이산화된 카오스 함수를 이용한 새로운 경량의 암호 시스템

종신회원 임 대 운*, 정회원 양 기 주*, 안 태 호**

A New Light Cryptosystem with a Discretized Chaotic Functions

Dae-Woon Lim* *Lifelong Member*, Gijoo Yang*, Ta-Ho An** *Regular Members*

요 약

카오스 함수의 출력 값은 예측 불가능하고 무작위처럼 보이며, 이러한 특성은 안전한 암호 시스템에서 요구하는 특성과 일치한다. 이러한 이유로 인해, 카오스 함수를 이용한 암호 시스템이 지금까지 다양하게 제안되어 왔다. 하지만, 대부분의 카오스 암호 시스템은 매우 높은 수준의 연산 능력을 필요로 하기 때문에 경량의 시스템에 적용하지 못했다. 본 논문에서는 적은 연산 능력을 가진 시스템에서도 응용 가능한 경량의 카오스 암호 시스템을 제안하고, 제안된 암호 시스템의 연산량 및 안전도와 관련된 성능을 모의 실험을 통하여 제시한다.

Key Words : Cryptosystem, discretized chaotic maps, discretized tent maps

ABSTRACT

The output values of chaotic functions look highly unpredictable and random-like. These features are in accord with the requirements for secure cryptosystems. For this reason, many kinds of cryptosystems using chaotic functions have been proposed so far. However, most of those algorithms are not applicable for light cryptosystems because they need a high level of computing ability. In this paper, we propose a new light chaotic cryptosystems which are suitable for the systems with a low level of computing ability. From the simulations, we show the performance of proposed cryptosystems on computational complexity and security level.

Ⅰ. 서 론

하드웨어의 크기와 암호 및 복호화에 걸리는 시간의 제약이 큰 RFID의 특성상 기존의 비밀키 알고리듬을 그대로 적용하는 것은 부적절하다. 국내에서는 RFID에 적용할 수 있는 초경량 암호 알고리즘에 대한 연구는 아직 초기 단계에 머물러 있다고 할 수 있다. 최근에 유럽에서는 eSTREAM 프로젝트를 통해 RFID에 적용할 수 있는 초경량의 스트림 암호를 확보한 바 있으며, 2007년에는 블록 암호를 이용한 초경량 암호 알고리즘인 PRESENT가 제안된 바 있다. 또한 유럽의 연구진들에 의해서 해쉬 함수 역시 초경량 블록 암호인 PRESENT를 사용해서 매우 작은 크기로 RFID의 특성에 최적화되어 제안되기도 하였다.

RFID 시장은 향후 급격한 성장이 예상되지만 아직 개당 수백원에 이르는 RFID 태그의 가격을 최대한 낮추는 것이 관건이다. 그러면서도 동시에 기본적인 보안 장치가 뒷받침되어야만 제대로 된 응용이 가능하다. 특히 오늘날에는 단순히 보안을 제공하는 것이 아니라 보안을 위한 인증 과정에서 개인의 프라이버시가 보호되는 것

※ 본 연구는 지식경제부의 산학협력중심대학육성사업과 동국대학교의 교비 지원으로 수행되었음.
* 동국대학교 정보통신공학과(daewoonlim@gmail.com, gjyang@dongguk.edu)
** 방위사업청 (antaho@naver.com)
논문번호 : KICS2010-06-281, 접수일자 : 2010년 6월 28일, 최종논문접수일자 : 2010년 11월 16일

역시 중요한 요소 중 하나로 떠오르고 있다. 이를 위해서 인증 과정은 익명으로 일어나야 한다. 따라서 RFID에도 어떤 형태로든 해쉬 함수가 포함되어만 한다.

