(12) 특허협력조약에 의하여 공개된 국제출원

(19) 세계지식재산권기구
국제사무국

(43) 국제공개일
2011 년 11 월 3 일 (03.11.2011)

PCT

(10) 국제공개번호
WO 2011/136614 A2

(51) 국제특허분류:
G06F 9/06 (2006.01) *G06F 17/10* (2006.01)

(21) 국제출원번호: PCT/KR2011/003219

(22) 국제출원일: 2011 년 4 월 29 일 (29.04.2011)

(25) 출원언어: 한국어

(26) 공개언어: 한국어

(30) 우선권정보:
10-2010-0040126 2010 년 4 월 29 일 (29.04.2010) KR

(71) 출원인 (US 을(를) 제외한 모든 지정국에 대하여): **동국대학교 산학협력단 (DONGGUK UNIVERSITY INDUSTRY-ACADEMIC COOPERATION FOUNDATION)** [KR/KR]; 서울특별시 중구 필동 3 가 26, 100-715 Seoul (KR).

(72) 발명자; 겸
(75) 발명자/출원인 (US 에 한하여): **임대운 (LIM, Dae Woon)** [KR/KR]; 서울특별시 중구 신당동 남산타운아파트 13 동 1104 호, 100-450 Seoul (KR). **양기주 (YANG, Gi Joo)** [KR/KR]; 서울특별시 서초구 서초2동 우성아파트 6 동 801 호, 137-773 Seoul (KR). **임태형 (LIM, Taehyung)** [KR/KR]; 서울특별시 관악구 남현동 1064-14, 151-800 Seoul (KR). **금은지 (KUM, Eun Ji)** [KR/KR]; 경기도 수원시 권선구 고색동 태산아파트 102-804, 441-728 Gyeonggi-do (KR).

(74) 대리인: **특허법인 충현 (CHUNG HYUN PATENT & LAW FIRM)**; 서울특별시 중구 신당2동 353-18 두지빌딩 4층, 100-828 Seoul (KR).

(81) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 국내 권리의 보호를 위하여): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 지정국 (별도의 표시가 없는 한, 가능한 모든 종류의 역내 권리의 보호를 위하여): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), 유라시아 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), 유럽 (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

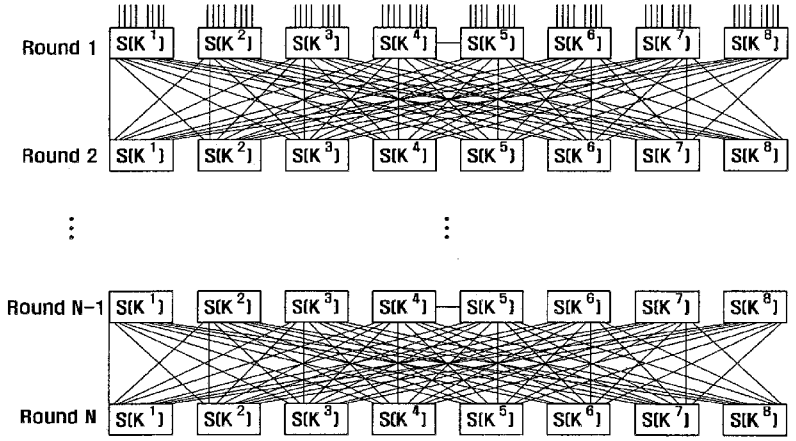
공개:
— 국제조사보고서 없이 공개하며 보고서 접수 후 이를 별도 공개함 (규칙 48.2(g))

[다음 쪽 계속]

(54) Title: ENCRYPTION SYSTEM USING DISCRETE CHAOS FUNCTION

(54) 발명의 명칭 : 이산화된 카오스 함수를 이용한 암호 시스템

【도 4】



(57) Abstract: The present relates to an encryption system comprising: an encryption round calculation unit for encrypting a plain text; and a substitution unit which is prepared at the encryption round calculation unit, is defined by a discrete chaos function using each of a plurality of key values as a parameter, and includes a plurality of S-boxes for performing a substitution calculation process for each of the words of the plain text which are divided by a plurality of numbers of key values. As the discrete chaos function becomes a reference of an S-box design and an encryption calculation operation is performed by the plurality of S-boxes, the present invention can be applied to a lightweight system having a small computational complexity.

(57) 요약서: 본 발명은

[다음 쪽 계속]

WO 2011/136614 A2

암호시스템에 관한 것으로, 평문을 암호화하기 위한 암호화 라운드 연산부; 및 상기 암호화 라운드 연산부에 마련되고, 복수의 키 값 각각을 파라미터로 하는 이산화된 카오스 함수에 의해 정의되며, 상기 복수의 키 값의 개수로 나누어지는 상기 평문의 워드들 각각에 대해 대체연산을 수행하기 위한 복수의 에스박스를 구비한 대체부를 포함하여, 이산화된 카오스 함수가 에스박스 디자인에 대한 기준으로 되고, 복수의 에스박스에 의해 암호화 연산이 수행되어 연산량이 적은 경량의 시스템에도 적용될 수 있는 효과가 있다.

【명세서】

【발명의 명칭】

이산화된 카오스 함수를 이용한 암호 시스템

【기술분야】

> 본 발명은 암호 시스템에 관한 것으로, 더욱 상세하게는 에스박스 디자인에 대한 기준을 제시함과 동시에 연산 능력이 적은 시스템에도 적용될 수 있는 이산화된 카오스 함수를 이용한 암호 시스템에 관한 것이다.

【배경기술】

> 네트워크 통신 및 전자 상거래의 발전에 따라 보안확보가 점점 중요해지고 있다. 보안확보의 방법 중 하나가 암호 시스템을 이용하여 정보에 대해 암호화하는 기술이다.

> 예측 불가능하고 무작위처럼 보이는 출력 값을 갖는 카오스 함수의 특성은 안전한 암호 시스템에서 요구하는 특성과 일치하여 여러 암호 시스템에서 제안되어 왔다. 하지만 대부분의 암호 시스템은 매우 높은 수준의 연산 능력을 필요로 하기 때문에 경량의 시스템에서는 그대로 적용하기가 어려운 것이 사실이다.

【발명의 상세한 설명】

【기술적 과제】

> 따라서, 본 발명이 해결하고자 하는 과제는, 에스박스 디자인에 대한 기준을 제시함과 동시에 연산량이 적어 경량의 시스템에도 적용될 수 있도록 하는 암호시스템을 제공하는 것이다.

【기술적 해결방법】

> 본 발명의 과제를 달성하기 위하여, 평문을 암호화하기 위한 암호화 라운드 연산부; 및 상기 암호화 라운드 연산부에 마련되고, 복수의 키 값 각각을 파라미터로 하는 이산화된 카오스 함수에 의해 정의되며, 상기 복수의 키 값의 개수로 나누어지는 상기 평문의 워드들 각각에 대해 대체연산을 수행하기 위한 복수의 에스박스를 구비한 대체부를 포함하는 암호시스템이 제공된다.

> 본 발명의 일 실시 예에 의하면, 상기 복수의 에스박스는 상기 복수의 키 값이 아래의 수학식에 대입되어 정의되는 것을 특징으로 한다.

[수학식]

$$S_{K_i}(x)=\begin{cases}\left\lfloor \frac{2^N}{K_i}(x+1)\right\rfloor -1, & 0\leq x<K_i\\ \left\lfloor \frac{2^N}{2^N-K_i}(2^N-x-1)\right\rfloor, & K_i\leq x<2^N\end{cases}$$

여기서, $S_{K_i}(X)$는 복수의 에스박스 중 어느 하나이고, K_i는 복수의 키값 중 어느 하나이다.

