수처리 계측제어설비 노드들 간의 무선 안전 전송을 위한 MS-WP 암호 프로세서에 관한 연구

이선근* · 유철** · 박종덕***

A Study on the MS-WP Cryptographic Processor for Wireless Security Transmission Network among Nodes of Water-Processing Measurement-Control-Equipment

Seon-Keun Lee* · Chool Yu** · Jong-Deok Park***

요 약

광범위한 지역의 센서들로부터 데이터를 획득, 제어, 감시 등을 수행하는 계측제어기는 중앙 제어실과 유기적 관계를 유지한다. 그러므로 계측제어기는 유선망보다 무선망이 효율적이다. 그러나 무선망을 이용하게 되면 외부로부터 안전성에 커다란 문제가 발생된다.

그러므로 본 논문은 계측제어기의 네트워크 효율성을 증대시키기 위하여 계측제어 무선망에 적합한 MS-WP 암호시스템을 제안하였다. 제안된 MS-WP 암호시스템을 칩 레벨로 구현하여 모의실험을 수행한 결과, AES 알고리즘에 비하여 130% 처리율 증가 및 시스템 효율이 2배 증가됨을 확인하였다. 제안된 MS-WP 암호시스템은 보안성을 증대시키며 저전력화가 가능하고 처리속도가 빨라 계측제어기에 적합할 것이라 사료된다.

ABSTRACT

Measurement controller that acquire and control and observe data from scattering sensors is organic with central control room. Therefore, measurement controller is efficient wireless network than wire network. But, serious problem is happened in security from outside if use wireless network.

Therefore, this paper proposed suitable MS-WP cryptographic system to measurement control wireless network to augment network efficiency of measure controller. Result that implement proposed MS-WP cryptographic system by chip level and achieve a simulation, confirmed that 130% processing rate increase and system efficiency are increased double than AES algorithm. Proposed MS-WP cryptographic system augments security and is considered is suitable to measurement controller because that low power is possible and the processing speed is fast.

키워드

Water-processing, RFID/USN, AES, Symmetric, MS-WP, Cryptographic algorithm

I. 서 론

수처리 분야에서 계측제어설비는 수처리 공정의 특수성으로 인하여 일정 규모 이상의 시설물 크기를 가지는 시설산업에 속하며, 각 공정별로 공정관리에 필요한 각종 센서(유량계, 수위계 등) 및 수질감시용 계

* 전북대학교 화학공학부(caiserrisk@googlemail.com)
** 교신저자 : 한국수자원공사 전북지역본부(jy231@kwater.or.kr) *** 한국수자원공사 수도기술처(duck77@kwater.or.kr)
접수일자 : 2011. 03. 13 심사(수정)일자 : 2011. 04. 15 게재확정일자 : 2011. 06. 15

측설비(탁도계, pH계 등)가 정수장내에 산재되어 있는 주요 공정 시설물에 설치되어 운영되는 특성을 가진다. 이러한 이유로 수처리 분야에서도 PLC, DCS등과 같은 산업용 계측제어설비가 도입되기 시작하면서 각 공정 데이터 관리는 중요하게 되었다[1].

각 공정의 계측제어설비를 효율적으로 운용되기 위해서는 중앙제어부문에 모든 데이터가 수집, 분석이 되어야 하므로, 각 계측기기에서 중앙제어실로 제어케이블 등을 기반으로 모든 신호가 집중화되어야 한다. 유선망이 기반인 시스템은 송수신 데이터 안정성은 우수하나, 초기투자비용 및 유지, 보수가 어렵다. 이러한 단점을 없애고자 무선망으로의 전환이 필요하지만, 수처리 부문은 광활한 지역을 대상으로 각 공정별 시설물이 산재되어 운용되기 때문에 외란 등에 의한 데이터 변형 및 해킹등이 문제시되고 있으며, 특히, 생산재인 용수생산, 공급의 특성상 국가주요시설물로써 수처리 공정의 각종 감시,제어 데이터에 대한 관리 및 보안성이 대두되고 있다.