RFID를 낮은 가격으로 유지하기 위해서는 총 7,500에서 15,000개 이하의 Gate로 하드웨어를 구성할 수 있어야 한다. 이 중에서 100비트의 EPC 칩을 구현하기 위해서 5,000에서 10,000 Gate가 필요하기 때문에 암호 모듈에서 사용 가능한 Gate는 2,500에서 5,000 정도에 불과하다. 이처럼 작은 크기로 하드웨어를 구성하는 것이 현 시점에서 RFID를 더욱 확산시키는데 중요한 요소로 더욱 부각되고 있다. 이를 위해 구체적으로 해쉬 함수나 암호 알고리즘을 2,000 Gate 이하로 구현할 필요가 있다. 특히 유도 전력으로 동작하는 RFID의 특성상 각각의 암호 알고리즘들은 전력 소모를 최소화해야 한다.

미국의 NIST에서 표준으로 채택한 블록 암호인 AES-128의 경우에도 최소 크기는 3400 Gate에 달한다. 이를 위해서는 더 작은 면적을 가지면서도 RFID 응용에서 충분한 안전성를 보장해 줄 수 있는 새로운 방법에 대한 연구가 필요하다.

카오스 함수는 정확한 초기값과 파라미터의 값을 알지 못할 경우, 출력 값은 예측 불가능하고 무작위처럼 보이며, 이러한 특성들은 암호학에서 필요로 하는 특성들과 일치하는 것이다. 이러한 이유로 인해, 암호 시스템에 카오스 함수를 이용하는 것은 효과적이라는 사실을 알 수 있다.

실제로 1990년대 초부터, 카오스 함수를 이용한 암호 시스템은 활발히 연구되어 왔다[2,4,5]. 그러나 개발된 대부분의 암호 시스템들은 암호와 복호 과정에서 큰 계산 능력을 필요로 하고 있기 때문에, 작은 연산 능력을 가지고 있는 시스템에는 부적절한 것이 사실이다.

본 논문에서는 카오스 함수의 성질을 이용하되, 적은 연산 능력을 가진 시스템에서도 응용 가능한 경량의 암호 시스템을 제안할 것이다.

본 논문의 구성은 다음과 같다. 먼저 제 2장에서 사전 지식으로 카오스 함수의 정의와 이를 이용해 제안된 기존의 암호 시스템을 소개한 뒤, 제 3장에서는 카오스 함수를 이용한 경량의 새로운 암호 시스템을 제안한다. 다음으로 제 4장에서는 제안된 시스템의 성능을 분석하며, 마지막으로 제 5장에서 결론을 맺는다.

Ⅱ. 카오스 함수

2.1 텐트 함수 (Tent Map)

다음과 같은 형태의 계차 방정식을 생각하자.

$$X_{n+1} = F(X_n),\ X_n \in [0,1]$$

이러한 계차 방정식을 반복하여 얻은 결과 값이 랜덤한 값을 가질 때, F는 카오스 함수(chaotic maps)라 불린다.

카오스 함수는 일반적으로 다음과 같은 성질을 만족시켜야 한다.

- 파라미터에 대한 민감성 : 만일 카오스 함수의 모양을 결정하는 파라미터가 약간 다른 두 개의 카오스 함수를 생각할 때, 동일한 초기 값을 입력으로 하여 두 개의 카오스 함수를 각각 반복해 얻은 두 결과 값은 결과적으로 크게 달라야 한다.
- 초기값에 대한 민감성 : 약간 다른 두 개의 초기값을 입력으로 하여 하나의 카오스 함수를 반복해 얻은 두 값은 결과적으로 크게 달라야 한다.
- 무작위성 : 거의 모든 가능한 초기값을 입력으로 하여 카오스 함수를 반복해 얻은 결과 값들은 [0,1]구간에서 랜덤하게 발생해야 하며, 그들의 분포는 균일(uniform)해야 한다.

암호 시스템에 적용될 수 있는 카오스 함수는 여러 가지가 제안되어 왔다. 그 중에서도 가장 간단하면서도 가장 널리 사용되는 카오스 함수는 텐트 함수이다.

