Journal of the Korea Academia-Industrial cooperation Society
Vol. 12, No. 6 pp. 2713-2717, 2011

DOI : 10.5762/KAIS.2011.12.6.2713

# Binary CDMA 시스템에 적용 가능한 PBS-AES 코릴레이터 설계에 관한 연구

이선근[1*]
[1]전북대학교 화학공학부

# A Study on PBS-AES Correlator Design adapted in Binary CDMA System

**Seon-Keun Lee**[1*]
[1]**Faculty of Materials & Chemical Engineering, Chonbuk National University**

**요 약** 수처리 기간산업 등의 산재된 센서들로부터 데이터를 전송하기 위해서 사용되는 Binary-CDMA 시스템은 자체적으로 안전성을 내포하고 있다. 그러나 급변하는 다양한 방식의 해킹 및 크래킹에 대한 방어기재로서 Binary-CDMA는 환경변화에 매우 민감하게 반응할 필요성이 대두되고 있다.
그러므로 본 논문은 이러한 문제점을 해결하기 위하여 Binary-CDMA에서 병목현상이 발생되는 코릴레이터에 안전성 확보 및 쉬운 업데이트를 위하여 보안 암호알고리즘을 추가하였다. 추가된 암호알고리즘은 대칭형 기반 암호알고리즘으로 센서들에 대한 1:1 대응을 수행함으로서 안전하지 않은 채널에서 안전한 정보를 통신할 수 있도록 한다.

**Abstract** To transmit data from straggling sensors in water-processing basic industries etc., used Binary-CDMA system has safety voluntarily. But Binary-CDMA is necessity that react very sensitively in environment change as defense about hacking and cracking of various way that change suddenly.
Therefore, this paper is that see added cryptographic algorithm for safety and easy update on correlator that a bottle-neck phenomenon is happened in Binary-CDMA to solve problem that is such. Added cryptographic algorithm does to communicate safe information in channel that is not safe as that achieve 1:1 confrontation for sensors by symmetric cryptographic algorithm.

**Key Words :** Binary-CDMA, Correlator, Cryptographic, Symmetric, Security-channel

## 1. 서론

최근 다양한 통신망 시장의 급속한 발전으로 인하여 통신시장은 다수의 사용자들에게 다양한 무선 멀티미디어 통신 서비스 증가를 부추기고 있다. 또한 RFID/USN의 증가로 인해 다양한 센서들로부터 전송 및 데이터 처리 속도가 저하되고 있는 상황에서 사용자들은 고속의 데이터를 처리할 수 있는 시스템을 요구하고 있다.[1]

기존 고속 데이터 전송에 적합한 Multi- Code CDMA 시스템의 단점인 하드웨어의 복잡성을 보완하고자 기존 CDMA 기술에 기반을 둔 Binary CDMA 기술이 제안되었다. 그러나 Binary CDMA 시스템에서 고속 데이터 연산 시 병목현상이 발생되는 코릴레이터는 고속 연산이 필요한 동기 획득과정에 매우 중요한 시스템 파라미터이다. 기존의 코릴레이터는 전력소모가 작다는 장점이 있지만 코릴레이션의 값을 얻기 위해 여러 단의 가산연산을 거쳐야 하므로 연산량 및 delay가 증대되어 처리 속도가 낮은 단점을 가지고 있다. 또한 이러한 처리시간의 증대는 다양한 센서로부터 데이터를 안전하게 전송할 경우, 외부로부터 쉽게 공격당하기 쉽다.[2,5,6]

그러므로 본 논문에서는 Binary CDMA 시스템에서 병목현상을 감소함과 동시에 대칭형 암호 알고리즘을 추가

*교신저자 : 이선근(caiserrisk@googlemail.com)
접수일 11년 04월 26일 수정일 11년 06월 06일 게재확정일 11년 06월 09일

