韓國컴퓨터情報學會 論文誌
第14卷 第7號, 2009. 7.

2009-14-7-3-3

유무선 네트워크 환경에 적합한 VCR 암호시스템 설계에 관한 연구

이 선 근*

A Study on the VCR Cryptographic System Design Adapted in Wire/Wireless Network Environments

Seon-Keun Lee *

요 약

본 논문은 네트워크 환경과 유/무선 통신망에 적합하며 구현상의 크기 및 재구성을 수행할 수 있으며 TCP/IP 프로토콜 구조에 적합한 VCR 암호알고리즘을 제안하고 하드웨어 칩 레벨로 구현하였다.

제안된 VCR 암호알고리즘은 TCP/IP 프로토콜의 보안 취약성을 보강하며 네트워크 환경에서 가변 라운드횟수 기능을 가짐으로서 다수의 사용자에 대한 보안을 유지하는데 주요한 목적이 있기 때문에 실시간 처리 및 대용량 데이터의 암호화 및 다자간 통신에 매우 유리하다.

Abstract

This paper proposed VCR cryptographic algorithm that adapted in TCP/IP protocol architecture and wire/wireless communication network environments. we implemented by hardware chip level because proposed VCR cryptographic algorithm perform scalable & reconfigurable operations into the security system.

Proposed VCR cryptographic algorithm strengthens security vulnerability of TCP/IP protocol and is very profitable real-time processing and encipherment of high-capacity data and multi-user communication because there is important purpose to keep security about many user as that have variable round numbers function in network environments.

▸ Keyword :암호알고리즘(Cryptographic algorithm), TCP/IP(TCP/IP), 통신(Communication), AES(AES), 라운드 보안 분야(Round Security field)

• 제1저자 : 이선근
• 투고일 : 2009. 04. 15, 심사일 : 2009. 06. 16, 게재확정일 : 2009. 07. 18.
* (주)율시스템즈 연구소장

Ⅰ. 서 론

현대 정보화 사회에서 네트워크 환경을 배제한 정보는 가치가 없다. 그러므로 정보의 네트워킹이 이루어져야한다. 네트워킹을 수행하기 위하여 사용되어지는 일반적인 TCP/IP 프로토콜은 보안에 관련된 기능이 IPv6가 있지만 계속적인 네트워크 및 시스템 발전으로 인하여 보안기능의 발전은 계속되어지거나 다른 방법을 사용하여 보안을 유지하여야 한다[1][7].

본 논문에서는 이와 같은 문제점들을 해결하고자 AES를 변형한 블록 암호알고리즘인 VCR(Symmetric Block Cryptographic Algorithm with Variable Computation Rounding) 암호 알고리즘을 제안하였다.

VCR 암호알고리즘은 구조적으로 대칭형과 같은 특징을 가지기 때문에 처리속도 및 암/복호화가 용이하고 가변 라운딩 연산을 포함하기 때문에 비도가 증대되었다. 또한 scalable 및 reconfigurable한 특징은 IP의 재사용이 가능하도록 하였으며 여러 가지 암호화에 필요한 키 생성 방법은 RTT(Round Trip Time) 방법에 노출되지 않기 위하여 VKG(Variable Keying Generation) 기법을 사용하였다. 사용된 VKG 기법은 입력데이터와 종속관계이므로 외부에서의 크랙 및 해킹이 어려우며 결정론적 라운드가 아닌 매 순간마다 결정되는 라운드에 의한 키 값을 생성한다.

그러므로 구현된 VCR 암호시스템은 대용량, 실시간 처리가 요구되어지는 휴대용 멀티미디어 응용서비스를 제공하기 위한 플랫폼에 적용이 용이하기 때문에 향후 기하급수적인 보급이 예상되는 PDA 및 휴대용 통신기기 등의 시스템에 매우 유용하리라 생각된다.

Ⅱ. 대칭형 암호알고리즘

대칭형 암호방식은 암호키와 복호키가 동일하므로 대칭키 암호방식이라고도 하며, 두 개체가 같은 키를 공유하면서 암/복호화를 수행한다. 대칭형 암호방식은 알고리즘 자체의 구조적 개념을 이용하여 암/복호화를 수행하기 때문에 수행 속도가 비대칭형 방식에 비하여 매우 빠른 장점을 가진다. 그러나 많은 수의 사용자가 네트워크 환경에 연결되어 있을 경우 키 관리 및 보관, 유지 등의 공유 문제가 발생한다는 것과 키 자체를 상대방에게 안전하게 전송해야 한다는 문제가 있다. 대칭형 암호방식은 비대칭형 암호방식에 비하여 월등히 처리 속도가 빠르고 구현상의 복잡도가 낮아 구현하기에 용이하기 때문에 매우 유용한 암호화 방식이다. 대칭형 암호 방식은 데이터 처리 방식에 따라 블록(block) 암호방식과 스트림(stream) 암호방식 등으로 분류된다[1].