텐트 함수란 일차원의 부분적인 선형 함수(piecewise linear map)의 일종이다. 아 함수는 [0,1]의 구간을 정의역으로 하여 같은 크기의 치역을 가지며, 오직 하나의 파라미터 α만을 갖는 특징을 가지고 있다. 텐트 함수는 다음과 같이 정의된다.

$$f_\alpha(x) = \begin{cases} \dfrac{x}{\alpha}, & 0 \le x \le \alpha \\ \dfrac{x-1}{\alpha-1}, & \alpha < x \le 1 \end{cases}$$

$$f_\alpha^{-1}(y) = \alpha y \quad \text{or} \quad 1+(\alpha-1)y$$

텐트 함수가 카오스 함수가 만족해야 할 성질을 갖는다는 것은 널리 알려진 사실이다[2]. 아래의 그림 1에서는 텐트 함수의 모양을 보여주고 있다.

텐트 함수 f_α는 하나의 출력 값에 대해 두 개의 입력 값을 갖는 함수이며, 역함수 f_α^{-1}는 하나의 입력 값에 대해 두 개의 출력 값을 갖는 함수임에 주목하자. 따라서, f_α^n은 하나의 출력 값에 대해 2^n개의 대응되는 입력 값을 가지고 있으며, f_α^{-n}은 하나의 입력 값에 대해 2^n개의 출력 값을 가지고 있다. 또한,

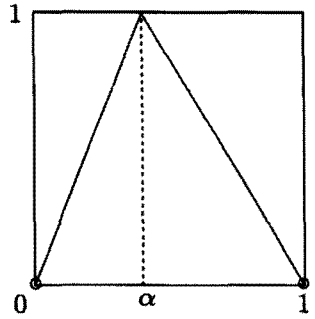


그림 1. Tent Map

$x = f_\alpha(f_\alpha^{-1}(x))$이기 때문에, $x = f_\alpha^n(f_\alpha^{-n}(x))$임을 쉽게 알 수 있다.

2.2 텐트 함수를 이용한 암호 시스템

텐트 함수를 이용한 가장 간단한 형태의 암호 시스템은 Habutsu에 의하여 다음과 같이 제안되었다[2].

- 비밀키 : 파라미터 α
- 암호화 : 암호화하고자 하는 메세지를 이용해 평문 p를 얻는다. 이 때, p는 0에서 1사이의 값을 갖는 실수이다. 다음으로 아래와 같은 수식처럼 f_α^{-1}을 연속적으로 수행해 암호문 c를 얻는다. 이 때, f_α^{-1}을 적용할 때마다 발생되는 두 개의 출력 값 중 하나만을 취한다.

$$c = f_\alpha^{-1}(f_\alpha^{-1}(\cdots f_\alpha^{-1}(p)\cdots)) = f_\alpha^{-n}(p)$$

- 복호화 : 수신 받은 메시지 C를 입력으로 하여 아래와 같은 수식처럼 f_α를 연속적으로 수행해 평문 p를 얻는다.

$$p = f_\alpha(f_\alpha(\cdots(f_\alpha(c)\cdots))) = f_\alpha^n(c)$$

그러나 이러한 방식의 암호 시스템은 몇 가지 단점을 가지고 있다.

- f_α와 f_α^{-1}은 일대일 함수가 아니다. 따라서 암호화와 복호화 과정이 유일(unique)하게 결정된다 하여도, f_α와 f_α^{-1}의 성질이 암호 공격에 있어서 약점으로 작용한다.
- 각 라운드의 입력 값과 출력 값은 정수가 아닌 실수이다. 따라서 암호화와 복호화의 유일성을 보장하기 위해서는 매우 정확한 수준의 연산이 필요하다.
- f_α와 f_α^{-1}은 부분적으로 선형(piecewise linear)이다. 따라서 암호 시스템은 선형 혹은 차분 암호 공격에 대하여 취약점을 갖는다.

이러한 단점들을 보안하기 위하여, Masuda는 이산화된 카오스 함수를 정의하고, 이를 이용하여 암호 시스템을 제안하였다[5].