그러므로 본 논문에서는 이러한 무선망의 단점을 없애기 위하여 RFID/USN망에 적용 가능한 암호알고리즘인 MS-WP(modified symmetric cryptographic algorithm for Nodes of Water-Processing Measurement-Control-Equipment) 암호알고리즘을 수처리 계측제어설비에 적용하여 보다 안전하며 시설설비효율이 높도록 하였다.

II. 다중노드/분할 PRN을 갖는 MS-WP 암호알고리즘

분산된 설비 제어를 효율적으로 관리하기 위하여 무선망을 사용하고 안전한 정보를 확보하기 위하여 사용할 수 있는 일반적인 암호알고리즘 매우 드물다.

그러므로 본 논문에서는 처리시간, 크기, 노드수 등을 고려한 구현상의 문제 해결과 노드증가로 인한 보안자원의 효율성 등을 위하여 MS-WP 기법을 제안하였으며 이를 AES인 Rijndael 암호알고리즘에 적용하였다. 제안된 MS-WP 기법은 기존 AES와 유사하게 기본연산자로 배타적 논리합을 사용하며 처리 수행단위는 바이트를 사용하였다. 바이트 연산은 처리속도를 매우 높게 수행할 수 있다는 장점과 더불어 역추적이 어렵기 때문에 비도 증가에도 매우 우수한 특성을 가진다. 또한 기존 Feistel과 SPN 구조를 혼용하기 때문에 암/복호화의 동시 수행이 가능하여 Rijndael[2] 또는 Serpent[3] 암호알고리즘에서 발생되는 효율 저하가 발생하지 않는다. 이러한 특징은 AES에 대한 충분한 전제조건을 만족함과 동시에 AES 다음 버전에 대한 내용을 제시할 수 있다. 이러한 특징으로 인하여 MS-WP 암호알고리즘은 실시간 처리 및 구현상의 문제점, 노드증가로 인한 관리문제 등을 해결할 수 있다.

2.1. MS-WP를 적용한 AES 암호알고리즘

MS-WP를 적용한 AES 암호알고리즘에 사용되는 입/출력/키 블록 크기는 128 비트이며 평문, 암호문 그리고 키의 크기도 1:1:1이 된다. MS-WP AES 암호알고리즘은 AES 암호알고리즘과 마찬가지로 다음과 같은 네 가지 기능블록을 포함하며 각 단계를 거치는 동안 바이트 단위의 변환으로 구성된 라운드를 이용하여 암/복호화를 수행한다.

i) Inv/SubByte : 조건 상태(CS : Condition State) 기능을 가진 S-box를 이용하여 바이트 치환 수행기능
ii) Inv/ShiftDiagonal : CS에 대한 행 방향 이동기능
iii) Inv/MixColumn : CS의 각 열에 해당하는 바이트들의 혼합기능
iv) AddRoundKey : CS와 라운드 키에 대한 1:1 덧셈기능

평문/암호문 128 비트의 입력은 CS 블록으로 초기 저장된다. CS는 MS-WP-AES 암호알고리즘을 형성하기 위한 비선형 특성을 가진 상태를 의미한다. CS는 식 (1) 및 그림 1과 같이 외부에서 주어지는 파라미터를 가지고 현재상태를 결정하며 결정된 현재상태는 불확실한 미래상태를 형성하는 기준값이 된다.

$$CS_{next} \leftarrow CS_{present}(prn_{seed} \bmod 8) \quad (1)$$

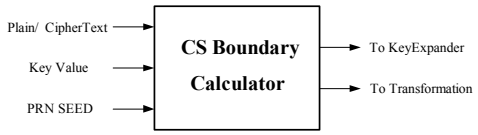

그림 1. 조건 상태(CS) 특성
Fig. 1 Condition State characteristic

CS는 입력으로 사용되는 여러 가지 파라미터를 이용하여 키 값을 생성하는데 필요한 자료를 만드는 동시에 암/복호화하는 과정 중에 치환변환을 제어하는 기능을 수행한다.