블록암호는 기본적으로 비선형 변환과 선형변환의 적절한 조합에 의해 설계되며 전체구조는 선형 변환을 적용시키는 Feistel 구조와 비선형 변환을 적용시키는 SPN 구조로 나눌 수 있다. DES, Blowfish, CAST128, LOKI91, MISTY, RC5, CAST256, DFE, E2, MARS, RC6, Twofish등이 Feistel 구조를 바탕으로 설계된 것들이며 SAFER, IDEA, Square, Crypto, Rijndael, SAFER+, Serpent 등이 SPN 구조를 바탕으로 설계된 알고리즘들이다[1][7][8].

블록암호에서 가장 중요한 비선형 변환에는 테이블을 이용하는 치환, 곱셈, 가변데이터에 의한 회전 및 이들과 서로 양립하지 않는 연산들의 결합 등이 이용된다. 각 연산에 따라 안전도, 프로세서 또는 하드웨어에 따른 효율성에 있어서 장단점이 있으나 일반적으로 작은 단위의 S-box를 적절히 이용하는 것이 대부분의 플랫폼에서 보다 효율적이다[5][6].

블록암호에 대한 가장 단순한 공격방법은 하나의 평문과 암호문 쌍에 대해 모든 가능한 키 값으로 주어진 평문을 암호화하여 주어진 암호문이 나오는지를 검사하는 전수 키 검사이다. 이러한 전수검사방법은 기술의 발전에 따른 키 길이를 결정하는 기준이 되며 현재 전문가들이 권고하는 키 길이는 대략 75에서 90 비트 정도이지만 최근에 개발된 대부분의 암호알고리즘들은 최소 128 비트의 키 길이를 지원하고 있다[7].

Ⅲ. 네트워크 환경에 적합한 VCR 암호알고리즘

네트워크를 통한 사용자수의 급격한 증가와 TCP/IP 프로토콜의 계속적인 사용, 다양한 통신망 서비스의 증가, 전자상거래 활성화 등은 네트워크 환경의 발전과 더불어 가능해졌다. 또한 네트워크 환경의 발달과 더불어 멀티미디어 통신에 대한 요구사항이 증가되는 추세이다. 이와 같은 상황에서 대용량 데이터, 실시간 처리를 요구하는 멀티미디어 통신과 TCP/IP 프로토콜, 사용자 수의 급증에 적용 가능한 암호알고리즘이 필요하게 되었다. 이러한 요구조건을 만족하기 위하여 제시된 AES인 Rijndael 암호알고리즘은 처리속도 및 구현상의 어려움으로 인하여 아직까지 활성화되지 못한 상황이다. 그러므로 본 논문에서는 Rijndael 암호알고리즘을 대체할 수 있으며 기타 AES 암호알고리즘 후보들에 비하여 우수

한 성능을 발휘하고 키 관리 및 유지에 덜 민감하도록 가변 라운딩 기능을 가짐으로서 네트워크 환경에 적합한 VCR 암호알고리즘을 제안하였다.

네트워크 환경에서 대칭형 암호알고리즘의 가장 큰 문제점은 사용자 증가로 인한 키 관리 및 분배가 용이하지 못하다는 것이다. 이러한 문제를 해결하기 위하여 다양한 방법이 강구되고 있으며 일반적인 방법으로 사용되는 블록크기 증대 방식을 이용하여 보다 안전한 채널을 확보하려 하지만 무한정 블록크기를 증대시키는 방법은 매우 비효율적이다. 그러므로 본 논문에서 제안한 VCR 암호알고리즘은 대칭형 기반 암호알고리즘이면서 가변 라운딩기능을 포함하는 기능을 삽입함으로서 이러한 문제점을 해결한다.

VCR 암호알고리즘은 표 1과 같이 32 비트가 하나의 블록크기가 되며 이를 기준으로 블록의 수(Nb)가 2, 4, 6, 8, 10일 때 라운드의 수(N_r)는 10, 11, 12, 13, 14회로 된다.

표 1. 블록 길이에 따른 라운드 수
Table 1. Round numbers of block length

	Nb=2 (64bits)	Nb=4 (128bits)	Nb=6 (192bits)	Nb=8 (256bits)	Nb=10 (320bits)
N_r	10	11	12	13	14

기존 암호방식들 중에도 가변 라운딩 기법을 사용하는 방식이 많이 있다. 그러나 VCR 암호알고리즘은 기존 방식과 다르게 평문에 대한 특성을 이용하여 라운딩을 결정짓는 방식을 사용하기 때문에 기존방식과는 판이하다.