2.3 이산화된 텐트 함수

함수의 정의역을 1에서 M사이의 정수라고 정의한다. 또한, 이산화된 텐트 함수의 파라미터를 A라고 정의한다. 이 때, A 역시 1에서 M사이의 정수 값을 갖는다. 이산화된 텐트 함수는 다음과 같이 정의된다[5].

$$F_A(X) = \begin{cases} \left\lceil \frac{M}{A} X \right\rceil, & 1 \le X \le A \\ \left\lfloor \frac{M}{M-A}(M-X) \right\rfloor + 1, & A < X \le M \end{cases}$$

또한, 이산화된 텐트 함수의 역함수는 다음과 같이 정의된다.

$$F_A^{-1}(Y) = \begin{cases} X_1, & m(Y) = Y, \frac{X_1}{A} > \frac{M-X_2}{M-A} \\ X_2, & m(Y) = Y, \frac{X_1}{A} < \frac{M-X_2}{M-A} \\ X_1, & m(Y) = Y+1 \end{cases}$$

이 때, X_1, X_2와 $m(Y)$는 아래와 같이 정의된다.

$$\begin{aligned} X_1 &\equiv \lfloor M^{-1}AY \rfloor \\ X_2 &\equiv \lceil (M^{-1}A-1)Y+M \rceil \\ m(Y) &\equiv Y + \left\lfloor \frac{AY}{M} \right\rfloor - \left\lceil \frac{AY}{M} \right\rceil + 1 \end{aligned}$$

Masuda는 자신의 논문에서, 위와 같이 정의된 이산화된 텐트 함수가 일대일 대응을 가지며 카오스 함수의 성질을 만족시킴을 보였다.

2.4 이산화된 텐트 함수를 이용한 암호 시스템

우선, 암호화하고자 하는 메시지를 이용해 평문 P를 얻는다. 이 때, P는 정수 값을 가지며, 가능한 평문의 최대값을 M이라 설정한다. 앞 섹션에서 정의된 이산화된 텐트 함수를 이용한 암호 시스템은 다음과 같이 정의된다.

- 비밀키 : 파라미터 A
- 암호화 : 평문 P를 초기값으로 하여 아래와 같

은 수식처럼 F_A를 연속적으로 수행해 암호문 C를 얻는다.

$$C = F_A(F_A(\cdots F_A(P)\cdots)) = F_A^m(P)$$

- 복호화 : 수신받은 메시지 C를 입력으로 하여 아래와 같은 수식처럼 F_A^{-1}를 연속적으로 수행해 복호화된 평문 P를 얻는다.

$$P = F_A^{-1}(F_A^{-1}(\cdots(F_A^{-1}(C)\cdots))) = F_A^{-n}(C)$$

이산화된 텐트 함수를 이용해 제안된 암호 시스템은, 실수 값을 갖는 텐트 함수를 이용한 암호 시스템이 가졌던 문제점을 해결할 수 있다. 하지만, 이러한 방식의 시스템도 암호화하고자 하는 평문 전체를 대상으로 카오스 함수를 반복 수행하기 때문에 매우 높은 수준의 연산 능력을 필요로 한다.

즉, 64bit 암호 시스템을 가정할 때, 이산화된 카오스 함수를 적용하기 위해서는 최대 2^{64} 크기의 정수들을 대상으로 하여 곱셈과 나눗셈으로 이루어진 실수 연산들을 반복 수행하여야 한다. 따라서, 이와 같은 암호 시스템은 적은 양의 연산 능력만을 갖춘 소형 시스템에는 적합하지 않다.

다음 절에서 우리는 이산화된 텐트 함수를 이용하되, 연산 능력이 적은 소형 시스템에서도 적용 가능한 경량의 새로운 암호 시스템을 제안할 것이다.

Ⅲ. 이산화된 카오스 함수를 이용한 경량의 새로운 암호 시스템

본 암호 알고리즘은 64bits의 평문을 입력으로 받아 64bits의 키(key)를 이용하여 64bits의 암호문을 출력으로 내도록 설계되었다. 각 라운드 변환은 대체(substitution)와 치환(permutation)으로 구성되어 있다. 암호화는 같은 라운드 변환을 16번 반복하여 수행된다. 또한 복호화 과정은 이와 거의 유사한 라운드 변환의 반복을 통하여 이루어지게 된다.