이때, 상기 복수의 에스박스는 입력과 상기 입력에 의한 상기 수학식의 결과의 대응 테이블인 것을 특징으로 한다.

또한, 상기 암호화 라운드 연산부에 마련되고, 상기 복수의 에스박스 각각의 출력에 대해 치환연산을 수행하기 위한 복수의 치환함수를 구비한 치환부를 더 포함하는 것을 특징으로 한다.

이때, 상기 복수의 치환함수는 상기 복수의 키 값의 개수와 동일한 개수의 워드들 각각과 아래의 수학식에 의해 정의되는 것을 특징으로 한다.

[수학식]

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

여기서, $r_i(X)$는 복수의 치환함수 중 어느 하나이고, 《는 오른쪽 순환을 의미하고, 》는 왼쪽 순환을 의미하고, $\oplus$는 비트간의 배타 논리합을 의미하고, ·는 비트 간 AND 연산을 의미하고, m_i는 입력워드(m_0-m_N)들 중 어느 하나이고, k는 사용자에 의해 설정되는 값이다.

【유리한 효과】

본 발명에 따르면, 이산화된 카오스 함수가 에스박스 디자인에 대한 기준으로 되고, 복수의 에스박스에 의해 암호화 연산이 수행되어 연산량이 적은 경량의 시스템에도 적용될 수 있는 효과가 있다.

【도면의 간단한 설명】

도 1은 종래의 카오스 함수를 이용하는 암호시스템에 이용되는 텐트 함수를 나타낸 그래프이다.

도 2는 SPN(Substitution-permutation network)구조의 암호 시스템을 나타낸 블록도이다.

도 3은 도 2과 같은 SPN 시스템에서 표 1과 같은 S-Box를 사용하는 경우, 입

력 값 X가 0000 0000 0000 0000이고 키 값 K^1이 1111 1111 1111 1111일 때 첫 번째 라운드의 수행 과정을 나타낸다.

> 도 4는 본 발명의 실시예에 따른 SPN 시스템을 도시한 것이다.

> 도 5는 본 발명의 일 실시 예에 따른 이산화된 텐트 함수를 이용하는 암호시스템을 나타낸 블록도이다.

> 도 6은 본 발명의 일 실시 예에 따른 이산화된 암호시스템의 평문에 대한 균일성 테스트를 수행한 결과를 나타낸 그래프이다.

> 도 7은 본 발명의 일 실시 예에 따른 이산화된 암호시스템의 키에 대한 균일성 테스트를 수행한 결과를 나타낸 그래프이다.

> 도 8은 본 발명의 일 실시 예에 따른 이산화된 암호시스템의 평문에 대한 암호문의 민감성 테스트를 수행한 결과를 나타낸 그래프이다.

> 도 9는 본 발명의 일 실시 예에 따른 이산화된 암호시스템의 평문에 대한 암호문의 민감성 테스트를 수행한 결과를 나타낸 그래프이다.

【발명의 실시를 위한 최선의 형태】

> 본 발명의 일 실시 예에 따른 이산화된 카오스 함수를 이용하는 암호시스템은 평문을 암호화하기 위한 암호화 라운드 연산부; 및 상기 암호화 라운드 연산부에 마련되고, 복수의 키 값 각각을 파라미터로 하는 이산화된 카오스 함수에 의해 정의되며, 상기 복수의 키 값의 개수로 나누어지는 상기 평문의 워드들 각각에 대해 대체연산을 수행하기 위한 복수의 에스박스를 구비한 대체부를 포함한다.

【발명의 실시를 위한 형태】

> 이하, 본 발명의 실시 예를 들어 본 발명을 더욱 상세하게 설명한다. 그러나 본 발명의 실시 예는 본 발명을 더욱 구체적으로 설명하기 위한 것으로, 본 발명의 범위가 이에 제한되지 않는다는 것은 본 발명이 속하는 기술분야에 속하는 통상의 지식을 가진 자에게 자명할 것이다.

> 카오스 함수를 이용하는 암호시스템은 예측 불가능하고 무작위처럼 보이는 출력 값을 갖는 카오스 함수를 이용한 것이다. 카오스 함수를 이용하는 암호시스템에는 텐트 함수를 이용하는 암호시스템이 있다. 텐트 함수를 이용하는 암호시스템은 텐트 함수와 이의 역함수를 이용하여 암호화와 복호화를 수행한다.

> 본 발명의 실시예에서는 연산량이 적어 경량의 암호 시스템에 적용할 수 있도록 하는 카오스 함수 중 가장 간단하면서도 널리 사용되는 텐트 함수를 적용하고자 한다. 텐트 함수란 일차원의 부분적인 선형 함수(piecewise linear map)의 일종이다. 이 함수는 [0,1]의 구간을 정의역으로 하여 같은 크기의 치역을 가지며, 오

직 하나의 파라미터 α만을 갖는 특징을 가지고 있다.

도 1은 종래의 카오스 함수를 이용하는 암호시스템에 이용되는 텐트 함수를 나타낸 그래프이다.

텐트 함수는 수학식 1과 수학식 2와 같이 정의되며 도 1과 같은 그래프로 표현되는 텐트 함수를 이용하여 복호화를 수행하고, 수학식 2와 같이 정의되는 텐트 함수의 역함수를 이용하여 암호화를 수행한다. 평문에 수학식 2와 같은 텐트 함수의 역함수를 적용할 때 발생하는 출력 값 중 하나를 취하는 방식을 연속적으로 수행하여 평문에 대해 암호화한다. 암호문에 아래의 수학식 1과 같은 텐트 함수를 연속적으로 적용하여 암호문에 대해 복호화한다.

【수학식 1】

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

여기서, 정의역(x)은 0에서 1 사이의 실수이고, α는 파라미터이다.

【수학식 2】

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

여기서, 정의역(y)은 0에서 1 사이의 실수이고, α는 파라미터이다.

그런데, 이러한 텐트 함수를 이용하는 암호시스템은 텐트 함수와 텐트 함수의 역함수가 일대일 함수가 아니고, 각 라운드의 입력 값과 출력 값이 정수가 아닌 실수이고, 텐트 함수와 텐트 함수의 역함수가 부분적인 선형함수이기 때문에 차분 암호 공격에 취약한 단점이 있다.

텐트 함수를 이용하는 암호시스템에 대하여 보다 상세하게 살펴보면 다음과 같다.

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

텐트 함수를 이용한 가장 간단한 형태의 암호 시스템은 다음과 같다.

- 비밀키 : 파라미터 α
- 암호화 : 암호화하고자 하는 메세지를 이용해 평문 p를 얻는다. 이 때, p

는 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 방식은 몇 가지 단점이 있다. 첫째 f_α와 f_α^{-1}은 일대일 함수가 아니고 둘째 각 라운드의 입력 값과 출력 값은 정수가 아닌 실수이며 마지막으로 f_α와 f_α^{-1}은 부분적으로 선형(piecewise linear)이기 때문에 선형 혹은 차분 암호 공격에 대하여 취약점을 갖는다.

이러한 단점을 보완하기 위해 수학식 3과 같이 정의되는 이산화된 텐트 함수를 이용하여 평문을 암호화하고, 수학식 4와 같이 정의되는 이산화된 텐트 함수의 역함수를 이용하여 암호문을 복호화하는 이산화된 텐트 함수를 이용하는 암호시스템을 이하에서 설명하기로 한다.