식 (1)에서 mod 8은 입력 데이터들에 대한 모듈러 연산을 의미하는 것으로서 입력값들에 대한 포맷을 바이트로 변환하기 위한 과정이다. 또한 PRN[4] SEED는 식 (2)와 같이 입력 데이터와 키 값을 이용하여 생성한다.

$$SEED = INPUT \bigoplus KEY_{7,15,\ldots,111,119,127} \quad (2)$$

식 (2)에 의하여 생성된 SEED는 식 (3)과 같은 PRN을 통하여 2 바이트의 출력값을 산출하게 된다.

$$PRN = PRN_{odd} \| PRN_{even} \quad (3)$$

$$PRN_{odd} = x^{16} + x^{13} + x^{12} + x^{11} + x^{7} + x^{6} + x^{5} + x^{4} + 1$$

$$PRN_{even} = x^{16} + x^{14} + x^{10} + x^{9} + x^{8} + x^{6} + 1$$

산출된 2 바이트 중 odd 정보는 MS-WP-AES의 내부 바이트 치환 제어에 사용되어지며, even 정보는 키 확장 제어에 사용된다.

odd와 even 정보는 예측 불가 함수를 생성하는 기능을 가짐으로서 내부 치환정보가 외부로 유출될 가능성이 적으며, 입력 데이터와 키 정보만을 가지고 생성된 것이기 때문에 별도의 프로세싱이 필요 없다.

식 (3)은 이동통신망에서 사용되는 PRN과 동일한 방정식으로서 2바이트를 하나의 방정식으로 간주하여 출력값을 산출하게 된다.

CS는 초기 라운드 키와 배타적 논리합을 수행한 후 n번의 라운드를 수행하게 된다. 모든 라운드가 실행되면 암/복호화를 마치게 된다. 이러한 MS-WP-AES 암호알고리즘에 대한 전체적인 흐름은 그림 2와 같다. MS-WP-AES 암호알고리즘의 가장 큰 특징은 그림 2에서 보는바와 같이 암/복호화가 동시에 수행된다는 점이다. 제어신호에 의하여 암/복호 모드가 결정되며 처리되어지는 연산은 순/역으로 동작한다.

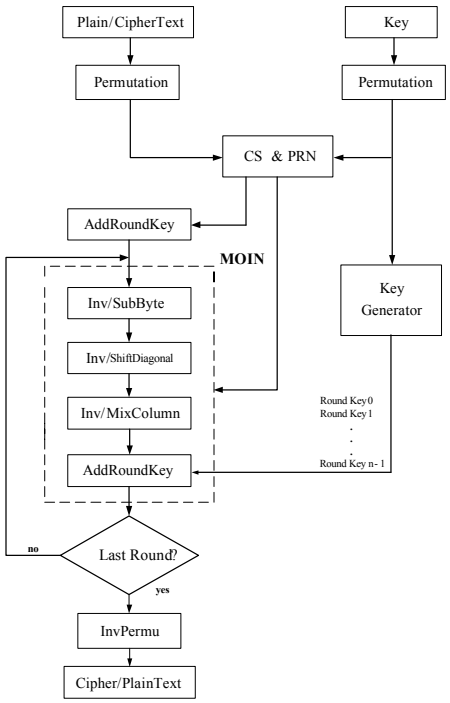

그림 2. MS-WP를 적용한 AES 암호알고리즘
Fig. 2 AES cryptographic algorithm adopted MS-WP

각 라운드마다 Inv/SubByte, Inv/ShiftDiagonal, Inv/MixColumn, Inv/AddRoundKey에 대한 데이터 값들은 CS & PRN에 의하여 별개로 동작하게 된다. 그러므로 라운드 수에 따라서 비도가 결정된다.

기존 AES는 데이터와 키의 길이를 128, 192, 256 비트들로 가변시키며, 변화하는 길이에 따라 최적화된 라운드 수를 결정하게 된다. 그러므로 기존 AES인 경우 데이터의 블록길이에 따라 라운드 수가 결정된다. 이러한 결과로 인하여, 데이터 심볼 크기를 파악하게 될 경우, 라운드 수를 파악할 수 있으며 라운드 수와 키 및 데이터와의 DC 및 LC에 의하여 크래킹이 가능해진다. 그러나 MS-WP AES인 경우 고정된 블록 및 키 크기를 가지고 있어도 내부적으로 라운드 수에 따라 데이터 내용이 변화되므로 라운드 수를 데이터 심볼 크기만을 가지고 파악할 수 없다는 장점이 있다.