3.1 Substitution S_k

암호 시스템에 사용될 64 bits의 키를 K라 하면 K는 다음과 같은 8개의 서브키로 나뉘어질 수 있다.

$$K = (K_0 K_1 \cdots K_7)$$

각각의 서브키 $K_i, 0 \leq i \leq 7$에 대하여 다음의 함수를 정의한다.

$$S_{K_i}(x) = \begin{cases} \left\lfloor \frac{256}{K_i}(x+1) \right\rfloor - 1, & 0 \leq x < K_i \\ \left\lfloor \frac{256}{256-K_i}(256-x-1) \right\rfloor, & K_i \leq x < 256 \end{cases}$$

S_{K_i}는 일대일 함수이고 이의 역함수를 $S_{K_i}^{-1}$라 한다.

이제 S_{K_i}를 이용하여 S_K를 정의하도록 한다. S_K의 입력인 64bits 메시지 X를 다음과 같이 8개의 워드(word)로 나눈다.

$$X = (X_0 X_1 \cdots X_7)$$

이 때, S_K는 다음과 같이 정의된다.

$$S_K(X) = (S_{K_0}(X_0) S_{K_1}(X_1) \cdots S_{K_7}(X_7))$$

비슷한 방법으로 S_K의 역함수 S_K^{-1}은 다음과 같이 정의된다.

$$S_K^{-1}(X) = (S_{K_0}^{-1}(X_0) S_{K_1}^{-1}(X_1) \cdots S_{K_7}^{-1}(X_7))$$

3.2 Permutation π

우선 64 bits의 메시지를 입력으로 받아 8 bits의 출력을 내는 함수 $\gamma_i, 0 \leq i \leq 7$를 정의하도록 한다. 이 때 입력 X는 대체 함수의 경우와 동일하게 정의되며, 또한 다음과 같이 8개의 워드를 정의한다.

$$m_0 = 10000000_2, m_1 = 01000000_2,$$
$$m_2 = 00100000_2, m_3 = 00010000_2,$$
$$m_4 = 00001000_2, m_5 = 00000100_2,$$
$$m_6 = 00000010_2, m_7 = 00000001_2.$$

이 경우 γ_i는 다음과 같이 정의된다.

$$\gamma_i(X) = \left(\oplus_{k=0}^{7}(m_i \cdot X_k \gg k)\right) \ll i$$

여기서 $\ll$와 $\gg$는 각각 왼쪽 방향과 오른쪽 방향의 순환(rotation)을 뜻하며, $\oplus$는 비트 간 XOR, $\cdot$은 비트 간 AND 연산을 의미한다.

이제 γ_i를 이용하여 γ를 다음과 같이 정의한다.

$$\gamma(X) = (\gamma_0(X)\gamma_1(X)\cdots\gamma_7(X))$$

γ는 일대일 함수이므로 역함수가 존재한다. 마지막으로 $\pi(X) = \gamma^{-1}(X), \pi^{-1}(X) = \gamma(X)$로 정의한다.

3.3 Encryption/Decryption

암호화와 복호화를 위한 라운드 함수는 각각 다음과 같이 정의된다.

$$R_K = \pi \circ S_k$$
$$R_K^{-1} = S_k^{-1} \circ \pi^{-1}$$

암호화는 동일한 라운드 변환을 16번 반복하여 수행되므로 암호화와 복호화 함수는 다음과 같이 표현된다.

$$E_k(X) = R_K^{16}(X)$$
$$D_K(Y) = R_K^{-16}(Y)$$

Ⅳ. 성능 및 안전성 분석

4.1 연산량

기존의 카오스 함수를 이용한 암호화 기법을 64 bits 암호 시스템에 적용할 경우, 각 라운드 함수를 수행하기 위하여 2^{64} 크기의 정수 값들에 대하여 나눗셈과 곱셈의 실수 연산이 필요했다. 반면, 본 논문에서 제안된 방식을 이용할 경우에는, 각 라운드 함수를 수행하기 위하여 2^8 크기의 정수 값들에 대한 곱셈과 나눗셈의 연산을 8번씩 수행하면 된다. 물론, 기존의 방식과 달리 추가적으로 치환 과정을 거쳐야 하지만, 이는 하드웨어나 소프트웨어로 구현시 매우 간단하게 수행될 수 있기에 연산량에 큰 부담을 주지 않는다.