【수학식 3】

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

여기서, 정의역(X)은 1에서 M사이의 정수이고, A는 이산화된 텐트 함수의 파라미터이다. A는 1에서 M사이의 정수값을 갖는다.

【수학식 4】

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

여기서, 정의역(Y)은 1에서 M사이의 정수이고, A는 이산화된 텐트 함수의 파

라미터이고, X_1, X_2 및 m(Y)는 아래와 같이 정의된다.

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

위와 같이 정의된 이산화된 텐트 함수는 일대일 대응을 가지며 카오스 함수의 성질을 만족시킨다.

다음은 위의 내용을 기반하고 있는 이산화된 텐트 함수를 이용한 암호 시스템을 설명하기로 한다.

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

- 비밀키 : 파라미터 A

- 암호화 : 평문 P를 초기값으로 하여 아래와 같은 수식처럼 F_A를 연속적으로 수행해 암호문 C를 얻는다.

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

- 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.

또한, 이산화된 카오스 함수를 이용하는 암호시스템은 암호화하고자 하는 평문 전체를 대상으로 하여 카오스 함수 연산을 반복하여 수행하기 때문에 매우 높은 수준의 연산 능력이 요구되는 단점이 있다. 즉, 64비트(bit) 암호시스템을 가정할 때, 이산화된 카오스 함수를 적용하기 위해서는 최대 2^{64} 크기의 정수들을 대상으로 곱셈과 나눗셈으로 이루어진 실수 연산들을 반복적으로 수행해야 하기 때문에 연산 능력이 적은 시스템에 이산화된 텐트 함수를 이용하는 암호시스템을 적용하기에 무

리가 있다.

도 2는 SPN(Substitution-permutation network)구조의 암호 시스템을 나타낸 블록도이다.

표 1은 SPN구조를 이용한 암호시스템에 이용되는 에스박스의 표를 나타낸 것이다. 표 1에서 z는 입력 값이고 $\pi_s(z)$는 출력 값이다.

【표 1】

z: 입력	$\pi_S(z)$: 출력
0000	1110
0001	0100
0010	1101
0011	0001
0100	0010
0101	1111
0110	1011
0111	1000
1000	0011
1001	1010
1010	0110
1011	1100
1100	0101
1101	1001
1110	0000
1111	0111

도 2를 참조하면, SPN구조를 가지는 암호시스템(100)은 키 연산계층(110)과 대체계층(120: Substitution) 및 치환계층(130: Permutation)을 포함한다. 이러한 SPN구조를 가지는 암호 시스템은 아래의 (1)-(3)과 같은 세 단계로 구성되는 라운드를 수회 수행하여 평문을 암호화한다.

(1) 우선, 입력 값(X)이 들어오면 키 연산계층(110)에서 입력 값(X)과 키 값(K)에 대해 배타 논리합(XOR) 연산을 수행한다.

(2) 그 다음, 대체 계층(120)에서 배타 논리합(XOR) 연산 결과에 대해 도 2에서 도시되는 바와 같은 표로 표현되는 에스박스를 이용하여 대체를 수행한다.

(3) 마지막으로, 치환 계층(130)에서 대체 수행 결과에 대해 치환을 하여 다음 라운드의 입력이 되도록 한다.

그러나, SPN 구조의 암호시스템은 에스박스의 설계 기준이 없어 실험적으로 최적의 에스박스를 만들어야 하는 단점이 있다.

SPN 시스템에서는 위에서 설명한 라운드가 N번 반복적으로 수행된다. S-Box는 입력 값이 z일 경우 그에 따른 출력 값 $\pi_s(z)$으로 표현할 수 있으며, 표 1은 4비트의 입력을 4비트의 출력으로 대체하는 S-Box 함수 $\pi_s(z)$의 예시이다.

도 3은 도 2과 같은 SPN 시스템에서 표 1과 같은 S-Box를 사용하는 경우, 입력 값 X가 0000 0000 0000 0000이고 키 값 K^1이 1111 1111 1111 1111일 때 첫 번째 라운드의 수행 과정을 나타낸다.

u^1은 입력 값과 키 값을 XOR 연산한 결과를 나타내며, u^1은 대체(Substitution)를 수행하는 S-Box의 입력 값이 된다. 다음으로 v^1은 입력 값에 해당되는 출력 값을 나타내며 위의 표 1에서 입력 값에 따른 출력 값을 확인할 수 있다. 마지막으로 w^1은 v^1를 치환한 결과로써 다음 라운드의 입력 값이 된다.

도 2에 도시된 SPN 시스템은 키와 S-box가 따로 설계되었지만 본 발명의 실시예에 따른 SPN 시스템에서는 S-box를 디자인하는 파라미터로 키 값을 사용하였으며 암호화하고자 하는 평문 전체를 대상으로 카오스 함수를 N번 반복 수행한다.

본 발명에서는 이산화된 텐트 함수를 이용하되, 연산 능력이 적은 소형 시스템에서 64bit 암호 시스템을 사용하더라도 높은 수준의 연산 능력이 필요하지 않은 경량의 새로운 암호 시스템을 개시하고자 한다.

본 발명의 실시예에 따른 암호 시스템은 64 bits의 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.

도 4는 본 발명의 실시예에 따른 SPN 시스템을 도시한 것이다.

본 발명의 실시예에 따른 SPN 시스템을 도 4을 참조하여 상세히 살펴보기로 한다.

1. 대체(Substitution) S_k

암호 시스템에 사용될 64 bits의 키를 K라 하면 K는 다음과 같은 8개의 서브

키로 나뉘어질 수 있다.

$K=(K_0K_1\cdots K_7)$

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

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

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.

$X = (X_0X_1\cdots X_7)$

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.

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

2. 치환(Permutation) π

우선 64 bits의 메시지를 입력으로 받아 8 bits의 출력을 내는 함수 γ_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, 《와 》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 π(X)=γ^-1(X), π^-1(X)=γ(X)로 정의한다.

3. 암호화/복호화(Encryption/Decryption)

암호화와 복호화를 위한 라운드 함수는 각각 다음과 같이 정의된다.

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

마지막으로 암호화와 복호화는 다음과 같은 과정을 통하여 이루어진다.

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

도 5는 본 발명의 일 실시 예에 따른 이산화된 텐트 함수를 이용하는 암호시스템을 나타낸 블록도이다.

도 5를 참조하면, 본 발명의 일 실시 예에 따른 암호시스템은 평문을 암호화하기 위해 라운드 연산을 수행하는 복수의 암호화 라운드 연산부(110-1~100-n)를 구비한 암호부(100) 및 암호문을 복호화하기 위해 라운드 연산을 수행하는 복수의 복호화 라운드 연산부(210-1~210-n)를 구비한 복호부(200)를 포함한다.

복수의 암호화 라운드 연산부(110-1~100-n) 각각은 복수의 키 값(K_0-K_N) 각각을 파라미터로 하고, 복수의 키 값(K_0-K_N)의 개수로 나누어지는 평문 입력(X)의 워드들(X_0-X_N) 각각에 대해 대체연산을 수행하기 위한 복수의 에스박스(SK^0-SK^N)를 구비한 대체부(S)와, 대체부(S)의 복수의 에스박스(SK^0-SK^N) 각각의 출력에 대해 치환연산을 수행하기 위한 복수의 치환함수(r_0-r_N)를 구비한 치환부(P)를 포함한다.