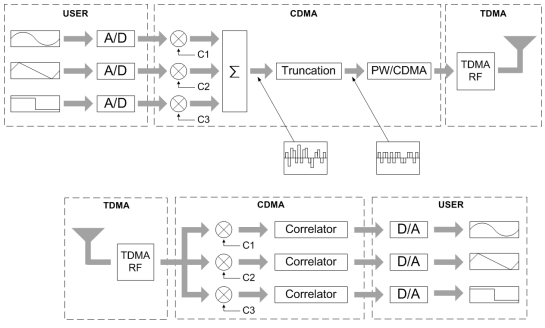
함으로서 고속의 데이터를 처리함과 동시에 데이터의 안전성을 확보할 수 있는 Binary CDMA용 보안 코릴레이터를 제안하였다.

## 2. Binary CDMA

Binary CDMA 기술은 기존 CDMA 기술의 장점인 우수한 보안성 및 통신용량을 증대시킬 수 있고, 주파수 재사용으로 인해 효율적이며 다중경로 페이딩에 강한 장점들을 그대로 가지고 있다. 또한 사용자가 증가할수록 송신 신호는 다중 레벨이 되는 문제로 인한 PAPR(Peak to Average Power Ratio)이 커지기 때문에 송신단에서 선형성이 매우 우수한 증폭기가 필요하기 때문에 비용이 증가하게 되는 단점을 가진다.[3]

그러므로 Binary CDMA는 다양한 레벨의 변조신호를 이진화하여 TDMA 신호 파형으로 만들어 전송하므로 TDMA용 RF 모듈을 이용하여 구조의 복잡성, 높은 가격, 높은 전력소모 등의 현존하는 문제를 해결할 수 있으며 근거리 무선통신 기술로 WPAN(Wireless Personal Area Network) 및 WLAN에 사용이 가능하다. 그림 1은 이와 같은 TDMA 특성을 가지는 Binary CDMA의 시스템 구성도이다.

그림 1에서 Binary CDMA는 입력 신호를 동시에 전송하기 위해 각각의 입력 신호에 서로 다른 직교 코드를 곱하여 채널간의 직교성을 보장한 후, 각 채널 신호를 모두 합하여 동시에 전송하게 된다. 이때 여러 채널을 동시에 더해서 전송하게 되면 각각의 채널 신호가 바이너리(binary) 파형일지라도 합해진 전체 신호는 멀티 레벨(Multi-Level) 신호로 바뀌게 된다.




[그림 1] Binary CDMA의 시스템 구성도
[Fig. 1] System architecture of Binary CDMA

Binary CDMA 방식은 PW/CDMA(Pulse Width/Code Division Multiple Access), MP/ CDMA(Multi-Phase/Code Division Multiple Access), CS/CDMA(Code Select/Code Division Multiple Access)로 나누어진다.[4]

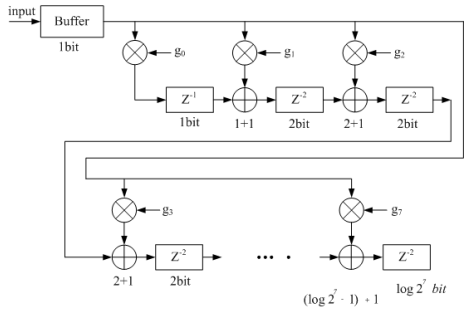
## 3. 시스토릭 어레이 파이프라이닝 구조(PBS)를 가지는 코릴레이터 설계

Binary CDMA 방식은 PW/MP/CS와 같이 여러방식으로 구현된다. 이때 데이터에 대한 동기를 획득한 상태에서 데이터를 처리하게 되는 코릴레이터는 동기시간에 대한 지연이 매우 높아 Binary CDMA의 데이터 처리에 대한 병목현상이 발생되는 곳이다. 이러한 동기 지연시간에 대하여 보다 높은 performance를 가지게 하기 위하여 많은 연구가 진행중에 있다. 가장 대표적인 방식으로는 systolic array 방식, pipeline 방식, full adder 방식 등이 있다.