VCR 라운드 횟수를 결정짓는 매개변수는 입력되어지는 기지 평문만을 이용한다. 기존 암호알고리즘의 경우 라운드 횟수를 결정짓는 매개변수는 평문과 키 정보였다. 그러나 이러한 정보들은 선택 암호문 공격법을 사용하면 오히려 해킹 및 크래킹의 근거자료로 활용됨으로서 비도를 저하시키는 요인이 되었다. 또한 평문과 키에 대한 confusion을 수행해야 하는 번거로움이 있기 때문에 VCR는 단순히 평문만을 이용하여 라운드를 결정짓는 구조로 구성하였다.

라운드를 사용하는 기존 암호알고리즘들은 고정된 하나의 라운드와 제어블록을 사용하거나 여러 개의 라운드를 사용하였다. 이때 여러 개의 라운드를 사용하는 경우라도 특정 라운드에 대하여 등비급수 형태로 제공되었다. 그러므로 선택된 평문 또는 암호문을 이용하여 크랙하는 방법인 Known-cipher/plaintext 공격법을 사용하면 쉽게 크랙이 가능하였다. 그러나 VCR 암호알고리즘의 경우 라운드 횟수가 64 비트 등비증가에 대하여 1씩 만큼 차이가 나므로 선택된 평문 또는 암호문이라 하더라도 그 차이가 매우 근소하게 나타난다. 이러한 이유로 인하여 LC 및 DC 특성을 찾아내기 어려워지므로 Known-cipher/plaintext 공격법을 이용한 크랙 등의 암호해석이 어려워진다[2][6].

표 1과 같이 정해진 라운드 횟수에 대하여 VCR는 가변적으로 라운드를 결정하기 위하여 식 (1)과 같은 데이터 매칭 여부를 탐색하게 된다.

```
if P_x = 64  then 10                    ..... (1)
else if = 128  then 11
else if = 192  then 12
else if = 256  then 13
else if = 320  then 14
else if others  then null
end if
```

식 (1) 구조는 외부로부터 입력되는 데이터들이 프레임 형태로 유입되지만 영상이나 음성과 같은 멀티미디어 데이터인 경우, 가변 프레임 형태가 많기 때문에 오히려 고정된 라운드 횟수보다 이와 같은 가변적인 라운드 횟수가 암호해석을 더욱 난해하게 한다. 특히, 식 (1)의 마지막 부분과 같이 입력 데이터들이 64, 128, 192, 256, 320 비트들 중 어느 하나가 아닐 경우 VCR는 아무런 동작을 수행하지 않는 null 동작을 수행하게 된다. 그러므로 프레임이 깨지거나 일부 데이터의 손실이 발생하게 되면 null 동작을 수행하게 되어 일부 손상된 데이터에 대한 암호화를 수행하지 않게 된다. 이러한 기능은 외부로부터의 공격법 중 하나인 PA 공격법에 매우 유용하다.

VCR 암호알고리즘은 암호화 및 복호화를 동시 수행 가능하며 암호화를 수행하기 위하여 암호 연산부를 크게 3 블록으로 구별하여 구성하였다.

암호 연산부로 데이터가 유입되기 전 입력데이터는 RD(Round Decimation) 변환을 수행하게 된다. RD 변환은 RD-I, RD-II로 구별되며 그림 1과 같이 구성된다.

그림 1에서 Updating 정보는 seed 값으로 취급하며 Cipher key는 대칭형 암호알고리즘에서 사용되는 비밀키를 나타낸다.

Updating 정보와 비밀키 정보는 RD-I에서 8 비트를 기준으로 64 비트씩 256 비트 데이터들이 단순 bitwise-XOR 연산을 수행한다. 이 변환은 식 (2)와 같으며 수행 결과값들 중 일부는 RD-II로, 일부는 키 스케줄러의 입력으로 사용된다. RD-I 변환은 비선형 S-box를 이용하는 기존 블록암호알

고리즘과는 별개로 선형성을 강조하기 위하여 식 (2)와 같이 modulo 연산을 수행하도록 하였다.