복수의 에스박스(SK^0-SK^N) 각각은 복수의 키 값(K_0-K_N) 각각과 아래의 수학식 5와 같은 이산화된 카오스 함수에 의해 정의된다. 여기서, 복수의 키 값(K_0-K_N)은 사용자에 의해 설정되는 값이다. 복수의 키 값들(K_0-K_N)의 개수는 본 발명의 일 실시 예에 따른 암호시스템 설계자에 의해 선택된다.

【수학식 5】

$$S_{K_i}(x)=\begin{cases}\left\lfloor \frac{2^N}{K_i}(x+1)\right\rfloor -1, & 0\leq x<K_i\\ \left\lfloor \frac{2^N}{2^N-K_i}(2^N-x-1)\right\rfloor , & K_i\leq x<2^N\end{cases}$$

여기서, $S_{K_i}(X)$는 복수의 에스박스 중 어느 하나이고, K_i는 복수의 키값 중 어느 하나이다.

이러한 복수의 에스박스(SK^0-SK^N) 각각은 워드들(K_0-K_N) 각각에 대해 수학식 5와 같은 이산화된 텐트 함수를 통해 대체연산을 수행한다.

한편, 복수의 에스박스(SK^0-SK^N) 각각은 수학식 5에 대응하는 테이블로 구현될 수 있다. 즉, 특정의 입력(X)과 특정의 입력(X)에 의한 수학식 5의 연산 값의 대응 테이블로 구현될 수 있다.

복수의 치환함수(γ_0-γ_N) 각각은 복수의 키 값(K_0-K_N)의 개수와 동일한 개수의 워드들(m_0-m_N) 각각과 아래의 수학식 6에 의해 정의된다.

【수학식 6】

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

여기서, 여기서 $\gamma_i(X)$는 복수의 치환함수 중 어느 하나이고, 《는 오른쪽 순환을 의미하고, 》는 왼쪽 순환을 의미하고, $\oplus$는 비트간의 배타 논리합을 의미하고, ·는 비트 간 AND 연산을 의미하고, m_i는 입력워드(m_0-m_N)들 중 어느 하나이고, k는 사용자에 의해 설정되는 값이다.

이러한 복수의 치환함수들(r_0-r_N) 각각은 복수의 에스박스(SK^1-SK^N) 각각의 출력(X_0-X_k)에 대해 치환연산을 수행한다.

암호부(100)는 복수의 라운드 연산부(110-1~110-n) 각각을 통해 평문에 대해 복수의 라운드 연산을 수행하여 평문을 암호화한다.

복수의 복호화 라운드 연산부(210-1~210-n) 각각은 복수의 암호문 입력을 이루는 복수의 워드 각각에 대해 역치환하기 위한 복수의 역치환함수들(r_0^{-1}~r_N^{-1})을 구

비한 역 치환부(P^{-1})와 역 치환부(P^{-1})의 출력을 이루는 각각의 워드에 대해 역 대체 연산을 수행하기 위한 복수의 역에스박스들(SK^{0-1}~SK^{N-1})을 구비한 역대체부(S^{-1})를 포함한다.

여기서, 복수의 역치환함수(r_0^{-1}-r_N^{-1}) 각각은 복수의 치환함수(r_0-r_N) 각각의 역함수이고, 복수의 역에스박스(SK^{0-1}-SK^{N-1}) 각각은 복수의 에스박스(SK^0-SK^N) 각각을 정의하는 수학식 6의 역함수들이므로, 역 치환부(P^{-1})와 역대체부(S^{-1})에 대한 상세한 설명은 생략하기로 한다.

복호부(200)는 복수의 복호 라운드 연산부(210_1~210_n) 각각을 통해 암호문에 대해 복수의 복호 라운드 연산을 수행하여 암호문을 복호화한다.

이하에서는 본 발명의 일 실시 예에 따른 암호시스템의 효과들 중 연산량과 안전도에 대해 보다 상세히 설명하기로 한다.

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 발명에서 제안된 방식을 이용할 경우에는, 각 라운드 함수를 수행하기 위하여 2^8크기의 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_K의 입력 값과 출력 값을 테이블로 작성하여 메모리에 보관한 후 이 테이블을 이용한다면, 매우 적은 양의 연산만으로도 암호화와 복호화를 수행할 수 있을 것이다.

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.

다음은 제안한 암호 시스템이 위에서 제시한 조건들을 만족시킴을 보이기 위한 통계적 실험의 결과를 제시하였다. 이와 같은 테스트 결과를 통하여 본 발명의 효과를 나타 낼 수 있다.

① 균일성 테스트 (U-P, U-K)

(a) 평문에 대한 암호문의 균일성 테스트는 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.

한편, 도 6은 본 발명의 일 실시 예에 따른 이산화된 암호시스템의 평문에 대한 균일성 테스트를 수행한 결과를 나타낸 그래프이다. 도 6은 M이 2^{64}이고, b가 2^8이고, n이 2^{16} 일 때 연속적인 구간 각각에 포함된 암호문의 빈도를 나타낸 그래프이다. 도 6에서 도시되는 바와 같이, 본 발명의 일 실시 예에 따른 이산화된 암호시스템에 의해 연속적인 구간 각각에 포함된 암호문의 빈도가 대체로 균일하게 나타나 평문에 대한 암호문의 균일성이 우수하였다.

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

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

한편, 도 7은 본 발명의 일 실시 예에 따른 이산화된 암호시스템의 키에 대한 균일성 테스트를 수행한 결과를 나타낸 그래프이다. 도 7은 M이 2^{64}이고, b가2^{8}이고, n이 2^{16} 일 때 연속적인 구간 각각에 포함된 암호문의 빈도를 나타낸 그래프이다. 도 7에서 도시되는 바와 같이, 본 발명의 일 실시 예에 따른 이산화된 암호시스템에 의해 연속적인 구간 각각에 포함된 암호문의 빈도가 대체로 균일하게 나타나 키에 대한 균일성이 우수하였다.

(c) 다음의 표준 편차 값을 구한다.

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

도 6와 도 7에 특정한 입력 값 X(K)에 대하여 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)

(a) 평문에 대한 암호문의 민감성 테스트는 암호문이 분포되어 있는 영역 [1,M]을 같은 크기를 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.

한편, 도 8은 본 발명의 일 실시 예에 따른 이산화된 암호시스템의 평문에 대한 암호문의 민감성 테스트를 수행한 결과를 나타낸 그래프이다. 도 8은 M이 2^{64}이고, b가 2^{8}이고, n이 2^{16} 일 때 연속적인 구간 각각에 포함된 암호문 쌍의 빈도를 나타낸 그래프이다. 도 8에서 도시되는 바와 같이, 본 발명의 일 실시 예에 따른

이산화된 암호시스템에 의해 연속적인 구간 각각에 포함된 암호문의 빈도는 대체로 균일하게 나타나 평문에 대한 암호문의 민감성이 우수하였다.

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

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

키에 대한 암호문의 민감성 테스트는 암호문이 분포되어 있는 [1,M]을 같은 크기를 갖는 b개의 연속적인 구간으로 나누고, 암호문 3과 같은 n개의 암호문 쌍의 값을 구하고, 각각의 암호문 쌍이 각각의 구간에 포함되어 있는 빈도(n_{ij})를 구하는 방식으로 테스트한다.

한편, 도 9는 본 발명의 일 실시 예에 따른 이산화된 암호시스템의 평문에 대한 암호문의 민감성 테스트를 수행한 결과를 나타낸 그래프이다. 도 9는 M이 2^{64}이고, b가 2^{8}이고, n이 2^{16} 일 때 연속적인 구간 각각에 포함된 암호문 쌍의 빈도를 나타낸 그래프이다. 도 9에서 도시되는 바와 같이, 연속적인 구간 각각에 포함된 암호문의 빈도는 대체로 균일하게 나타나 키에 대한 암호문의 민감성이 우수하였다.