본 논문은 기존 동기알고리즘들에 대한 장단점들을 하나의 구조로 묶어 동기획득시간의 감소를 가져올 수 있는 PBS(Pipeline Based on Systolic array) 구조와 PBS의 입력을 키 정보로 사용하여 동작하는 암호블록(AES : Rijndael)을 제안하였다.[7] 제안된 PBS-AES 구조는 PBS process element(PE)들로 구성되어 있으며, PBS PE는 그림 2와 같다. 입력이 8비트이며 $a=\{a_0,a_1,a_2,...,a_7\}$ 일때, PBS PE의 출력 $b=\{b_0,b_1\}$는 식 (1)과 같다.

$$b = g_0 \cdot 1 + g_1 \cdot Z^{-1} + g_2 \cdot Z^{-2} + g_3 \cdot Z^{-2} + g_4 \cdot Z^{-2} + g_5 \cdot Z^{-2} + g_6 \cdot Z^{-2} + g_7 \cdot Z^{-2} \quad (1)$$

식 (1)에서 g-function은 gold code 함수로서 입력데이터들에 대한 weight를 제공하게 되며, 동시에 Rijndael 암호알고리즘의 입력 키로 사용된다. 이러한 weight는 동기신호를 획득하기 위한 weight로서 동작하고 각각의 delay 소자는 직렬방식으로 데이터들에 대한 동기를 수행하게 된다.



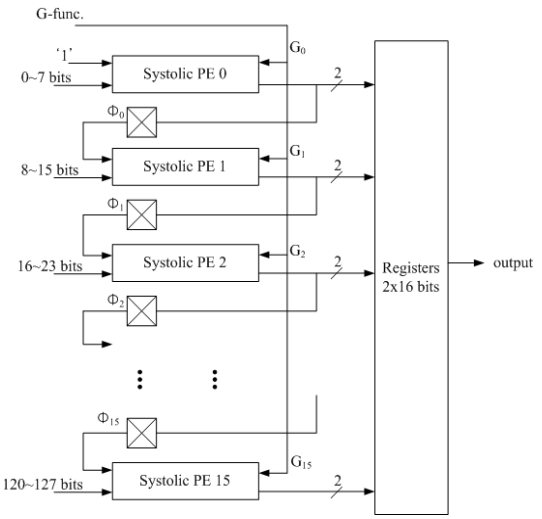

[그림 2] PBS-AES 프로세스 소자
[Fig. 2] PBS-AES processor element

그림 2와 같이 PBS는 기존 systolic array 방식과 동일하지만 PBS를 구성하는 기본 연산 수행이 다르다. 기존 방식은 데이터의 크기가 증가하게 되면 연산되는 systolic array 구조는 비례적으로 증가하게 된다. 즉 $\log_2^n$으로 증가하기 때문에 128, 192, 256비트들에 대하여 처리시간의 지연을 가져올 수 있다는 단점과 더불어 면적 및 소비전력의 증가라는 문제점도 내포하게 된다.

이러한 단점을 없애고자 본 논문에서는 PBS PE를 이용하여 pipeline 방식이 가능하며 데이터량이 증가하여도 동기획득시간의 증가가 발생되지 않는 구조를 갖는 PBS 구조를 제안하였다.

그림 3은 PBS에 대한 기본 구조이다. 그림 3에서 Systolic PE는 8비트씩 16개로 구성되며 입력은 128비트이다. 이때 Rijndael 암호입력도 128비트가 기준이 되어 동작하게 된다. 또한 $\phi$와 Register 2x16은 pipeline 기능을 수행할 수 있도록 중간 결과값을 저장하는 기능을 수행하게 된다. 이때 $\phi$에 저장된 데이터들중 LSB만을 사용하게 된다. 그리고 G는 식 (2)와 같이 g-함수에 대한 블록데이터들이다.

입력 128비트는 8비트씩 16개의 블록으로 분류된다. 분류된 16비트들의 데이터들은 각각의 PE에서 weight와 동기에 관련된 기능을 수행한 후, 2비트의 데이터로 출력된다. 출력된 데이터들중 일부는 다음 stage PE로 이동하며 일부는 Register2x16으로 이동한다.