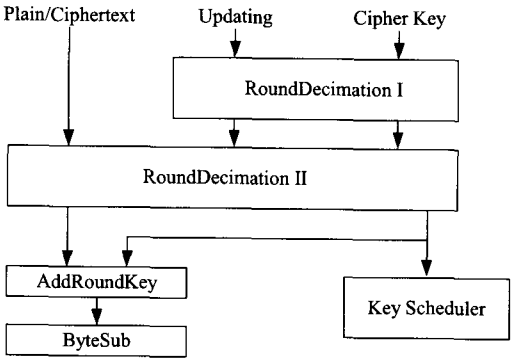

그림 1. RD-I, RD-II 구성
Fig. 1. RD-I, RD-II structure

식 (2)는 선형성을 가지므로 역(inverse) 변환이 가능하다.

$$RD-I = Up_8(256) \oplus K_8(256) \quad \cdots\cdots (2)$$

이때 선형성을 강조하여 선형동작만을 수행하도록 하면 외부로부터의 공격에 쉽게 노출될 수 있으므로 식 (3)과 같은 아핀(affine) 변환을 $GF(2^8)$상에서 수행하도록 한다.

$$b_i = b_{(i+o)\bmod 8} \oplus b_{(i+e)\bmod 8} \oplus c_i \quad \cdots\cdots (3)$$
$$b_j = b_{(j+o)\bmod 8} \oplus b_{(j+e)\bmod 8} \oplus c_i$$

i와 j의 변화 범위가 $0 \leq i, j \leq 7$ 일 때, b_i, b_j는 최소 바이트의 i번째와 j번째 비트이고, o는 홀수번째, e는 짝수번째 비트들이다. c_i는 Updating 초기 정보값이며 $\{d9\}$인 $\{11011001\}$ 값을 갖는 c바이트의 i번째 비트이다. 이러한 변환을 행렬 형태로 나타내면 식 (4)와 같이 표현된다.

$$\begin{bmatrix} b_{7o} \\ b_{6o} \\ b_{5o} \\ b_{4o} \\ b_{3o} \\ b_{2o} \\ b_{1o} \\ b_{0o} \end{bmatrix} = \begin{bmatrix} 10000000 \\ 01000000 \\ 00100000 \\ 00010000 \\ 00001000 \\ 00000100 \\ 00000010 \\ 00000001 \end{bmatrix} \begin{bmatrix} b_7 \\ b_6 \\ b_5 \\ b_4 \\ b_3 \\ b_2 \\ b_1 \\ b_0 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} \quad \cdots\cdots (4a)$$

$$\begin{bmatrix} b_{7e} \\ b_{6e} \\ b_{5e} \\ b_{4e} \\ b_{3e} \\ b_{2e} \\ b_{1e} \\ b_{0e} \end{bmatrix} = \begin{bmatrix} 00000001 \\ 00000010 \\ 00000100 \\ 00001000 \\ 00010000 \\ 00100000 \\ 01000000 \\ 10000000 \end{bmatrix} \begin{bmatrix} b_7 \\ b_6 \\ b_5 \\ b_4 \\ b_3 \\ b_2 \\ b_1 \\ b_0 \end{bmatrix} \oplus \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} \quad \cdots\cdots (4b)$$

RD-II 변환은 평문 또는 암호문과 RD-I의 결과값을 bitwise-XOR 연산을 수행한 후 substitution 블록으로 출력한다. 출력된 값은 64 비트씩 입력을 받아 64 비트씩 1:1 비율로 치환을 수행하게 된다. 이때 기준 표를 기준으로 각각 1 byte 씩 왼쪽 이동을 수행한 후 나머지 치환을 수행하게 된다.

$$\begin{aligned} R_{sub0} &= sub_0 \ \& \ rd_0 \\ R_{sub1} &= 8 \lll R_{sub_0} \ \& \ rd_1 \\ R_{sub2} &= 8 \lll R_{sub_1} \ \& \ rd_2 \\ R_{sub3} &= 8 \lll R_{sub_2} \ \& \ rd_3 \end{aligned} \quad \cdots\cdots (5)$$

식 (5)는 RD-II 변환식이다. R_{sub0}는 첫 번째 substitution 블록이고, $sub0$는 기준표이며 rd_0는 R_{sub0}의 redundancy를 나타낸다.

이때 치환된 데이터들 중 64 비트씩 4 블록의 redundancy 값 $16 \times 4 = 64$ 비트에 대한 weight를 구한다. 구해진 값은 VCR 암호알고리즘의 라운드를 결정짓는 라운드 횟수를 정하게 된다.

$$Rd_0 = 1 \Big|_{rd_i > 32767} \quad \cdots\cdots (6)$$

식 (6)에서 i는 16 비트를 가지는 바이트 블록이며 $0 \leq i \leq 3$을 가진다. Rd는 식 (6)과 같은 조건을 만족할 때 1의 값을 가지며 식 (7)과 같이 Nr이라는 라운드 횟수를 결정짓는 매개체로 사용된다.

$$Nr = 10+n \Big|_{Rd_n = 1 \quad (0 \leq n \leq 3)}$$
$$Nr = 14 \Big|_{Rd = 1} \qquad Nr = 0 \Big|_{Rd = 0} \quad \cdots\cdots (7)$$

식 (7)과 같이 Nr을 결정하는 것은 Rd이며 Rd는 식 (5)에 의하여 산출되는 값이다. 이때 우선순위는 $Rd_0 < Rd_1 < Rd_2 < Rd_3$이다.