(c) 다음의 표준 편차 값을 구한다.

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

도 8과 도 9에 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 편차의 값은 평균적으로 대략 16으로 나타난다.

이상과 같이 본 발명에서는 구체적인 구성 요소 등과 같은 특정 사항들과 한정된 실시예 및 도면에 의해 설명되었으나 이는 본 발명의 보다 전반적인 이해를 돕기 위해서 제공된 것일 뿐, 본 발명은 상기의 실시예에 한정되는 것은 아니며, 본 발명이 속하는 분야에서 통상적인 지식을 가진 자라면 이러한 기재로부터 다양

한 수정 및 변형이 가능하다. 따라서, 본 발명의 사상은 설명된 실시예에 국한되어 정해져서는 아니되며, 후술하는 특허청구범위뿐 아니라 이 특허청구범위와 균등하거나 등가적 변형이 있는 모든 것들은 본 발명 사상의 범주에 속한다고 할 것이다.

【청구의 범위】

【청구항 1】

평문을 암호화하기 위한 암호화 라운드 연산부; 및

상기 암호화 라운드 연산부에 마련되고, 복수의 키 값 각각을 파라미터로 하는 이산화된 카오스 함수에 의해 정의되며, 상기 복수의 키 값의 개수로 나누어지는 상기 평문의 워드들 각각에 대해 대체연산을 수행하기 위한 복수의 에스박스를 구비한 대체부를 포함하는 암호시스템.

【청구항 2】

제1항에 있어서,

상기 복수의 에스박스는 상기 복수의 키 값이 아래의 수학식에 대입되어 정의되는 것을 특징으로 하는 암호시스템.

[수학식]

$$S_{K_i}(x)=\begin{cases}\left\lfloor \frac{2^N}{K_i}(x+1)\right\rfloor -1, & 0\le x<K_i\\ \left\lfloor \frac{2^N}{2^N-K_i}(2^N-x-1)\right\rfloor , & K_i\le x<2^N\end{cases}$$

여기서, $S_K(X)$는 복수의 에스박스 중 어느 하나이고, K_i는 복수의 키값 중 어느 하나이다.

【청구항 3】

제2항에 있어서,

상기 복수의 에스박스는 입력과 상기 입력에 의한 상기 수학식의 결과의 대응 테이블인 것을 특징으로 하는 암호시스템.

【청구항 4】

제1항에 있어서,

상기 암호화 라운드 연산부에 마련되고, 상기 복수의 에스박스 각각의 출력에 대해 치환연산을 수행하기 위한 복수의 치환함수를 구비한 치환부를 더 포함하는 것을 특징으로 하는 암호시스템.

【청구항 5】

제4항에 있어서,

상기 복수의 치환함수는 상기 복수의 키 값의 개수와 동일한 개수의 워드들 각각과 아래의 수학식에 의해 정의되는 것을 특징으로 하는 암호시스템.

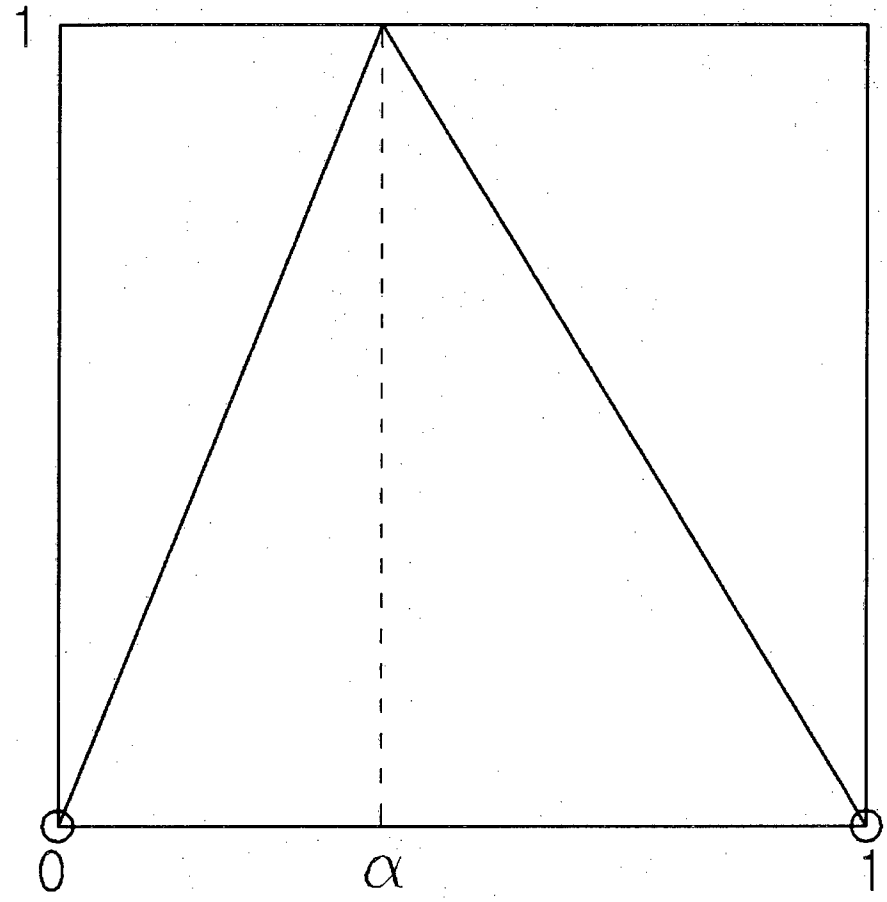
[수학식]