이러한 네 가지 변환을 MOIN(Minimum Operation for Inverse/Non-inverse)이라고 정의하면 식 (4)와 같다.

$$MOIN_{n-round} \leq Inv/SubByte(odd)_n + Inv/ShiftDiagonal(odd)_n + Inv/MixColumn(odd)_n + AddRoundKey(odd)_n$$

$$MOIN_{(n-1)-round} \leq Inv/SubByte(even)_{n-1} + Inv/ShiftDiagonal(even)_{n-1} + Inv/MixColumn(even)_{n-1} + AddRoundKey(even)_{n-1} \quad (4)$$

1) Inv/SubByte 변환

Inv/SubByte 변환은 바이트 단위로 구성된 S-box를 이용하여 CS에 의한 외부상태값들을 각각의 레지스터에 저장하고, 저장된 값들은 각각 독립적으로 존재하는 바이트들을 비선형적으로 변형하여 비선형 변형된 바이트 집합을 생성하게 된다. Inv/SubByte 변환에 사용되는 S-box는 역변환(inverse transformation)이 가능하며 유한체 GF(2^8)에서 곱에 대한 역이 존재하며 식 (5)와 같이 정의되는 affine 변환을 GF(2^8)에 적용할 수 있는 비선형 변환이 가능한 함수들의 집합이다.

$$[ab]_i = [ab]_i \bigoplus [ab]_{(i+4)\bmod 8} \bigoplus [ab]_{(i+5)\bmod 8} \bigoplus [ab]_{(i+6)\bmod 8} \bigoplus [ab]_{(i+7)\bmod 8} \bigoplus [ac]_i \quad (5)$$

여기에서 ab는 CS & PRN의 출력 정보 중 내부 정보를 변환시켜 주는 부분인 a 부분의 비트 블록을 의미하며 $0 \leq i \leq 7$일 때 $[ab]_i$는 각각 독립적으로 분리되어 동작하는 바이트들의 i 번째 해당 비트이고 $[ac]_i$는 특정 ac 바이트 블록의 i 번째 비트를 의미한다. mod8은 내부 연산시 바이트 단위로 수행되지만 실제적인 연산은 비트 단위이다. 그러므로 비트와 바이트에 대한 분리 표현을 위하여 모듈러 연산을 유한체 GF(2^8)상에 나타냄으로서 MS-WP-AES 암호알고리즘은 1 바이트 연산이 기준이 된다는 것을 나타낸다. 이 변환을 행렬 형태로 표현하면 식 (6)과 같다. 여기에서 ab'는 변환된 새로운 상태배열을 의미하며 $s_{00} \sim s_{77}$는 S-box에 대한 값이며 PN_0는 랜덤수를, α(alpha)는 PRN에 대한 SEED값을 의미한다.

2) Inv/ShiftDiagonal 변환

Inv/ShiftDiagonal 변환은 데이터 상태배열의 행 및 열 단위를 기준으로 대각선 방향으로 동시에 이루어진다. 이러한 변환은 식 (7)과 같은 방정식으로 표현할 수 있다.

$$\begin{bmatrix} ab'_0 \\ ab'_1 \\ ab'_2 \\ ab'_3 \\ ab'_4 \\ ab'_5 \\ ab'_6 \\ ab'_7 \end{bmatrix} = \begin{bmatrix} s_{00} & s_{01} & \cdots & s_{07} \\ s_{10} & s_{01} & \cdots & s_{17} \\ & & \cdots & \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdots & \cdot \\ & & & \\ s_{60} & s_{61} & \cdots & s_{67} \\ s_{70} & s_{61} & \cdots & s_{77} \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} \times \begin{bmatrix} PN_0 \\ PN_1 \\ PN_2 \\ PN_3 \\ PN_4 \\ PN_5 \\ PN_6 \\ PN_7 \end{bmatrix} + \begin{bmatrix} \alpha_0 \\ \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \alpha_4 \\ \alpha_5 \\ \alpha_6 \\ \alpha_7 \end{bmatrix} \quad (6)$$

$$\begin{aligned} S_a'(03,12,21,30) &= S_a(00,11,22,33) \\ S_b'(13,22,31,00) &= S_b(01,12,23,30) \\ S_c'(23,32,01,10) &= S_c(02,13,20,31) \\ S_d'(33,02,11,20) &= S_d(03,10,21,32) \end{aligned} \quad (7)$$