출력값인 R_{sub}는 VCR-AddRound 변환을 수행하기 위한 VCR-AddRound 변환부로 입력된다.

RD 변환을 거치면 암호 연산부에서 실제적인 암호화 과정을 수행하게 된다. 암호 연산부는 암/복호화가 동시 수행이 가능하다.

암호 연산부는 VCR-AddRound 변환, VCR-ByteSub 변환, VCR-DiaMat 변환으로 구성된다.

1. VCR-AddRound 변환

VCR-AddRound 변환은 RD로부터 산출된 데이터 R_{sub}와 식 (8)과 같이 산출된 K_{seed}를 식 (9)와 bitwise-XOR 연산을 수행하여 라운드에 대한 정보를 암호화 과정에 합하는 변환을 수행하게 된다. 이때 연산은 바이트가 기본이 된다.

식 (8)에서 $rw(RD-I)$는 식 (2)의 RD-I 변환 결과값에 대하여 redundancy를 구하고 RD-I redundancy에 대한 weight를 구한 값이다.

$$K_{seed} = Nr_{Rd_i\ condition} \otimes rw(RD-I) \quad \cdots\cdots (8)$$

$$= \begin{bmatrix} none \\ Rd_0 \\ Rd_1 \\ Rd_2 \\ Rd_3 \end{bmatrix} \otimes [Up_8(256) \oplus K_8(256)]$$

$$T_{AR} = R_{sub_i} \oplus K_{seed} \quad \cdots\cdots (9)$$

식 (9)에서 T_{AR}은 VCR-AddRound 변환을 의미하며 T_{AR}은 R_{sub_i}와 K_{seed}를 이진합을 이용하여 구하게 된다.

2. VCR-ByteSub 변환

VCR-ByteSub 변환은 바이트 단위로 substitution을 수행하는 기능블록을 의미한다.

VCR-ByteSub 변환은 표 2 w와 같은 기본 치환표를 식 (10)의 변환을 이용하여 w, x, y, z의 VCR-ByteSub 치환 변환표를 형성한다.

$$\begin{aligned} w &\Leftarrow w \\ x &\Leftarrow w \mid x-axis \\ y &\Leftarrow w \mid y-axis \\ z &\Leftarrow w \mid y=x \end{aligned} \quad \cdots\cdots (10)$$

표 2. VCR-ByteSub 기본 치환 모듈
Table 2. Basic VCR-ByteSub substitution module

w	0	1	2	3	4	5	6	7
0	07	2c	23	10	27	17	08	16
1	26	06	1c	01	38	1d	31	1e
2	0f	0e	30	11	2e	3b	02	2b
3	25	37	22	00	3f	24	39	20
4	1b	0d	36	32	12	3c	09	15
5	2a	3d	19	28	3a	33	03	34
6	35	05	3e	2d	04	18	14	21

3. VCR-DiaMat 변환

VCR-DiaMat 변환은 Diagonal Matrix로서 행과 열을 동시에 이동시키며 연산을 수행하는 변환으로서 암/복호화가 동시에 가능할 수 있도록 하는 연산부이다.

VCR-DiaMat 변환은 기본 바이트들의 첫째 행을 제외한 나머지 행들을 각각 서로 다른 offset으로 byte unit cyclic rotation을 통해 위치를 교환하는 변환이다. 즉, 기본 바이트들의 첫째 행 Row0, 열 Column0는 C0 byte 만큼 rotation 시킨다. 실제로는 rotation이 수행되지 않는다. 두 번째 행 Row1, 열 Column1은 C1 byte 만큼 rotation 시키고, Row2, 열 Column2는 C2만큼, Row3, 열 Column3은 C3만큼 rotation 시킨다.