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

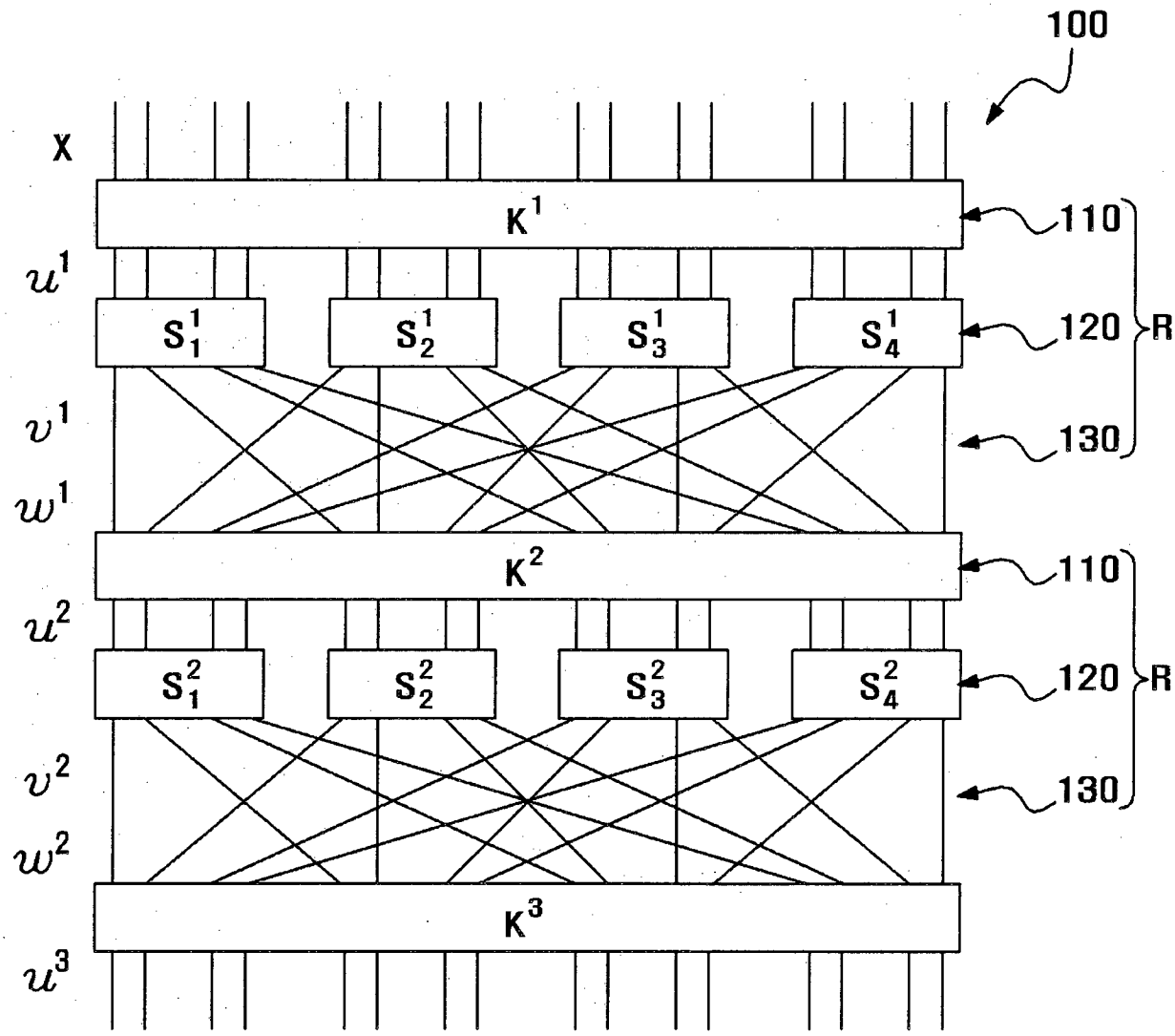
여기서, $\gamma_i(X)$는 복수의 치환함수 중 어느 하나이고, ≪는 오른쪽 순환을 의미하고, ≫는 왼쪽 순환을 의미하고, ⊕는 비트간의 배타 논리합을 의미하고, ·는 비트 간 AND 연산을 의미하고, m_i는 입력워드(m_0-m_N)들 중 어느 하나이고, k는 사용자에 의해 설정되는 값이다.

【도면】

【도 1】



【도 2】


100
X
K^1
110
u^1
S_1^1
S_2^1
S_3^1
S_4^1
120
R
v^1
130
w^1
K^2
110
u^2
S_1^2
S_2^2
S_3^2
S_4^2
120
R
v^2
130
w^2
K^3
u^3