또한, 대체 함수인 S_{K_i}의 입력 값과 출력 값을 테이블로 작성하여 메모리에 보관한 후 이 테이블을 이용한다면, 매우 적은 양의 연산만으로도 암호화와 복호화를 수행할 수 있을 것이다.

4.2 안전도

일반적으로 안전한 암호 시스템은 다음의 조건들을 만족시켜야 한다.

- 평문에 대한 암호문 분포의 균일성(U-P) : 평문을 연속적으로 변화시킬 때, 결과로서 발생되는 암호문은 가능한 암호문의 전 영역에 걸쳐 균일하게 분포되어야만 한다.
- 키에 대한 암호문 분포의 균일성(U-K) : 키의 값을 연속적으로 변화시킬 때, 결과로서 발생되는 암호문은 가능한 암호문의 전 영역에 걸쳐 균일하게 분포되어야만 한다.
- 평문에 대한 암호문의 민감성(S-P) : 암호문은 평문의 변화에 대하여 민감해야 한다. 즉, 평문의 1 bit 변화가 완전히 다른 형태의 암호문을 생성해내야만 한다.
- 키에 대한 암호문의 민감성(S-K) :암호문은 키의 값의 변화에 대하여 민감해야 한다. 즉, 키 값이 1bit 변화가 완전히 다른 형태의 암호문을 생성해내야 한다.

본 절에서는 제안한 암호 시스템이 위에서 제시한 조건들을 만족시킴을 보이는 통계적 실험의 결과를 제시하고자 한다. 이러한 목적을 위하여 다음의 테스트들을 수행한다.

① 균일성 테스트 (U-P, U-K)

(a) 암호문이 분포되어 있는 영역 $[1, M]$을 같은 크기를 갖는 b개의 연속적인 구간으로 나눈다. 이 때, i번째 구간을 I_i라 부르기로 한다.

(b) U-P 테스트를 위하여 다음의 n개의 암호문의 값을 구한다.

$$E_k(X), E_k(X+1), \cdots, E_k(X+n-1).$$

그리고, 각각의 암호문이 I_i에 포함되어 있는 개수를 헤아려 빈도 n_i를 구한다.

U-K 테스트를 위하여는 다음의 n개의 암호문의 값을 구한 뒤, U-P 테스트의 경우와 같이 빈도 n_i를 구한다.

$$E_{\gamma^{-1}(\gamma(K))}(X), E_{\gamma^{-1}(\gamma(K)+1)}(X), \cdots, E_{\gamma^{-1}(\gamma(K)+n-1)}(X)$$

(c) 다음의 표준 편차 값을 구한다.

$$\delta = \sqrt{\frac{\sum_{i=1}^{b}\left(n_i - \frac{n}{b}\right)^2}{b}}$$

② 민감성 테스트 (S-P, S-K)

(a) 암호문이 분포되어 있는 영역 $[1, M]$을 같은 크

기를 갖는 b개의 연속적인 구간으로 나눈다. 이 때, i번째 구간을 I_i라 부르기로 한다.

(b) S-P 테스트를 위하여 다음의 n개의 암호문의 쌍의 값을 구한다.

$$\{E_k(X_1),E_k(X_1+1)\},\cdots,\{E_k(X_n),E_k(X_n+1)\}$$

그리고, 각각의 암호문이 $\{I_i,I_j\}$에 포함되어 있는 개수를 헤아려 빈도 n_{ij}를 구한다.