VCR-DiaMat 변환은 전체 바이트들의 row, column들을 $GF(2^8)$상에서의 다항식들 $a(x)$, $b(x)$로 정의하고, rotation 결정횟수인 rotation offset들을 고정된 다항식 $c(x)$로 정의하면 식 (11)과 같은 연산이 가능하다.

$$a(x) \otimes c_r(x) = \mathrm{mod}\, x^4 + 1 \quad \cdots\cdots (11)$$

$$b(x) \otimes c_c(x) = \mathrm{mod}\, x^4 + 1$$

이때 $c(x)$는 식 (12)와 같다. 그러므로 변환전 값인 m은 변환후 값 $m'(x) = c(x) \otimes m(x)$로 식 (13)과 같은 행렬식으로 나타낼 수 있다.

$$c_r(x) = \{03\}x^3 + \{02\}x^2 + \{01\}x + \{01\} \quad \cdots (12)$$

$$c_c(x) = \{30\}x^3 + \{20\}x^2 + \{10\}x + \{10\}$$

$$\begin{bmatrix} m'_{0,c} \\ m'_{1,c} \\ m'_{2,c} \\ m'_{3,c} \\ m'_{c,0} \\ m'_{c,1} \\ m'_{c,2} \\ m'_{c,3} \end{bmatrix} = \begin{bmatrix} 02\,03\,01\,01 \\ 01\,02\,03\,01 \\ 01\,01\,02\,03 \\ 03\,01\,01\,02 \\ - - - - \\ 02\,01\,01\,03 \\ 03\,02\,01\,01 \\ 01\,03\,02\,01 \\ 01\,01\,03\,02 \end{bmatrix} \begin{bmatrix} m_{0,c} \\ m_{1,c} \\ m_{2,c} \\ m_{3,c} \\ m_{c,0} \\ m_{c,1} \\ m_{c,2} \\ m_{c,3} \end{bmatrix} \quad \cdots\cdots (13)$$

식 (13)의 결과를 바이트 단위로 정리하면 식 (14)와 같이 표현된다.

이상 3가지 암호변환은 VCR 암호알고리즘의 암/복호화를 동시에 수행 가능하도록 함으로서 암/복호화 시간이 절약되며 시스템 IP화가 가능하여 다른 플랫폼에 암호시스템을 적용할 경우 시스템의 성능을 향상시킬 수 있는 조건이 된다.

$$\begin{aligned} m'_{0,c} &= (\{02\} \cdot m_{0,c}) \oplus (\{03\} \cdot m_{1,c}) \oplus m_{2,c} \oplus m_{3,c} \\ m'_{1,c} &= m_{0,c} \oplus (\{02\} \cdot m_{1,c}) \oplus (\{03\} \cdot m_{2,c}) \oplus m_{3,c} \\ m'_{2,c} &= m_{0,c} \oplus m_{1,c} \oplus (\{02\} \cdot m_{2,c}) \oplus (\{03\} \cdot m_{3,c}) \\ m'_{3,c} &= (\{03\} \cdot m_{0,c}) \oplus m_{1,c} \oplus m_{2,c} \oplus (\{02\} \cdot m_{3,c}) \end{aligned} \quad \cdots\cdots (14)$$

$$\begin{aligned} m'_{c,0} &= (\{02\} \cdot m_{c,0}) \oplus m_{c,1} \oplus m_{c,2} \oplus (\{03\} \cdot m_{c,3}) \\ m'_{c,1} &= (\{03\} \cdot m_{c,0}) \oplus (\{02\} \cdot m_{c,1}) \oplus m_{c,2} \oplus m_{c,3} \\ m'_{c,2} &= m_{c,0} \oplus (\{03\} \cdot m_{c,1}) \oplus (\{02\} \cdot m_{c,2}) \oplus m_{c,3} \\ m'_{c,3} &= m_{c,0} \oplus m_{c,1} \oplus (\{03\} \cdot m_{c,2}) \oplus (\{02\} \cdot m_{c,3}) \end{aligned}$$

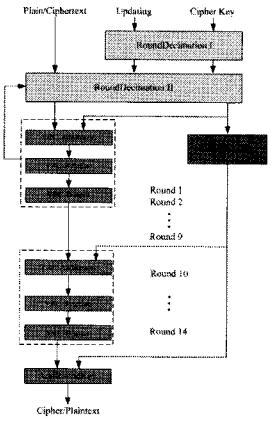

그림 2. VCR 암호알고리즘
Fig. 2. VCR Cryptographic algorithm

이상과 같이 VCR 암호알고리즘의 구성은 기존 대칭형 기반 블록 암호알고리즘과는 확연한 차이를 가진다. 이러한 특징을 가진 VCR 암호알고리즘의 전체 블록도는 그림 2와 같다.

그림 2에서 VCR 암호알고리즘은 입력 기지 데이터와 Updating 정보, 비밀키 정보를 RD-I, RD-II에서 전처리를 수행하고 VCR-AddRound, VCR-ByteSub, VCR-DiaMat 블록에서 암호화를 수행한다.