【도 3】

$$X = 0000\ 0000\ 0000\ 0000$$

$$K^1 = 1111\ 1111\ 1111\ 1111$$

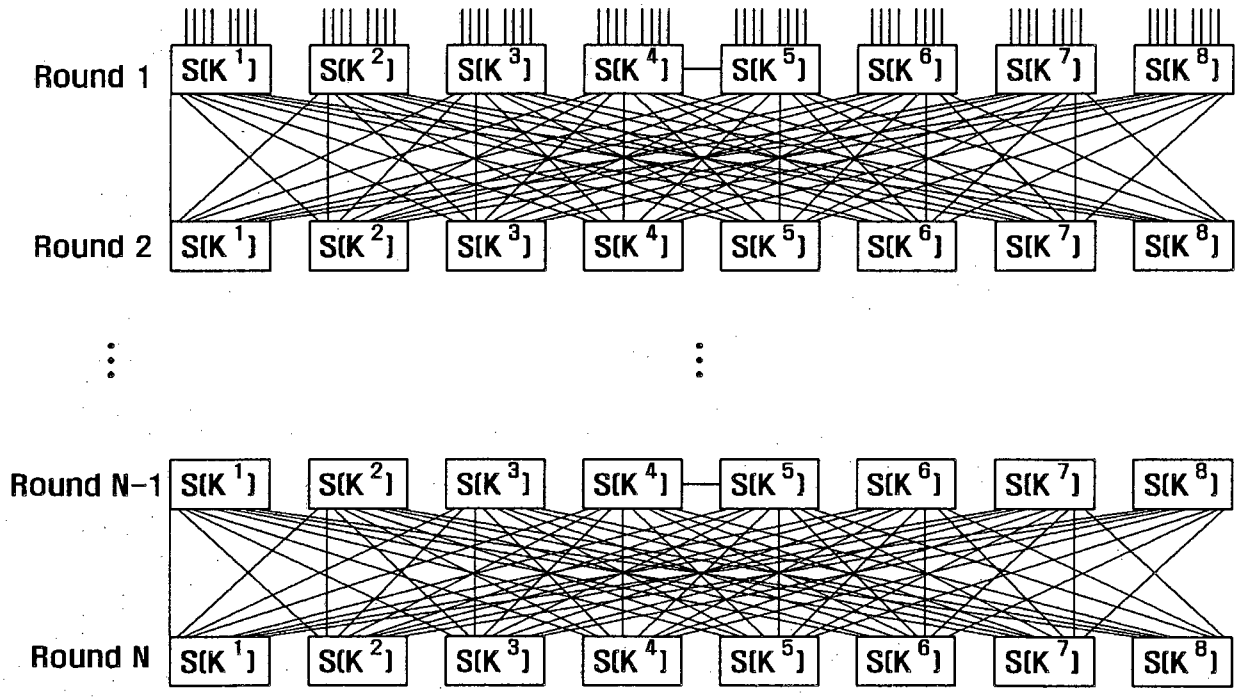
$$S_1^1 = S_2^1 = S_3^1 = S_4^1$$

$$u^1 = 1111\ 1111\ 1111\ 1111$$

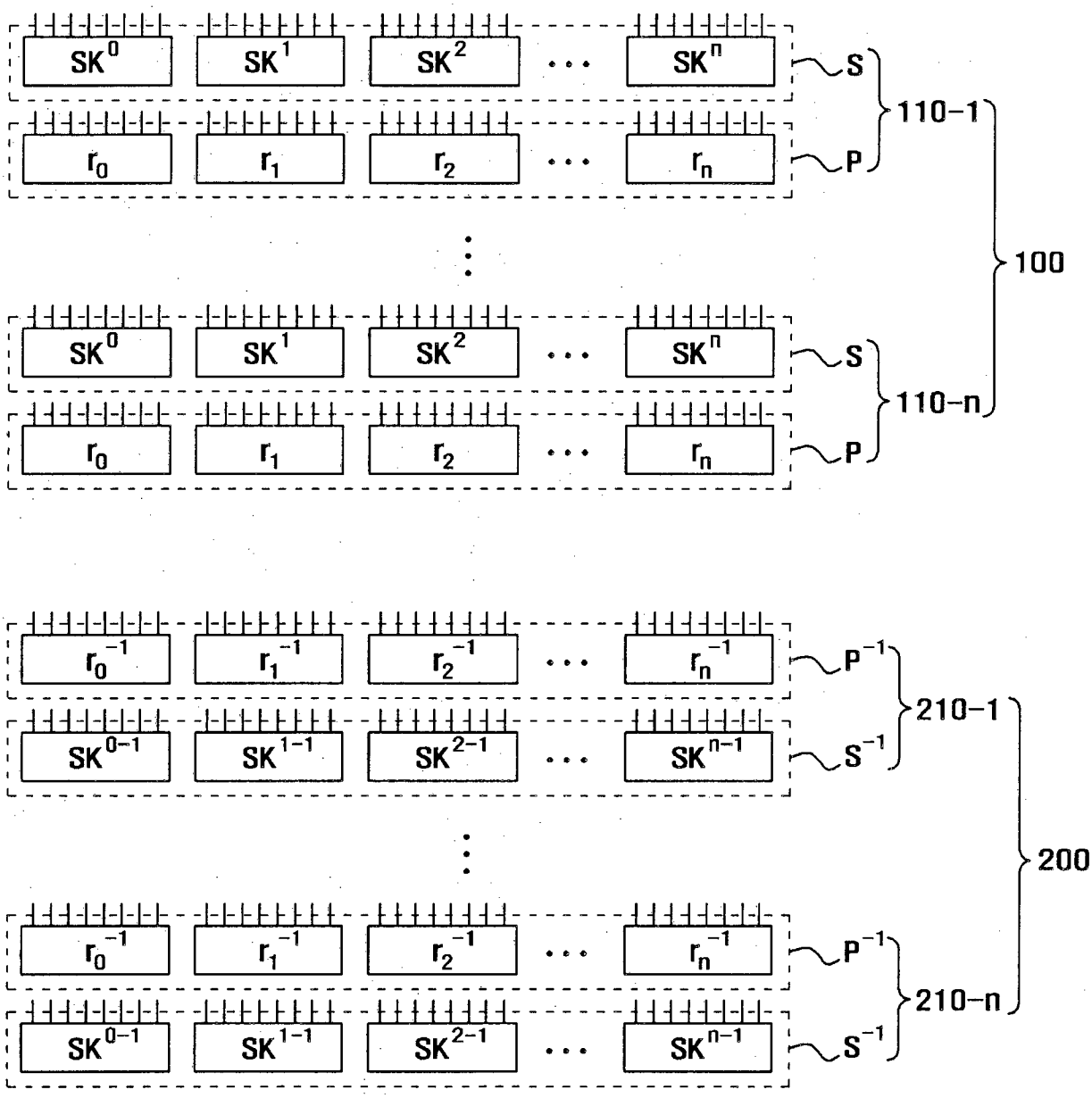
$$v^1 = 0111\ 0111\ 0111\ 0111$$

$$w^1 = 0000\ 1111\ 1111\ 1111$$

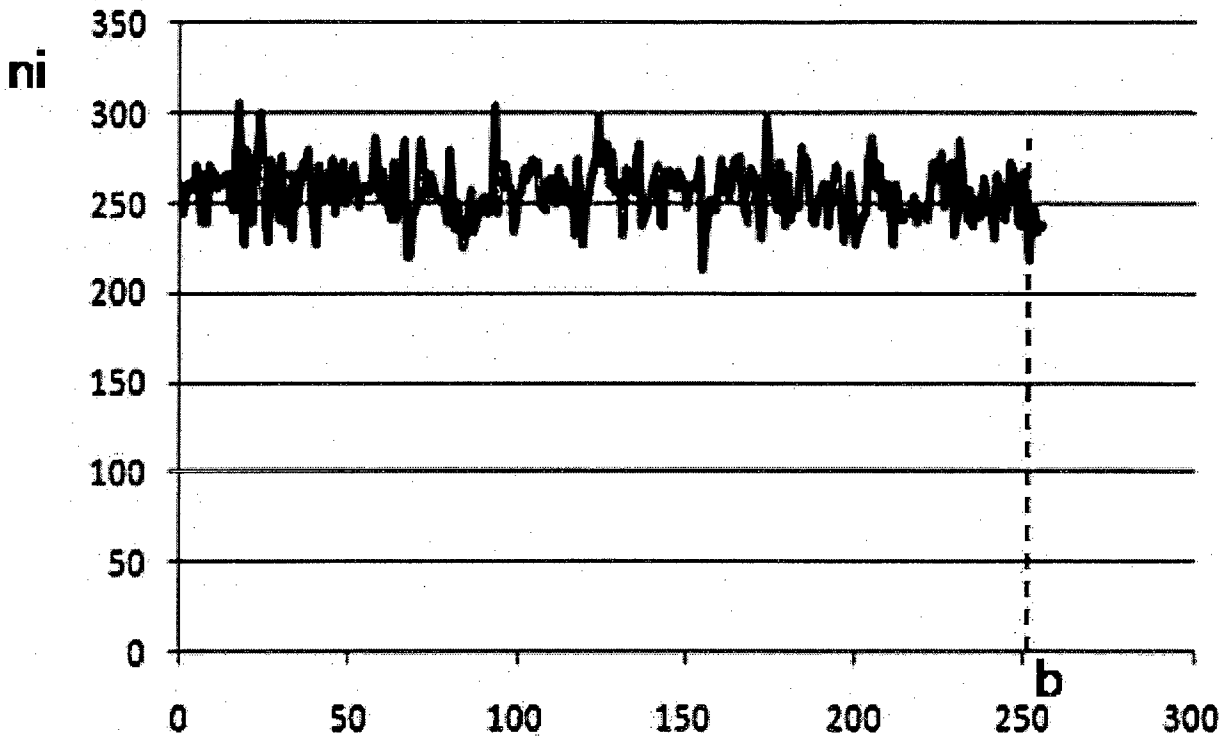
【도 4】



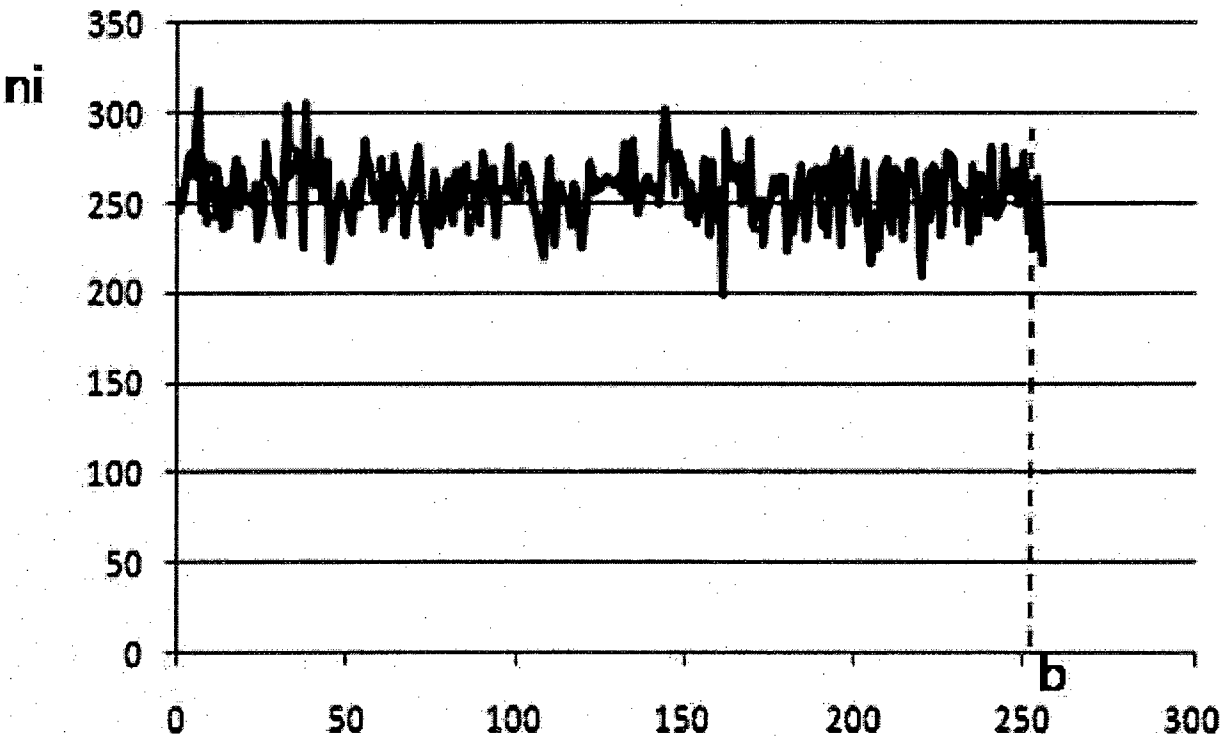
【도 5】


SK0
SK1
SK2
SKn
S
r0
r1
r2
rn
P
110-1
110-n
100
r0-1
r1-1
r2-1
rn-1
P-1
SK0-1
SK1-1
SK2-1
SKn-1
S-1
210-1
210-n
200