식 (7)에서 각 상태배열에 대하여 행과 열이 대각을 중심으로 변환됨을 알 수 있다. 이러한 대각변환은 역치환 및 계산 수행이 용이할 뿐만 아니라 랜덤성을 보장하게 된다. 그러므로 Inv/ShiftDiagonal 변환은 Rijndael 또는 Serpent 암호알고리즘과 같은 계산속도의 1/2배의 특성을 가지며 비도는 2배 증가를 가지게 된다.

식 (7)과 같이 대각방향으로 이동되는 Inv/ShiftDiagonal 변환은 행번호가 0인 첫행 첫열은 3번 0번 shift 되며, 마지막 행 및 열은 0번 3번 이동하게 된다. 이와 같은 대각 변환은 같은 행에 있는 바이트들이 행의 번호가 낮은 위치로 이동하는 결과를 가져오며 행 번호가 낮은 위치의 바이트는 상위행의 위치로 이동하게 된다.

Inv/ShiftDiagonal 변환은 대각 변환을 이용하여 변환되기 때문에 역변환도 동일한 과정으로 변환하게 된다.

3) Inv/MixColumn 변환

Inv/MixColumn 변환은 고정된 다항식인 $a(x)$를 곱하여 새로운 변환 배열을 생성한다. 이때 전체 변환식은 곱셈연산이 기본이 된다. 즉 변환된 함수 $s'(x)$는 변환 전 함수인 $s(x)$에 대하여 $a(x)$를 곱한 형태를 가지게된다. 이러한 $s'(x) = a(x) \otimes s(x)$ 곱셈형태는 식 (8)과 같이 표현된다.

식 (8)의 결과값은 상태 배열에서 네 개의 바이트 열들로 식 (9)와 같이 변환된다.

식 (9)에서 동일한 계수값에 대하여 연속적인 계산을 요구하는 항이 존재하게 된다. 이러한 동일 연산은 배타적 논리합을 이용하면 소거되므로 식 (9)를 다시

정리하면 식 (10)과 같이 변형될 수 있다.

$$\begin{bmatrix} s'_0 \\ s'_1 \\ s'_2 \\ s'_3 \end{bmatrix} = \begin{bmatrix} 02 & 01 & 03 & 03 \\ 01 & 03 & 03 & 02 \\ 03 & 03 & 02 & 01 \\ 03 & 02 & 01 & 03 \end{bmatrix} \begin{bmatrix} s_0 \\ s_1 \\ s_2 \\ s_3 \end{bmatrix} \quad (8)$$

$$\begin{aligned} s'_0 &= (\{02\}\cdot s_0)\oplus(\{01\}\cdot s_1)\oplus(\{03\}\cdot s_2)\oplus(\{03\}\cdot s_3) \\ s'_1 &= (\{01\}\cdot s_0)\oplus(\{03\}\cdot s_1)\oplus(\{03\}\cdot s_2)\oplus(\{02\}\cdot s_3) \\ s'_2 &= (\{03\}\cdot s_0)\oplus(\{03\}\cdot s_1)\oplus(\{02\}\cdot s_2)\oplus(\{01\}\cdot s_3) \\ s'_3 &= (\{03\}\cdot s_0)\oplus(\{02\}\cdot s_1)\oplus(\{01\}\cdot s_2)\oplus(\{03\}\cdot s_3) \end{aligned} \quad (9)$$

$$\begin{aligned} s'_0 &= (\{02\}\cdot s_0)\bigoplus(\{01\}\cdot s_1) \\ s'_1 &= (\{01\}\cdot s_0)\bigoplus(\{02\}\cdot s_3) \\ s'_2 &= (\{02\}\cdot s_2)\bigoplus(\{01\}\cdot s_3) \\ s'_3 &= (\{02\}\cdot s_1)\bigoplus(\{01\}\cdot s_2) \end{aligned} \quad (10)$$

식 (10)을 이용하여 Inv/MixColumn 변환을 수행하면 그림 3과 같이 상태배열의 일부만이 변환된다는 것을 알 수 있다. Inv/ShiftDiagonal 변환과 비슷하게 대각변환을 수행하고 있지만, Inv/MixColumn 변환은 $y = x$에 해당하는 대각변환만을 수행하게 된다. 즉, MS-WP-AES 암호알고리즘의 대각변환을 수행함에 있어 식 (11)과 같이 대각변환이 구별되어진다.