이때 전처리 연산은 알고리즘이 수행할 라운드 정보를 만들어내며 암호 연산부는 라운드 정보에 의하여 9회까지는 기본적인 라운드를 수행하고 10회에서 14회 까지 설정된 라운드 횟수에 의하여 다양한 라운드 연산을 수행한다.

IV. VCR 암호시스템 설계 및 분석

VCR 암호시스템은 전처리부, 후처리부, Linearity 프로세서로 구성된다. 전/후처리부에서 데이터들에 대한 크기는 32 비트로 한정되어 입력되거나 출력된다. 전/후처리부, Linearity 프로세서, 키 생성부 등의 블록들을 제어해 주는 블록이 그림 3이다. 그림 3의 제어블록은 VCR 암호알고리즘과 별개로 암호시스템 구현시 요구되는 제어신호를 발생하는 블록이다. 32 비트들을 64 비트, 128 비트, 192 비트, 256 비트, 320 비트들을 구별시켜주며 암호 연산부와 전후처리부와의 데이터 패스를 결정지으며 암호 연산부 내부의 블록들간의 interfacing을 주로 관할하게 된다.

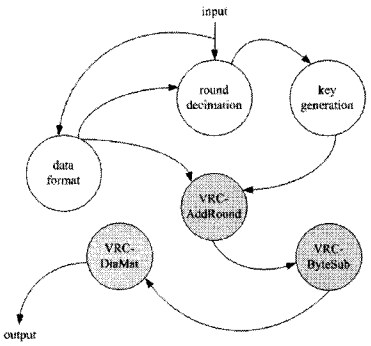

그림 3. VCR 제어블록
Fig. 3. VCR control block mechanism

VCR 암호알고리즘은 대칭형 블록암호알고리즘으로서 기존 AES의 Rijndael, Twofish 암호알고리즘 등이 수행할 수 없었던 기능을 수행함으로서 네트워크 환경에 보다 잘 적응하며 구현하기 용이하게 만든 알고리즘이다.

표 3은 기존 암호알고리즘들과 제안된 VCR 암호알고리즘

을 상호 비교 분석한 표이다[4][9].

VCR 암호알고리즘은 기존 암호알고리즘들과 비교했을 경우 기존 암호알고리즘들의 장점만을 가지므로 많은 차이를 나타낸다. 그러므로 안전성 문제에 대하여 많은 장점을 가지게 된다.

표 3. 기존 암호알고리즘과 VCR 암호알고리즘 비교
Table 3. Comparison of existed and VCR cryptographic algorithms

매개변수	기존 암호알고리즘		제안된 VCR 암호알고리즘
	구조적 기반형	수학적 기반형	구조적 기반형
종 류	DES, Triple-DES, Rijndael, SEED, Twofish, etc	RSA, ECC, ElGamal	VCR 암호알고리즘
원리	구조적 (*Feistel,SPN*)	수학적(소인수문제, 이산대수문제등)	구조적 (*SPN,sharing*)
N_r	고정	사용치 않음	가변
연산자	XOR, Addition, Non-linearity, Mod-2	Mod-n, *Multiplier*, Exponential	XOR, XNOR, Mod-2, Linearity, Addition
키 특성	암호키=복호키	암호키≠복호키	암호키=복호키
키 생성	별도 키 생성	별도 키 생성	별도 키 생성
인 증	어려움	용이함	용이함
속 도	빠름	매우 느림	빠름
키관리자	dealer	dealer, joiner	dealer, joiner
키관리수	많음	적음	적음

표 4. VCR 암호시스템 성능 분석표
Table 4. Performance analysis of VCR cryptosystem

50@㎒	VCR	Rijndael	xDES(3)	RSA
gate count	55K(54,756)	30K(30,213)	20K(19,914)	186K
iteration	10-14 (variable)	14	30	
round	1	1	4	
In/Out length	64/128/192 /256/320 bits(variable)	64/128 /192/256 bits(fixed)	64/128	128
Authentication	x			x
Throughput	356Mbps	402Mbps	256Mbps	94Kbps

표 4는 본 논문에서 제안한 VCR 암호에 대한 성능분석표이다[3][8][9][10]. VCR 암호시스템의 처리율은 구조적 기반형 암호시스템인 Rijndael에 비하여 0.89배, xDES에 비하여 1.39배의 처리율을 보이고 있으며 수학적 기반형 암호시스템인 RSA에 비하여 3,787배 빠름을 확인하였다. 또한 VCR 암호프로세서 구현에 소요되는 게이트 수가 55k로서 구조적 기반형인 Rijndael에 비하여 1.8배 증가, xDES에 비하여 2.75배 증가, 수학적 기반형에 비하여 0.29배 증가하였다.