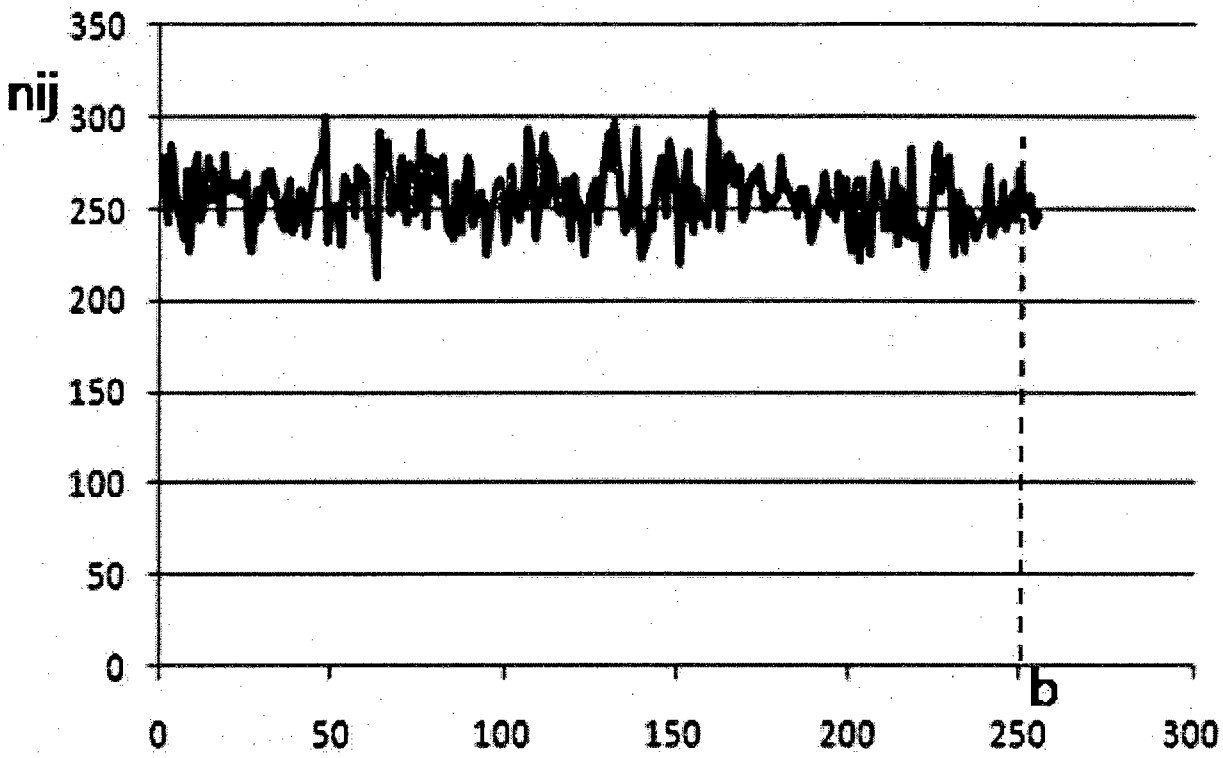
【도 6】


ni
350
300
250
200
150
100
50
0
0
50
100
150
200
250
300
b

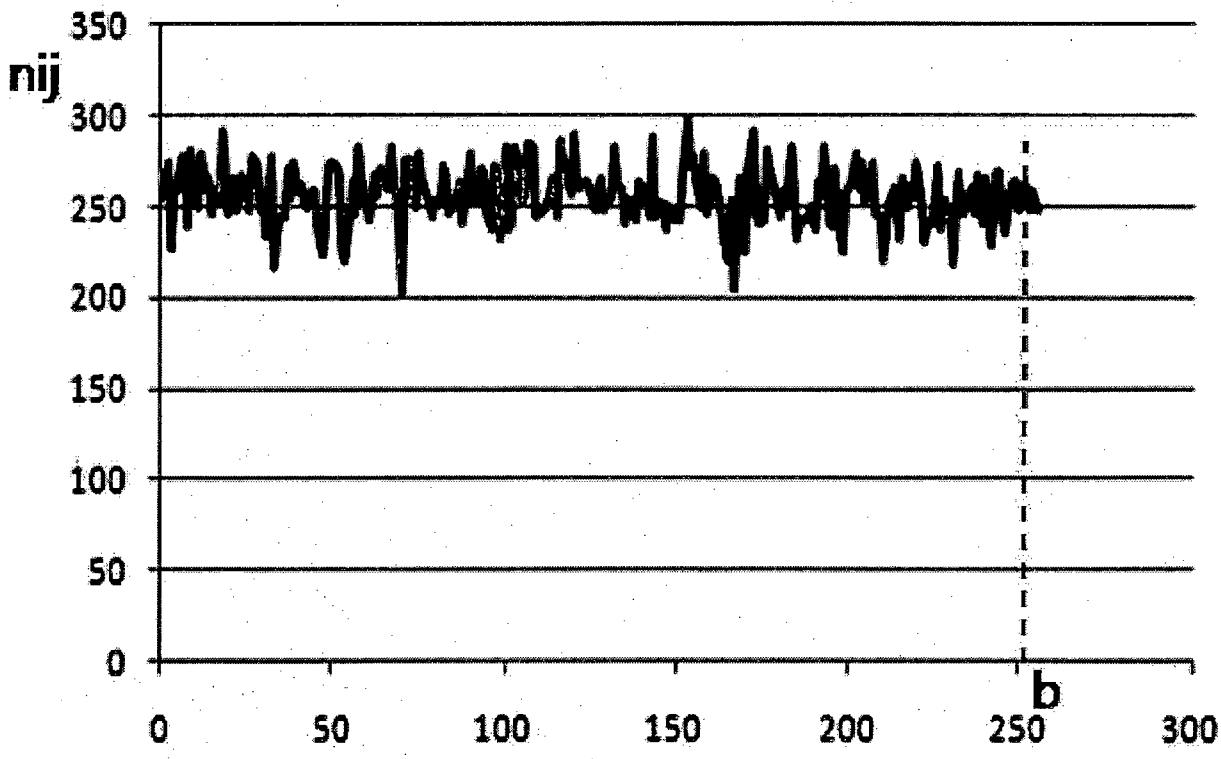
【도 7】


ni
350
300
250
200
150
100
50
0
0
50
100
150
200
250
300
b

【도 8】


nij
350
300
250
200
150
100
50
0
0
50
100
150
200
250
300
b

【도 9】


nij
350
300
250
200
150
100
50
0
0
50
100
150
200
250
300
b