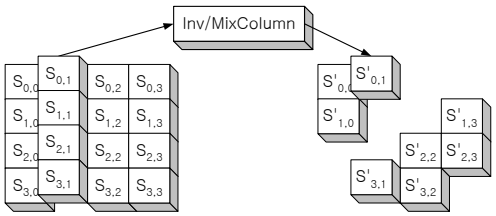

그림 3. Inv/MixColumn 변환
Fig. 3 Inv/MixColumn transformation

식 (11)과 같이 하나의 상태배열에 대하여 대각 변환을 x방향과 $-x$방향으로 수행함으로서 전체 대각을 변환시킬 수 있다. 이러한 대각변환은 기존 암호알고리즘과 같이 곱셈연산을 수행해야하는 번거로움을 줄일 수 있다. 제안된 MS-WP-AES 암호알고리즘은 식 (10)과 같이 다른 값들에 대해서만 곱셈계산을 수행함으로서 수행속도의 단축 및 자리올림 현상이 발생하지 않으며 동시에 반대방향으로 대각변환을 수행함으로서 비도를 향상시킬 수 있다.

$$\begin{aligned} y &= -x; \quad Inv/ShiftDiagonal \\ y &= x; \quad Inv/MixColumn \end{aligned} \quad (11)$$

4) AddRoundKey 변환

AddRoundKey 변환은 라운드 키와 상태 배열(CS)을 더하는 연산을 수행한다. 각 라운드 키는 키 스케쥴로부터 천이상태가 발생될 때마다 별개의 독립된 값을 산출하며, 산출된 값들은 식 (12)와 같은 연산을 수행한다.

$$\begin{aligned} &[s'_0, s'_1, s'_2, s'_3] \\ &= [s_0, s_1, s_2, s_3]\bigoplus[w_{round}\cdot PN_{round}] \end{aligned} \quad (12)$$

여기에서 w_{round}는 라운드 수행에 대한 키 스케쥴 워드이며, PN_{round}는 CS & PRN에 대한 라운드 수행 범위를 의미한다. AddRoundKey 변환은 라운드 범위에 따라서 계산되는 횟수는 다르지만 계산되어지는 양은 동일하게 단순 더하기 기능만을 수행하게 된다.

2.2. MS-WP를 적용한 AES 키 스케쥴링

일반적인 암호알고리즘은 키 생성 알고리즘 및 키 스케줄링 작업을 수행한다. 이러한 키 스케줄링 작업은 보다 복잡한 키를 생성하기 위한 수단으로서 알고리즘의 안전도에 절대적인 역할을 수행한다.

MS-WP AES 암호알고리즘의 경우, 키 스케줄링을 라운드에 따라 변화하는 방법을 사용하지 않고, 단지 CS & PRN 방법을 사용하여 생성한다. 암호문을 생성하고자 하는 평문의 일부를 이용하여 PRN의 SEED로 사용하고 PRN은 각 event가 발생할 때마다 라운드과정으로 인식하여 암호화에 필요한 키를 생성하게 된다. 이러한 키 생성은 각 라운드마다 필요한 별개의 키를 효율적으로 생성할 수 있으며 생성된 키를 이용하여 암호화를 수행할 경우 라운드를 구별하는 기준점을 별도로 설정할 필요성이 없어지게 된다.

키 생성은 PRN의 event 발생 때마다 변화하는 값을 이용하며 내부의 암호문은 MOIN 블록, 즉 네 단

계의 변환을 수행할 때마다 변화하는 동시에 PRN의 값이 변환을 조절하게 된다. 이러한 이유로 다른 암호 알고리즘에서는 키와 암호문과의 크기 조절을 위하여 키 길이의 확장 및 축소과정을 거치게 되지만, MS-WP AES 암호알고리즘은 이러한 키 길이의 조작을 별도로 수행할 필요성이 없다.