S-K 테스트를 위하여는 다음의 n개의 암호문의 쌍의 값을 구한 뒤, S-P 테스트의 경우와 같이 빈도 n_{ij}를 구한다.

$$\{E_{\gamma^{-1}(\gamma(K_1))}(X),E_{\gamma^{-1}(\gamma(K_1)+1)}(X)\},$$
$$\cdots,\{E_{\gamma^{-1}(\gamma(K_n))}(X),E_{\gamma^{-1}(\gamma(K_n)+1)}(X)\},$$

(c) 다음의 표준 편차 값을 구한다.

$$\delta=\sqrt{\frac{\sum_{i=1}^{b}\sum_{j=1}^{b}\left(n_{ij}-\frac{n}{b^2}\right)^2}{b^2}}$$

본 절의 나머지 부분에서는 각각의 테스트에 대하여 수행한 모의 실험한 결과를 제시하도록 한다.

① 균일성 테스트 (U-P, U-K)

균일성 테스트를 위하여 우리는 다음과 같은 파라미터를 사용하도록 한다.

- $M=2^{64},\ b=2^8,\ \ n=2^{16}$

그림 2와 그림 3에 특정한 입력 값 $X(K)$에 대하

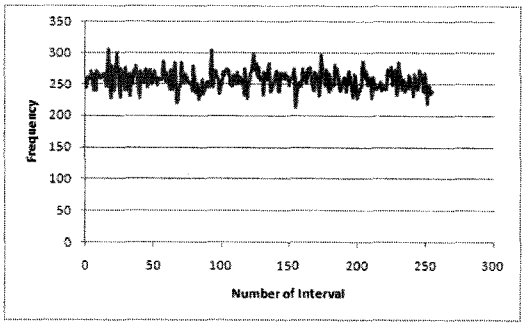


그림 2. U-P 테스트 결과

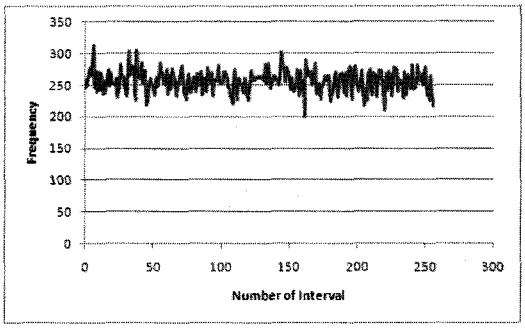


그림 3. U-K 테스트 결과

여 구한 빈도 값 n_i가 나타나 있다. 여러 입력 값에 대하여 구한 표준 편차의 값은 U-P와 U-K의 경우 동일하게 대략 16으로 나타난다.

② 민감성 테스트 (S-P, S-K)

민감성 테스트를 위하여 우리는 다음과 같은 파라미터를 사용하도록 한다.

- $M=2^{64},\ b=2^4,\ n=2^{16}$

그림 4와 그림 5에 특정한 S-P 테스트와 S-K 테스트에 대하여 구한 빈도 값 n_i가 나타나 있다. S-P 테스트와 S-K 테스트를 여러 번 반복하여 얻은 표준 편

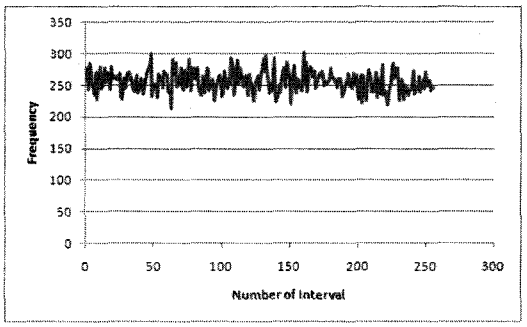


그림 4. S-P 테스트 결과

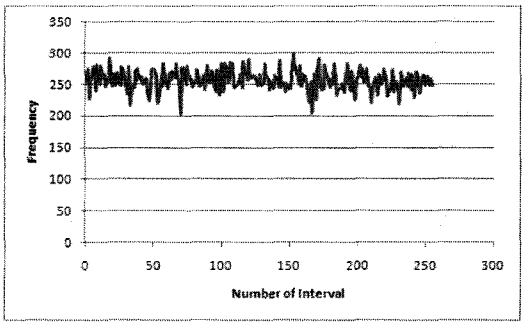


그림 5. S-K 테스트 결과

차의 값은 평균적으로 대략 16으로 나타난다.

