1}{t} \ln \frac{|\Delta x(x_0, t)|}{\Delta x_0}$$

determines whether the orbits of a certain mapping exhibits chaotic feature or not. If $\lambda > 0$ the orbits produced by the mapping exhibits chaotic effects.

Let us consider a one-dimensional dynamical system $f: I \to I$. When $\lambda > 0$, for every $\varepsilon > 0$, there exists $n_1, n_2 \in \mathbb{N}$, there exists $x \in U_{n_1,n_2}$, and for every $n \in [n_1, n_2]$, for every $z_1, z_2 \in U_{n_1,n_2}$, we have $\exp\{(\lambda - \epsilon)n\}|z_1 - z_2| < |f^n(z_1) - f^n(z_2)| < \exp\{(\lambda - \epsilon)n\}|z_1 + z_2|$.

This means that the initial distance $|z_1 - z_2|$ between 2 arbitrary points z_1, z_2 (which are elements of the neighborhood U_{n_1,n_2} of point x) after n iterations will increase by at least $\exp\{(\lambda - \epsilon)n\}$ times. If the Lyapunov exponent is either 0 or less than 0, the orbits produced by the mapping does not exhibit chaotic effects.

THE BETA-TRANSFORM

Definition 1.1

Let $\beta > 0$, the beta-transformation is given by $f_\beta(x) = \beta x (\text{mod } 1)$, where $f_\beta: (0,1) \to (0,1)$. It could also be written iteratively in the following form: $X(m+1) = \beta X(m) (\text{mod } 1)$ where $m = 0,1,2,...$ and $X(0)$ is the initial condition.

The Lyapunov exponent for the beta-transformation is given by $\lambda = \log \beta$. The Lyapunov exponent is always positive for $\beta > 0$. Thus, the orbits produced by this mapping exhibit chaotic features. For $\beta = 2$, the beta-transformation is also known as the dyadic transformation. Well known results regarding the dyadic transformation facilitates operations for other integer values of β. Observe that $x (\text{mod } 1)$ represents the fractional part of x. As an example, $3.142 (\text{mod } 1) = 0.142$. In the binary number system multiplying by 2 corresponds to the left shift by one bit and taking the fractional part corresponds to the upper bit truncation. Therefore $X(m+1)$ is the Bernoulli shift of $X(m)$. As an example (in base 2 representation) let $X(0) = 0.1010100$ ..., multiplying by 2 we will have $1.010100\ldots$. To take

the modulus we simply drop the integer part, and we have $X(1) = 0.010100\ldots$. Continuing we have $X(2) = 0.10100\ldots$. The sequence $(X(0), X(1), X(2), \ldots)$ is called the orbit of the point $X(0)$.

For any other integer value of β, the process is simply a combination of shifting the bits and adding it to the previous string of bits. In programming via C++, the multiplication library executes this process automatically. If $X(0)$ is rational, the image of $X(0)$ contains a finite number of distinct values within [0, 1) and the forward orbit of $X(0)$ is eventually periodic, with period equal to the period of the binary expansion of $X(0)$. If $X(0)$ is irrational, the image of $X(0)$ contains an infinite number of distinct values and the forward orbit of $X(0)$ is never periodic.

Within any sub-interval of [0,1), no matter how small, there are therefore an infinite number of points whose orbits are eventually periodic, and an infinite number of points whose orbits are never periodic. This sensitive dependence on initial conditions is a characteristic of chaotic maps. This is analogous to the question which arises in the RSA cryptosystem with regards to how many primes does there exist; which is answered via the Prime Number Theorem.

Theorem 1.1 (Prime Number Theorem)

Let $\pi(x)$ be the prime-counting function that gives the number of primes less than or equal to x, for any real number x. As $x \to \infty$,

$$\pi(x) \sim \frac{x}{\ln x}$$

Thus, there are enough primes for the RSA algorithm to utilize.

The analogue to the above question for the beta-transformation is: "how many orbits with large cycles are available?" It is to be noted here that the importance to have orbits with large cycles is to avoid attacks manipulating the size of the cycle.

The answer to this question is answered by the following theorem.