[그림 3] 제안된 PBS-AES 구조
[Fig. 3] Proposed PBS-AES

$$
\begin{aligned}
G_0 &= \{g_0, g_1, \ldots, g_7\} \\
G_1 &= \{g_8, g_9, \ldots, g_{15}\} \\
&\vdots \\
G_n &= \{g_{8n}, g_{8n+1}, \ldots, g_{8n+7}\}
\end{aligned} \tag{2}
$$

다음 stage PE로 이동된 중간 결과값의 LSB는 PE의 carry로서 동작하게 되며 Register2x16으로 이동한 데이터들은 2비트씩 16개의 32비트 데이터를 생성하게 된다.

생성된 32비트 데이터들과 각 stage PE의 2비트씩 16개는 systolic array 기능을 수행함과 동시에 pipeline 기능을 수행하기 위한 준비과정을 거치게 된다. 만약 192비트가 입력으로 사용될 경우, PE들은 8개 증가된다. 그러나 이때 8개의 PE는 실제적으로 존재하지 않고 PBS 블록의 PE0~PE7블록이 리셋되며 나머지 64비트 데이터들을 입력으로 받아 연산을 수행하게 된다.

## 4. 제안된 Binary CDMA용 PBS architecture 설계

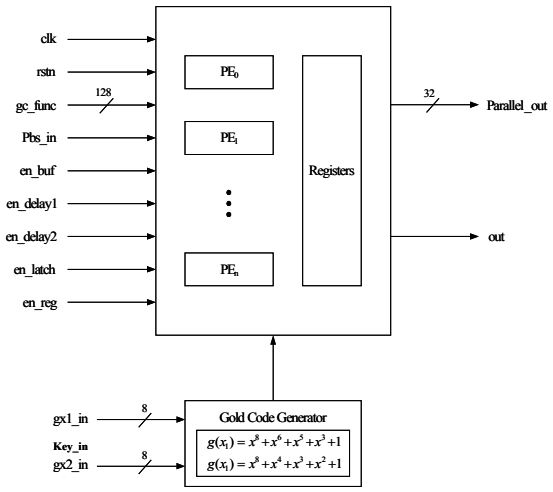
본 논문에서 제안하는 구조는 시스토릭 어레이 구조에 기반을 둔 파이프라인 구조와 AES인 Rijndael 암호알고리즘의 동시 프로세싱이다. 이러한 구조는 기존 구조에 비하여 일정한 크기를 갖는 시스토릭 어레이 구조만을 이용하여 데이터량에 따라 iteration 기능을 수행할 수 있도록 하는데 있다.

식 (3)은 제안된 PBS 구조에 사용할 gold code generator에 대한 원시다항식이다.

$$
\begin{aligned}
g(x_1) &= X^8 + X^6 + X^5 + X^3 + 1 \\
g(x_2) &= X^8 + X^4 + X^3 + X^2 + 1
\end{aligned} \tag{3}
$$

식 (3)은 기본 8비트연산을 수행하면서 확장이 가능한 다항식이다. 그러므로 본 논문의 PBS 구조와 매칭이 되므로 식 (3)의 다항식을 사용하여 코릴레이터를 구성하였다.

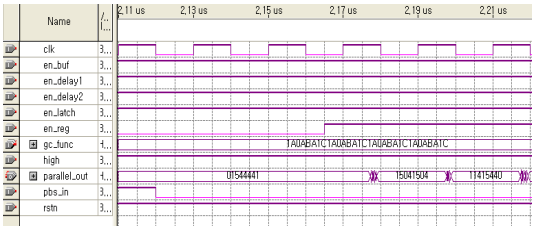
그림 4는 PBS-AES 블록에 대한 입출력 포트를 나타내고 있다.[8,9]