V. 결 론

본 논문에서는 이산화된 카오스 함수를 이용한 경량의 새로운 암호 시스템을 제안하였다. 카오스 함수를 이용한 기존의 암호 시스템들은 매우 높은 수준의 연산 능력을 필요로 하기 때문에 소형 시스템에는 적용하기가 적합하지 않았다. 그러나 본 논무에서 제안된 방식은 비교적 적은 양의 연산 혹은 테이블을 이용하여 구현될 수 있기 때문에 경량의 시스템에 적합하다는 이점을 갖는다. 또한 모의 실험을 통하여 새로이 제안된 암호 시스템의 안전도를 보였다.

참 고 문 헌

[1] S.Aono and Y.Nishio, "Chaotic map with parameter changing shape of the map for a cryptosystem," *Proceedings of NOLTA'08*, pp. 384-387, 2008.

[2] T.Habutsu, Y.Nishio, I.Sasase, and S.Mori, "A Secret Key Cryptosystem by Iterating a Chaotic Map", in *Proc. Advances in Cryptology-EUROCRYPT'91*. Berlin, Germany : Springer-Verlag, 1991, pp. 127-140.

[3] G. Jakimoski and L. Kocarev, "Chaos and Cryptography : Block Encryption Ciphers Based on Chaotic Maps", *IEEE Trans. Circuits Syst.* Vol.48, No.2, pp.163-169, Feb 2001.

[4] Z. Kotulski and J. Szczepanski, "Discrete Chaotic Cryptography," *Ann. Phys.*, Vol.6, pp. 381-394, 1997.

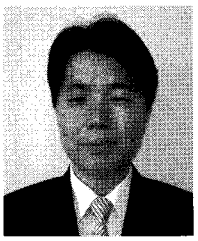
[5] N. Masuda and K. Aihara, "Cryptosytems With Discretized Chaotic Maps", *IEEE Trans. Circuits Syst.* Vol.49, No.1, pp.28-40, Jan 2002.

[6] N. Masuda, G. Jakimoski, K. Aihara and L. Kocarev, "Chaotic Block Ciphers : From Theory to Practical Algorithms," *IEEE Trnas. Circuits and Systems,* Vol.53, No.6, pp.1341-1352, 2006.

[7] N.K. Pareek, Vinod Patidar and K.K. Sud, "Discrete Chaotic Cryptography using External Key," *Physics Letters*, A 309, pp.75-82, 2003.

[8] Xun Yi, Chik How Tan, and Chee Kheong Siew, "A New Block Cipher Based on Chaotic Tent Maps", *IEEE Trans. Circuits Syst.* Vol.49, No.12, pp.1826-1829, Dec 2002.

임 대 운 (Dae-Woon Lim) 종신회원



1994년 2월 한국과학기술원 전기및전자공학과 학사
1997년 2월 한국과학기술원 전기및전자공학과 석사
2006년 8월 서울대학교 전기·컴퓨터공학부 박사
1995년 9월~2002년 8월 LS산전선임 연구원
2006년 9월~현재 동국대학교 정보통신공학과 조교수

안 태 호 (Ta-Ho An) 정회원

1996년 8월 국민대학교 산업대학원 정보통신공학과 석사
2010년 2월 광운대학교 방위사업학과 박사 수료
2001~2004년 3월 5군단 751 노드대대장
2004~2005년 3월 수고군단 정보통신계획과장
2005~2005년 12월 육본 전력개발단 정보통신계획장교
2006년 1월~현재 방위사업청
<관심분야> EVMS 성과관리, 반도체 이론, 시공간 부호

양 기 주 (Gijoo Yang) 정회원

1984년 5월 Univ. of Wisconsin, 전산학 학사
1986년 5월 Univ. of Michigan EECS 석사
1991년 12월 Univ. of Delaware 전산학 박사
1992년 6월~1995년 2월 KT 연구소 선임 연구원
1995년 3월~1995년 8월 용인대 경영정보학과 조교수
1995년 9월~현재 동국대학교 정보통신공학과 교수
<관심분야> 인공지능, 통신시스템