Theorem 1.2 (Prime Orbit Theorem for the beta-transformation. M.R.K.Ariffin [10])

Let τ be a closed orbit of the beta-transformation. Let $\kappa(\tau)$ denote the length of the orbit. Let $\pi_\beta(N) = \{\#\tau_j \mid \kappa(\tau_j) \leq N \text{ for } j = 1,2,3,\ldots\}$ denote the

number of closed orbits for the beta-transformation with a cycle less or equal to N. Then as $N \to \infty$,

$$\pi_\beta(N) \sim \frac{\beta^{N+1}}{N(\beta-1)}$$

The lower and upper bounds are given by the following Chebychev-type estimation.

Corollary 1.3 (M.R.K.Ariffin [10])

There exists constants $K_1, K_2 > 0$ such that

$$K_1 \frac{\beta^{N+1}}{N(\beta-1)} \leq \pi_\beta(N) \leq K_2 \frac{\beta^{N+1}}{N(\beta-1)}$$

THE AA_β-CRYPTOSYSTEM

We utilize the beta-transformation given by definition 3.1, to define the following AA_β function. But first we will define the set of binary strings of length k.

Definition 2.1

The set of binary strings with a length of k bits is given by $S_k^* = \left\{ s = \{b_i\}_{i=0}^k : b_i \in \{0,1\} \right\}$ where $k = 1,2,3, \ldots$.

In the AA_β-cryptosystem we will treat the binary string $s \in S_k^*$ as a vector of k-dimension. We will use the notation $\vec{s} = (b_0, b_1, b_2, \ldots, b_k)$. For $s_1, s_2 \in S_k^*$ the act of concatenating the 2 strings of binaries is the act of joining 2 vectors. From the parallelogram law we have the following diagram:

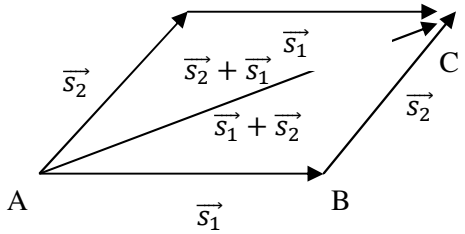


Figure 1

Example 2.1:

Let $s_1 = 11001100$ and $s_2 = 11100100$. Concatenating the 2 strings we have the following results:

$s_1 s_2 = 1100110011100100$ and $s_2 s_1 = 1110010011001100$.

Adding the 2 strings as vectors (modulo 2 addition) we have the following result:

$$\overrightarrow{s_1} + \overrightarrow{s_2} = 101000 = \overrightarrow{s_2} + \overrightarrow{s_1}$$

Definition 2.2

Let $\alpha, \beta > 0$ and $\alpha \neq \beta$. The function $AA_\beta\big(X(m)\big)$ is defined as

$$X(m+1) = AA_\beta\big(X(m)\big) = \begin{cases} [X(m) + \alpha X(m-1)](\text{mod } 1), & b_i = 0 \\ [\beta X(m) + X(m-1)](\text{mod } 1), & b_i = 1 \end{cases}$$

where $m = 0,1,2, \ldots$, $X(-1) = 0$, $\alpha X(m-1)$, $\beta X(m)$ are evaluated via the beta-transformation and $s = \{b_i\}_{i=0}^{k}$ is the binary string.

Theorem 2.1

Let $s_1, s_2 \in S_k^*$. Let $s_1 s_2$ and $s_2 s_1$ represent concatenated strings of binaries. For a particular $X(0)$,

$$AA_\beta{}^{s_1 s_2}\big(X(0)\big) = AA_\beta{}^{s_2 s_1}\big(X(0)\big)$$

Proof:

We will take $s_1, s_2 \in S_k^*$ to be represented as vectors $\overrightarrow{s_1}$ and $\overrightarrow{s_2}$. By definition 2.1, the act of concatenating will be taken as the act of joining 2 vectors. By the parallelogram law it is obvious that

$$AA_\beta{}^{\overrightarrow{s_1}+\overrightarrow{s_2}}\big(X(0)\big) = AA_\beta{}^{\overrightarrow{s_2}+\overrightarrow{s_1}}\big(X(0)\big) \text{ or}$$

$$AA_\beta{}^{s_1 s_2}\big(X(0)\big) = AA_\beta{}^{s_2 s_1}\big(X(0)\big) \blacksquare$$