[그림 4] 제안된 PBS-AES 블록
[Fig. 4] Proposed PBS-AES block

PE 블록은 8비트의 시스토릭 어레이 구조를 가진다. 8비트 시스토릭 어레이 구조는 내부 gated delay가 2.73ns가 걸렸다. 그림 4에서와 같이 직렬입력 128비트는 순차적으로 PBS 블록으로 입력된다. 입력된 데이터들은 PE 블록으로 8비트씩 분리되어 입력되며 입력된 데이터들은 각각의 PE에서 시스토릭 어레이 연산을 수행하게 된다. 연산 수행 결과, PE의 출력 2비트의 데이터들은 Register2x16으로 입력됨과 동시에 다음 PE블록의 carry로 동작하기 위하여 PE 출력 2비트중 LSB가 입력된다.

그림 5는 PBS에 대한 최종 모의실험결과 파형이다. gold code generator의 입력과 각종 제어신호들, 그리고 직렬입력신호에 대한 출력값을 보여주고 있다.




[그림 5] PBS-AES 모의실험
[Fig. 5] Simulation of PBS-AES

모의실험에 사용된 툴은 QUARTUS II Ver. 7.1이며 clock period는 20ns로 셋팅하였다.

[표 1] 처리시간에 따른 성능분석표
[Table 1] Performance analysis for processing times

| @128 bits | Delay(ns) | Freq.(MHz) |
|---|---|---|
| systolic array | 3.97 | |
| non-pipeline | 13.25 | @35 |
| pipeline 1 | 12.25 | @70 |
| pipeline 2 | 12.49 | @85 |
| pipeline 3 | 11.91 | @100 |
| PBS-AES | 2.73 | @50 |

## 5. 결론

본 논문에서 제안한 PBS-AES 구조는 Binary CDMA 코릴레이터의 동기획득시간을 감소시킴과 동시에 다양한 센서 데이터를 보호하기 위한 것이다. 제안된 PBS-AES 구조의 모의실험 결과, 표 1과 같이 기존 systolic array 구조 및 pipeline 구조들에 비하여 전달지연시간이 매우 감소됨을 확인하였다.

그러므로 본 논문에서 제안된 PBS-AES 구조를 Binary CDMA 시스템에 사용하게 될 경우, 매우 높은 동기시간을 가짐과 동시에 안전한 채널을 확보할 수 있어 시스템 자체의 performance가 매우 증가할 것으로 사료된다.

## References

[1] IEEE 802. 11 standard, "Wireless LAN medium access control(MAC) and physical layer(PHY) specification", 1997.

[2] K. Pahlavan and A. H. Levesque, Wireless information networks, Wiley Interscience Publication, 1995.

[3] K. Ben Letaief, J. C-I Chuang, and R. D. Murch, "Multicode High-Speed Transmission for Wireless Mobile Communications", Proceedings of the IEEE International Conference on Universal Personal Communications, pp. 1835-1839, 1996.

[4] A. A. M. Saleh and J. Salz, "Adaptive Linearization of Power Amplifiers in Digital Ratio Systems", The Bell System Technical Journal, Vol. 62, pp. 1019-1033, April 1983.

[5] NIST, "Draft FIPS for the AES", http://csrc.nist.gov/publications/drafts.html, Feb. 2001.

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

[7] B. Schneier, "Applied Cryptography : Protocols, Algorithms, and Source Code in C", John Wiley & Sons, Inc., New York, USA, 1994.
[8] NIST, "Draft FIPS for the AES", http://csrc.nist.gov/publications/drafts.html.
[9] Helion, "Rijndael core", http://www.heliontech. com/core2.htm.

**이 선 근**(Seon-Keun Lee) **[정회원]**

- 1997년 8월 : 원광대학교 전자공학과 (공학석사)
- 2003년 2월 : 원광대학교 전자공학과 (공학박사)
- 2011년 4월 ~ 현재 : 전북대학교 화학공학부 겸임교수

<관심분야>
프로세서 설계, 암호알고리즘 분석, 보안시스템설계