III. MS-WP를 적용한 AES 암호시스템 설계 및 모의실험

MS-WP AES 암호알고리즘의 구현은 VHDL을 이용하여 Top-down 방식으로 진행하였으며 회로합성은 Synopsys Design Analyser Ver. 1999.10, QUARTUS 7.0을 사용하였고, 모의실험에 사용된 툴은 Synopsys VHDL Debegger, ModelSim 5.8C를 사용하였다. 구현을 위한 테스트베드는 ALTERA Cyclone EP1C6Q240 C8N 디바이스를 사용하였다.

CS & PRN 처리부는 상태 조건을 바탕으로 조건 상태를 산출하게 되며 산출된 조건 상태 배열들인 CS는 바이트 치환을 수행하게 된다. 식 (1)과 같이 CS에 대한 상태 변화는 PRN과 mod 연산을 통하여 변화하게 된다. 이때 입력으로 사용되는 데이터들은 암호문 또는 평문과 키 값 그리고 PRNG(PRN Generator)[4]의 SEED값이다.

입력 데이터 128 비트에 대하여 키 값 역시 128 비트이며 키 값 128 비트 중 일부 데이터는 입력데이터와 2진곱 연산을 수행한 후 PRNG SEED 값으로 사용된다.

암호/복호모드에 따라서 PRNG의 even, odd가 결정되며 결정된 PRNG는 키 정보를 SEED값으로 받아 랜덤한 키 정보를 출력한다. 이때 출력되어지는 키 정보는 암/복호문의 일부와 전처리 SEED 연산을 수행하게 된다. SEED 포맷과정을 거친 키 정보는 MOIN 블록 내부의 AddRoundKey 블록의 입력으로 사용된다. 이때 MS-WP AES 암호시스템의 round는 10회로 결정되어 있다. 이와같이 MOIN 블록에 대한 키 정보를 입력시켜주며 랜덤한 키 정보를 생성하는 블록이 keyscheduler 블록이다.

MS-WP AES 암호시스템은 입력 128 비트에 대하여 출력 128 비트를 산출하며 암호문 또는 평문에 대하여 평문 또는 암호문을 출력하게 된다.

암/복호화를 수행하는데 있어 필요한 정보인 키 정보는 실제적으로 암/복호화를 수행할 때는 필요 없으며, 단지 새로운 키 정보를 생성하기 위한 기본 자료로 활용될 뿐이다.

표 1은 기존 암호시스템과 제안된 MS-WP AES 암호시스템을 상호 비교 분석한 표이다[5-8].

표 1. MS-WP AES 성능분석표
Table 1. MS-WP AES performance analysis

@50MHz	구 조	라운드수	데이터길이 (bits)	키 길이 (bits)	처리율 (Mbps)
DES	Feistel	16	64	56	31.6
3DES	Feistel	48	64	112/168	15.6
SEED	Feistel	16	128	128	313.7
Serpent	SPN	32	128/192/256	128	197.3
AES	SPN	10	128/192/256	128	387.9
MS-WP	Feistel & SPN	10	128	128	532.0

표 1에서 기존 대칭형 블록 암호시스템에 비하여 MS-WP AES 암호시스템이 처리율면에서 130% 증가됨을 확인하였다. 또한 라운드 횟수와 비도에 의한 암호 효율 측면에서 MS-WP AES 암호시스템은 암호화에 사용되어지는 키 정보가 내부 CS와 PRN에 의하여 생성되며 암/복호화가 동일한 시스템에서 동시에 실행 가능함으로서 기존 블록 암호시스템에 비하여 암/복호측면에서 2배의 효율을 가짐을 알 수 있다. 그러므로 전체적인 시스템 효율은 기존 블록 암호시스템에 비하여 MS-WP AES 암호시스템이 2배의 성능을 가짐을 알 수 있다. 이와 같이 MS-WP-AES 암호알고리즘은 기존 블록 암호알고리즘에 비하여 RFID/USN과 같은 자원제약조건을 가진 환경에서 효율적임을 확인할 수 있었다.