Remark 2.1

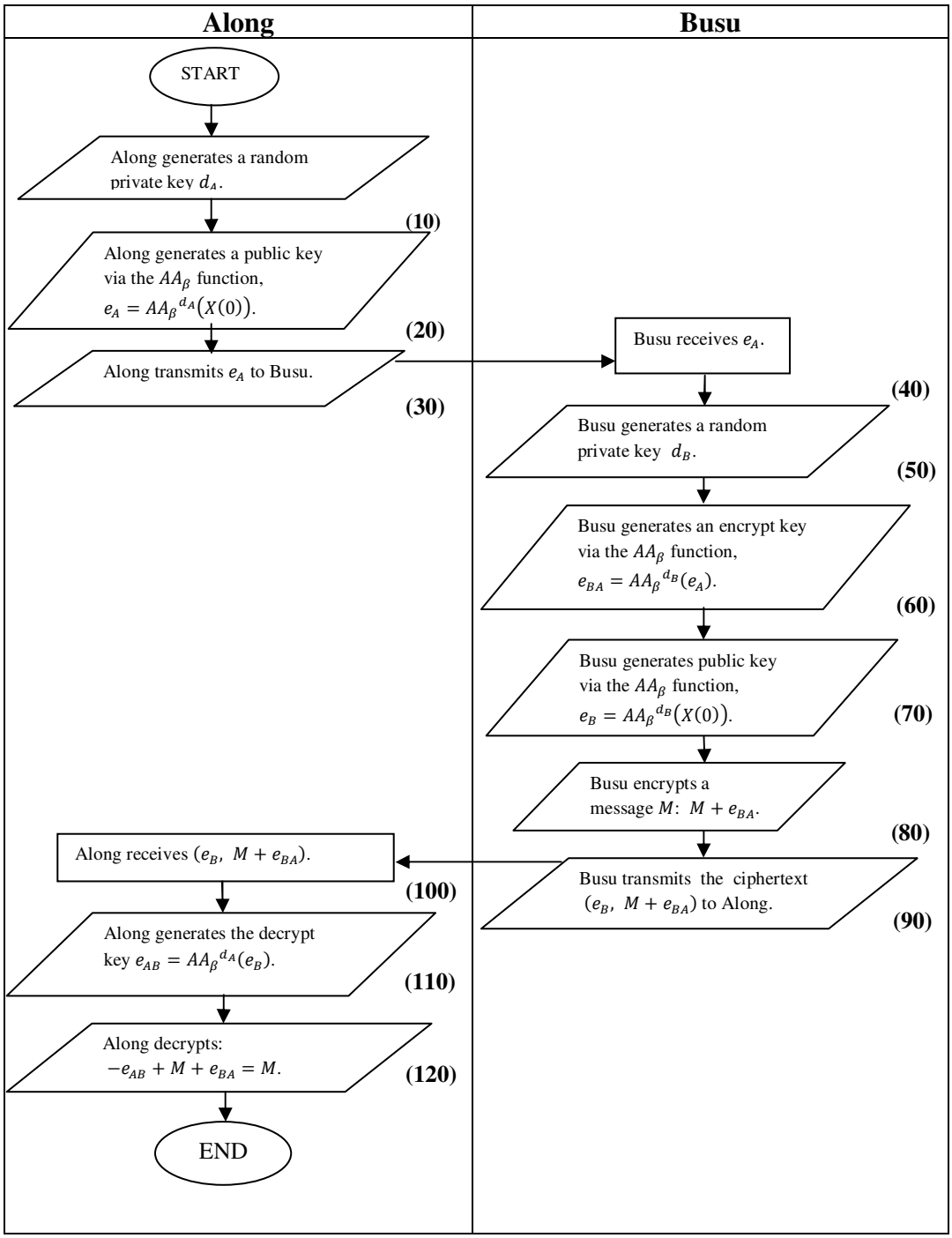
Theorem 2.1, proves that by taking either concatenated vectors of the form $\overrightarrow{s_1} + \overrightarrow{s_2}$ or $\overrightarrow{s_2} + \overrightarrow{s_1}$ would result in the exact same output when operated with the AA_β function given by definition 2.2.

The result given by theorem 2.1, does not give the value of the shared key. The shared key is derived together with the AA_β function by utilizing the full path to be taken by the string of bits. Refer to figure 1.That is, we will evaluate the AA_β function with $\overrightarrow{s_1} + \overrightarrow{s_2} = \overrightarrow{AB} + \overrightarrow{BC}$ and not the equivalent $\overrightarrow{s_1} + \overrightarrow{s_2} = \overrightarrow{AC}$.