그림 4에서 x축 상에 가깝게 근접해야 시스템 효율이 좋으므로 xDES가 다른 암호시스템에 비하여 우수함을 알 수 있다.

그러나 xDES는 네트워크 환경에서 키 관리 및 분배 문제 등과 더불어 크랙 및 해킹의 위험성이 매우 높다. 또한 x축으로부터 멀어질수록 속도가 좋다. 이런 면에서 Rijndael 암호알고리즘이 우수하다 할 수 있으나 Rijndael 암호알고리즘은 암호화와 복호화가 다른 구조로 인하여 시스템의 효율성이 매우 낮다.

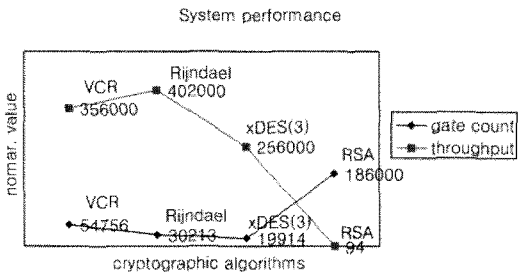

그림 4. VCR, Rijndael, xDES(3), RSA에 대한 성능 비교
Fig. 4. Comparison of VCR, Rijndael, xDES(3) and RSA

그러므로 xDES, Rijndael, RSA는 전체적인 시스템 효율 및 처리율이 낮아서 대용량, 실시간 처리, 고속 전송에 문제가 있으므로 미래 정보사회에서의 활용도는 미지수이다.

V. 결 론

기존 암호알고리즘은 고정된 결정론적 라운드를 수행한다. 그러므로 시스템 복잡도와 신호병목현상을 증가시키고 처리시간의 지연을 가져온다.

그러므로 본 논문에서는 TCP/IP 보안문제, 비도유지, 실시간 처리, 암/복호화 등문제점들을 해결하기 위하여 새로운 구조적 대칭형 블록암호알고리즘 기반 VCR 암호알고리즘을 제안하였으며, 하드웨어 기반 칩 레벨로 구현하기 위하여, 사용된 툴은 Synopsys v1999.10, Synplify v7.7.1, ALTERA QUARTUS II v7.1, ModelSim v6.0이며 테스트보드에 사용한 디바이스는 Cyclone EP1C6Q240C8이다.

모의실험 결과, VCR 암호시스템은 기존 암호시스템들에 비하여 전체적인 성능이 높음을 확인할 수 있었으며 비도유지와 IP 구성블록의 잇점으로 인하여 휴대용 및 다양한 플랫폼에 적합하리라 생각한다.

참고문헌

[1] B. Schneier, "*Applied Cryptography : Protocols, Algorithms, and Source Code in C*", John Wiley & Sons, Inc., New York, USA, 1994.

[2] L. Brown and J. Seberry, "Key scheduling in DES type Cryptosystems", abstract of AUSCRYPT'90, 1990.

[3] 이선근, 정우열, "대용량 고속화 수행을 위한 변형된 Feistel 구조 설계에 관한 연구," 한국컴퓨터정보학회논문지, 제 10권 제 3호, 183-188쪽, 2005년 7월.

[4] vPro Technology *http://www.intel.com/technology/itj/2008/v12i4/10-paper/5-sec-features.htm.*

[5] L. Brown and J. Seberry, "On the Design of Permutation P in Des Type Cryptosystem", Abstract of AUSCRYPT' 90, 1990.

[6] E. Biham and A. Shamir, "Differential Cryptanalysis of DES-like Cryptosystems", Journal of CRYPTOLOGY Vol. 4 No. 1, 1991.

[7] Third AES candidate conference, "AES3 Proceedings, *http://csrc.nist.gov/encryption/aes/round2/ conf3/papers/", pp. 44-54, April, 2000.*

[8] NIST, "Draft FIPS for the AES", *http://csrc.nist.gov/publications/drafts.html.*

[9] Helion, "Rijndael core", *http://www.heliontech.com/core2.htm.*

[10] 이선근, 정우열, "휴대용 보안시스템에 적합한 MT-Serpent 암호알고리즘 설계에 관한 연구," 한국컴퓨터정보학회논문지, 제 13권 제 6호, 195-201쪽, 2008년 11월.

저 자 소 개

이 선 근

1997: 원광대학교 공학석사.
2003: 원광대학교 공학박사.
2009 - 현재: (주)율시스템즈 연구소장
관심분야: 암호시스템, 암호알고리즘, 프로세서 설계, ASIC 설계, 유전자 알고리즘, 네트워크 보안시스템 SoC 설계