IV. 결 론

효율적인 수처리를 위한 계측제어설비분야에 대한 무선망의 초기 및 유지비용, 해킹 및 크래킹을 방지하기 위한 기법으로 다양한 방식의 암호기법이 사용되고 있지만 무선망 자체 또는 기존 암호알고리즘을 사용하는 이유로 인하여 트랩도어가 존재할 수 있으며, 설비노드의 효율적인 관리가 어렵다는 점에서 계측제

어설비에 대한 효율적 무선망 관리가 쉽지만은 않다.

본 논문은 이러한 수처리 계측제어설비 무선망에 적합한 암호알고리즘인 MS-WP를 적용한 AES 암호 알고리즘을 제안하였다.

제안된 MS-WP 암호시스템은 암호화를 수행하는 자원으로서 자체 정보만을 가진다. 또한 처리시간 및 비도는 동시다발적인 연산으로 인하여 기존 대칭형 암호시스템에 비하여 처리율면에서 130% 증가를 가져왔다. 또한 암/복호화를 하나의 시스템으로 처리 가능하므로 전체적인 시스템 효율면에서 2배의 성능을 가짐을 확인하였다.

본 논문에서 제안한 MS-WP 암호알고리즘은 기존 암호알고리즘에 비하여 높은 전송률 및 시스템 효율을 가지며, 특정 길이의 키 결정을 수행할 필요가 없는 구조적 기반 알고리즘이기 때문에 시스템 복잡도가 매우 낮고 처리시간이 빠르다. 그러므로 제안된 새로운 MS-WP 암호알고리즘은 RFID/USN을 이용하거나 노드수가 불규칙적인 수처리 계측제어설비 등과 같은 환경적 자원제약 조건을 극복하기에 적합한 암호알고리즘으로 사료된다.

참고 문헌

[1] 김창환, “유비쿼터스 환경에서의 정보보호기술”, http://www.eic.re.kr, 11, 2008.

[2] NIST, "AES Algorithm (Rijndael) Information", http://csrc.nist.gov/archive/aes/rijndael

[3] I. Damaj, M. Itani, H. Diab, "Serpent Cryptography on Static and Dynamic Reconfigurable Hardware," aiccsa, IEEE International Conference on Computer Systems and Applications, pp. 680-684, 2006.

[4] NIST, "pseudo-random number generator", http://www.itl.nist.gov/div897/sqg/dads/HTML/pseudorandomNumberGen.html

[5] Microelectronic Systems Laboratory, "Implementation of DES Algorithm Using FPGA Technology", http://www.alagger.com/des-vhdl/report.pdf, 2002.

[6] "DES and 3DES cores", http://www. helion tech.com/des.htm

[7] “SEED 블록암호알고리즘”, http://service2.nis.go. kr/pw_certified/seed.jsp

[8] "A candidate block cipher for the advanced encryption standard", http://www.cl.cam.ac.uk/~rja14/serpent.html

저자 소개

이선근(Seon-Keun Lee)

1997년 8월 : 원광대학교 전자공학과 (공학석사)

2003년 2월 : 원광대학교 전자공학과 (공학박사)

2011년 4월 ~ 현재 : 전북대학교 화학공학부 겸임교수

※ 관심분야 : 프로세서 설계, 암호알고리즘, 보안시스템설계

유 철(Chool Ryu)

1995년 2월 : 원광대학교 전자공학과 (공학학사)

1995년 10월 ~ 현재 : 한국수자원공사 전북지역본부 근무

2005년 9월 : 광역상수도 수도통합운영시스템 설계, 구축

※ 관심분야 : 수처리공정자동화, 수요예측 알고리즘, 산업보안시스템설계

박종덕(Jong-Duk Park)

1994년 2월 : 조선대학교 전자공학과 (공학석사)

2011년 8월 : 전북대학교 제어계측공학 (공학석사)

1994년 4월 ~ 현재 : 한국수자원공사 근무

※ 관심분야 : 제어 자동화, 데이타베이스 설계, Fuzzy Logic