We will now present the AA_β-cryptosystem. We will use the following flow chart. The addition "+" notation refers to the basic arithmetic operation of adding and the subtraction "-" notation refers to the basic arithmetic operation of subtracting. The generator point $X(0)$ will be an irrational number taken from the interval $(0,1)$. In this section we will assume that the AA_β-cryptosystem is working on the continuum. We will discuss the discretized AA_β-cryptosystem in another paper.

We will use the Malay characters "Along" and "Busu". Along will first generate a public key e_A by utilizing the the generator point $X(0)$ that was agreed upon in public prior to the communication process before transmitting it to Busu via an insecure channel. Busu will then generate an encrypt key via Along's public key e_{BA} and also generates his own public key e_B also by utilizing $X(0)$. Busu will then proceed to encrypt his message by utilizing the basic arithmetic operation of addition and will transmit the ciphertext consisting of $(e_B,\ M + e_{BA})$.

Along will then utilize Busu's public key to generate the decrypt key e_{AB}. And since $e_{AB} = e_{BA}$ Along will proceed to decrypt the ciphertext by utilizing the basic arithmetic operation of subtraction $M = -e_{AB} + M + e_{BA}$. The mechanism is akin to the ECC, thus opening areas of research which are comparable to ECC.


Along
Busu
START
Along generates a random private key d_A.
(10)
Along generates a public key via the AA_β function, $e_A = AA_\beta{}^{d_A}(X(0))$.
(20)
Along transmits e_A to Busu.
(30)
Busu receives e_A.
(40)
Busu generates a random private key d_B.
(50)
Busu generates an encrypt key via the AA_β function, $e_{BA} = AA_\beta{}^{d_B}(e_A)$.
(60)
Busu generates public key via the AA_β function, $e_B = AA_\beta{}^{d_B}(X(0))$.
(70)
Busu encrypts a message M: $M + e_{BA}$.
(80)
Busu transmits the ciphertext $(e_B,\ M + e_{BA})$ to Along.
(90)
Along receives $(e_B,\ M + e_{BA})$.
(100)
Along generates the decrypt key $e_{AB} = AA_\beta{}^{d_A}(e_B)$.
(110)
Along decrypts: $-e_{AB} + M + e_{BA} = M$.
(120)
END

We will now give a 32-bit example of key exchange by utilizing the generator point is $X(0) = 0\text{xC83C59C0} = 0.78217087686061859$. We will take $\alpha = 2$ and $\beta = 3$.

Along

i. Along generates an 8-bit private key $d_A = 0\text{x000000B3} = 10110011$.
ii. Along generates a public key $e_A = AA_\beta^{d_A}\big(X(0)\big) = 0\text{xF152AA40} = 0.94266761839389801$.
iii. Along sends e_A to Busu.

Busu

i. Busu generates an 8-bit private key $d_B = 0\text{x000000B7} = 10110111$.
ii. Busu generates a public key $e_B = AA_\beta^{d_B}\big(X(0)\big) = 0\text{x9625EEC0} = 0.58651630580425262$.
iii. Busu sends e_B to Along.

Along

i. Along generates the shared key $e_{AB} = AA_\beta^{d_A}(e_B) = 0\text{x6FD74540} = 0.4368785172700882$.

Busu

i. Busu generates the shared key $e_{BA} = AA_\beta^{d_B}(e_A) = 0\text{x6FD74540} = 0.4368785172700882$.

The process of encrypting and decrypting is trivial.

The Hard Mathematical Problem

We will now proceed to formalize the hard mathematical problem for the AA_β-Cryptosystem.

Determine the exact sequence $s \in S_k^*$ *such that* $AA_\beta{}^s\big(X(0)\big) = E$ *where* $X(0)$ *and* E *are public parameters.*

Remark 2.2

Based on the example above, for implementation purposes, we will utilize the fact that any "number" has its binary representation. As an example depending on the "type" of "number" one wants to utilize, the binary 1011_2

can either be the integer 11_{10} or the decimal number 0.6875_{10}. We will discuss the implementation techniques in another paper.

THE AA_β-FUNCTION IS A ONE-TO-ONE FUNCTION UNDER MINIMUM CONDITIONS

In tandem with the characteristics of the popular Diffie-Hellman key exchange methodology, we should choose a generator that has the "maximum" order. In the case of the Diffie-Hellman key exchange, the generator g from the congruence relation $A \equiv g^a \pmod p$ is of order p.

Theoretically, if an irrational number $X(0)$ is chosen within the interval $(0,1)$ its order (i.e. period) is infinity when iterated via the beta-transformation. However, in real life implementation we will choose an irrational number $X(0)$ with a finite binary representation. As an example, let us choose a j-bit irrational number $X_j(0)$. The question is: "What is the cycle of $X_j(0)$ under the AA_β function?" Mathematically, the problem statement is:

"Does there exist 2 non-identical sequences of equal length $s_1, s_2 \in S_k^*$ such that

$$AA_\beta{}^{s_1}\left(X_j(0)\right) = AA_\beta{}^{s_2}\left(X_j(0)\right)?"$$

We will first state the following definition.

Definition 3.1

Let $s \in S_k^*$ and AA_β be the function as defined in definition 2.2, the expansion $AA_\beta{}^s(1) = Esv$ is known as the symbolic representation of the AA_β function generated by s.

From the above definition we will observe the "symbolic representation" of a 4-bit key and its value for selected α and β.

Binary string	Symbolic representation	Symbolic representation value $\alpha = 1, \beta = 2$	Symbolic representation value $\alpha = 2, \beta = 3$
1000	$\alpha + \beta + 2\alpha\beta + \alpha^2$	8	21
1001	$\alpha + \beta + \alpha\beta + \alpha\beta^2 + \beta^2$	13	38
1010	$\alpha^2 + 2\alpha\beta + \beta^2 + \beta$	11	28
1011	$\alpha + \beta + \alpha\beta^2 + \beta^2 + \beta^3$	19	59
1100	$\alpha + \alpha\beta + \alpha\beta^2 + \beta^2 + 1$	12	36
1101	$\beta + \alpha\beta^2 + \beta^2 + \beta^3 + 1$	19	58
1110	$\beta^3 + \alpha\beta^2 + 2\beta + \alpha$	17	53
1111	$\beta^4 + 3\beta^2 + 1$	29	109

Lemma 3.1

If $s \in S_k^*$, $X(0)$ is an irrational number within the interval $(0,1)$ and AA_β is a function as defined in definition 2.2, then with the correct choice of α and β the cycle of $X(0)$ when utilized by the AA_β function is 2^{k-1}.

Lemma 3.2

If $s \in S_k^*$ and AA_β is a function as defined in definition 2.2, then ${AA_\beta}^s\big(X(0)\big) = {AA_\beta}^s(1) \cdot X(0)$; where $X(0)$ is an irrational number within the interval $(0,1)$.

Theorem 3.1

Let $s \in S_k^*$, ${AA_\beta}^s(1) = Esv$ is unique.

Proof:

Assume for 2 non-identical sequences $s_1, s_2 \in S_k^*$ we have:

$$ {AA_\beta}^{s_1}(1) = {AA_\beta}^{s_2}(1). $$

Choose a third sequence $s_3 \in S_k^*$ where $s_1 \neq s_2 \neq s_3$. By the parallelogram law the concatenated vectors:

$$ s_1 s_3 \neq s_2 s_3, $$

because $s_1 \neq s_2$.

Thus,

$$AA_\beta{}^{s_1 s_3}(1) \neq AA_\beta{}^{s_2 s_3}(1).$$

This is a contradiction. Thus, the assumption is false. ■

Corollary 3.1

Let $s \in S_k^*$ and $X(0) \in (0,1)$ be the generator point. There exists α and β such that the output $AA_\beta{}^{s}\big(X(0)\big) = E$ is unique.

Proof:

For $s \in S_k^*$ let $\{Esv_i(\alpha,\beta)\}_{i=1}^{k-1}$ be the set of all symbolic representations of $AA_\beta{}^{s}(1)$. Let $\{M_i(\alpha,\beta)\}_{i=1}^{k-1}$ be the value of each symbolic representation for particular α and β. Choose α and β such that $M_1(\alpha,\beta) \neq M_2(\alpha,\beta) \neq \cdots \neq M_{k-1}(\alpha,\beta)$ which implies that the output $AA_\beta{}^{s}\big(X(0)\big) = E$ is unique. ■

Remark 3.1

Observe that, for the correct choice of value for α and β, AA_β is a one-to-one function. It is obvious that for 2 non-identical sequences of different lengths $s_1 \in S_k^*$ and $s_2 \in S_l^*$ we can prove mathematically that for a j-bit irrational number $X_j(0)$

$$AA_\beta{}^{s_1}\Big(X_j(0)\Big) \neq AA_\beta{}^{s_2}\Big(X_j(0)\Big).$$

CONCLUSION

In this paper we have disclosed a public key cryptosystem that utilizes the chaotic beta-transformation. It is neither a variant of the RSA nor ECC algorithm. We utilized the method of concatenating 2 strings of binaries as was introduced by Bose who did not provide a mathematical explanation. However, we were careful not to repeat Bose's mistake of utilizing 2 commutative functions. We still utilize 2 linear functions with the extra property that they are not commutative, but through the recurrence relation they provide a secure key exchange method, and this overcomes the attack that Bose's method was exposed to.

We also observe the fact that in order for an attacker to determine the private key string of binary$s \in S_k^*$, from the public key e the attacker has to have all the binary positions in the correct order. Hence, making it possible

for further research to determine whether this cryptosystem can only utilize a private key of length 128-bits and thus having the same key strength as a symmetric cryptosystem.

Remarks

The authors welcome any comments on the cryptosystem especially with regards to the implementation of floating numbers $x \in (0,1)$ on finite machines. The authors are finalizing a paper discussing the matter and will disclose a concrete and scientific method of utilizing such floating numbers via its base 2 representation.

REFERENCES

[1] Alvarez, G. & Li, Shujun. 2006. Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems. *International Journal of Bifurcation and Chaos*, **16**(8): 2129-2151.

[2] Alvarez,G., Montoya, F., Romera, M. & Pastor,G. 2003. Cryptanalysis of an ergodic chaotic cipher. *Phys. Lett. A* **311**: 172-179.

[3] Baptista, M. S. 1998. Cryptography with chaos. *Phys. Lett. A* **240**: 50–54.

[4] Bergamo, P. & Arco, P. 2005. Security of public key cryptosystems based on Chebyshev polynomials. *IEEE Trans. Circuits Syst, I,* **52**: 1382-1393.

[5] Bose, R. 2005. Novel public key encryption technique based on multiple chaotic systems. *Phys. Rev. Lett.*, **26**.

[6] Klein, E., Mislovaty, R., Kanter, I. & Kinzel, W. 2005. Public channel cryptography using chaos synchronization. *Phys. Rev. E.,* **72**.

[7] Koblitz, N. 1987. Elliptic Curve Cryptosystems. *Math. Of Comp.* **48**: 203-209.

[8] Kocarev, L. & Tasey, Z. 2003. Public key encryption based on Chebyshev maps, *Proc. 1st Circuit and Syst Symposium*: 25-28.

[9] Kocarev,L. & Sterjev, M. 2004. Public key encryption scheme with chaos. Chaos, **14**: 1078-1081.

[10] Masuda, N. & Aihara, K. 2002. Cryptosystems with discretized chaotic maps, *IEEE Trans. Circuits Syst. I*, **49**: 28–40.

[11] M.R.K.Ariffin. 2009. Membilang orbit serta aplikasi sistemkripto berdasarkan sistem dinamik kalut. (*Counting orbits and a cryptosystem application based on chaotic dynamical system*). Phd thesis. Universiti Kebangsaan Malaysia.

[12] M.R.K.Ariffin & M.M.Noorani. 2009. Conditions for counter Measures Against OTP Attack on Baptista Type Chaotic Cryptosystem. *Int. J. Crypt. Res.* **1**(1): 93-101.

[13] M.R.K.Ariffin & M.M.Noorani. 2008. Modified Baptista type chaotic cryptosystem via matrix secret key. *Phys. Lett. A* **372**: 5427-5430.

[14]Tenny, R. & Tsimring, L. 2005. Additive mixing modulation for public key encryption based on distributed dynamics. *IEE Trans. Circuits Syst I.,* **52**: 672-679.

[15] Wang, K., Pei, W. & Zhou, L. 2006. Security of public key encryption technique based on multiple chaotic systems. *Phys. Lett. A*, **360**: 259-262.

[16] Yi, Tan & Siew. 2002. A New Block Cipher Based on Chaotic Tent Maps, *IEEE Trans. Circuits Syst, I,* **49**(12): 1826-1829.

[17] Zhang, L. 2008. Cryptanalysis of the public key encryption based on multiple chaotic systems. *Chaos, Solitons and Fractals*, **37**: 669-674.