KIPS Tr. Comp. and Comm. Sys.
Vol.5, No.3 pp.71~78 pISSN: 2287-5891

http://dx.doi.org/10.3745/KTCCS.2016.5.3.71

Analysis of the Cryptographic Algorithms's Performance on Various Devices Suitable for Underwater Communication

Chae-Won Yun[†] · Jae-Hoon Lee[††] · Okyeon Yi[†††] · Su-Young Shin[††††] · Soo-Hyun Park[†††††]

ABSTRACT

Recently, The interest about underwater acoustic communication is increase such as marine resources, disaster prevention, weather prediction, and so on. Because the underwater acoustic communication uses a water as media, the underwater acoustic communication has a lot of restrictions. Although the underwater acoustic communication is hard, it is important to consider the security. In this paper, we estimate the performance of cryptographic algorithms(AES, ARIA, and LEA) on a various devices, available in underwater acoustic communication, and analysis the results. This result will be provide effective data confidentiality for underwater communication.

Keywords : Underwater Sensor Network, Underwater Acoustic Communication, Cryptographic Algorithm, Performance

수중통신에 활용가능한 다양한 플랫폼에서의 암호 알고리즘 성능비교

윤 채 원[†] · 이 재 훈[††] · 이 옥 연[†††] · 신 수 영[††††] · 박 수 현[†††††]

요 약

최근 환경오염에 의한 수질관리, 재난방지, 해양자원탐사 및 군사목적 등으로 수중환경에서의 음파통신에 대한 관심이 증가하고 있다. 그러나 수중네트워크는 물이라는 특수한 환경으로 인해 많은 제약사항이 존재한다. 이를 극복하기 위한 노력은 계속되고 있으며 더불어 보안의 필요성도 함께 중요시 되고 있다. 본 논문에서는 수중 음파통신에서 활용가능한 다양한 플랫폼에서 AES, ARIA, LEA 암호 알고리즘의 성능을 측정하고 그 결과를 비교 분석하여, 향후 수중 네트워크에서의 통신에 효율적으로 기밀성을 제공할 수 있도록 한다.

키워드 : 수중 네트워크, 수중 음파통신, 암호 알고리즘, 성능비교

1. 서 론

최근 환경오염에 의한 수질관리, 재난방지, 해양자원탐사 및 군사목적 등으로 수중환경에서의 음파통신에 대한 관심이 증가하고 있다[1]. 그러나 수중네트워크는 물이라는 특수한 매체에서 동작을 하므로 지상에서의 네트워크에 비해 많은 제약사항이 존재한다. 물속에서는 지상에서와 같이 고주파 RF를 이용한 통신이 불가능하고, 음파를 이용한 제한적인 통신으로 데이터를 송수신할 수 있다. 음파를 이용한 통신은 지상에서의 통신에 비해 전송속도가 약 10^5배 이상 낮아서 전송할 수 있는 데이터의 양이 제한적이고, 전송 시 패킷 충돌 및 간섭 등이 발생할 수 있다[2]. 열악한 수중 환경을 극복하여 물속에서도 효율적인 네트워크 통신이 가능하도록 하기 위한 노력은 계속되고 있으며 수중 네트워크에 대한 보안의 필요성도 대두되고 있다.

수중 음파통신은 크게 물리 계층, 데이터링크 계층, 네트워크 및 상위 계층으로 나누어 볼 수 있다. 물리 계층에서는 센서를 통해 들어온 신호를 수중 모뎀에서 데이터로 변환하여 데이터링크 계층으로 전달하거나, 데이터링크 계층으로부터 받은 정보를 아날로그 신호를 생성하는 역할을 한

※ 이 논문은 2016년도 BK21 플러스 사업에 의하여 지원되었음.
※ 본 연구는 해양수산부의 지원으로 수행하고 있는 "수중 광역 이동통신 시스템 개발" 사업 결과의 일부임을 밝히며 지원에 감사드립니다.
※ 이 논문은 2014년도 한국정보처리학회 추계학술발표대회에서 '성능비교를 통한 수중통신에 적합한 암호 알고리즘 탐색 '의 제목으로 발표된 논문을 확장한 것임.
† 준 회 원 : 국민대학교 금융정보보안학과 석사과정
†† 준 회 원 : 국민대학교 금융정보보안학과 석 · 박사통합과정
††† 정 회 원 : 국민대학교 수학과 교수
†††† 정 회 원 : 국민대학교 특수통신연구센터 부센터장/전임연구교수
††††† 종신회원 : 국민대학교 정보시스템전공 교수
Manuscript Received : December 22, 2015
First Revision : February 22, 2016
Second Revision : February 26, 2016
Accepted : February 26, 2016
* Corresponding Author : Okyeon Yi(oyyi@kookmin.ac.kr)

다. 데이터링크 계층에서는 상위 계층과 하위 계층의 데이터 흐름을 제어하면서 실제 데이터를 처리하는 기능을 담당하므로 우선적으로 보안의 적용이 고려된다.

본 논문에서는 다양한 플랫폼에서 여러 가지 암호 알고리즘의 성능을 비교분석하여 운영환경에 따른 적합한 암호 알고리즘을 보이고자 한다.

본 논문의 구성은 다음과 같다. 2장에서는 블록암호 알고리즘 AES, ARIA, LEA에 대해 설명하고, 3장에서는 본 논문에서 실험한 다양한 플랫폼에 대한 설명과 각 플랫폼에서의 실험 결과를 비교·분석하고, 4장에서는 결론 및 향후 연구 방향에 대해 제시한다.

2. 관련 연구

정보보호 제품이나 시스템에 보안을 적용하는 경우, 암호 알고리즘은 사용 환경에 적합한 안전성 수준을 고려하여 선택해야 한다. 적절한 암호 알고리즘 선택을 위해 미국, 일본, 유럽 등뿐만 아니라 국내에서도 「암호 알고리즘 및 키 길이 선택」 기준에 대한 가이드라인을 제시하고 있다. 암호 알고리즘의 보안강도는 알고리즘 사용의 유효기간에 의해 결정되는데 2030년 이후까지도 사용을 고려한다면, 기밀성을 제공하는 대칭키 기반 암호 알고리즘은 최소 128비트 이상의 보안강도를 만족하도록 권고하고 있다[3]. 해당 보안강도를 만족하는 적합한 대칭키 암호의 종류로는 국외에서 공통적으로 많이 사용되는 국제표준 암호 알고리즘인 AES-128/192/256이나, 국내표준 암호 알고리즘인 ARIA-128/192/256와 HIGHT, SEED 암호 알고리즘 등이 있다. 이에 더불어 최근 국가보안기술연구소에서 개발한 경량암호 알고리즘인 LEA도 함께 고려할 수 있다. 본 논문에서는 수중환경에 사용가능한 다양한 플랫폼에서 표준 암호 알고리즘인 AES, ARIA와 경량암호로 개발된 LEA, 세 암호 알고리즘의 성능 비교를 통해 지상의 무선 네트워크에 비해 제약사항이 많이 존재하는 수중 환경에 더 적합한 암호 알고리즘을 찾고자 한다.

2.1 AES (Advanced Encryption Standard)

1990년대 DES(Data Encryption Standard) 암호 알고리즘의 해독의 가능성이 높아짐에 따라 미국 NIST에서 1997년에 블록암호 AES(Advanced Encryption Standard)[4]를 공모하였다. 공모 결과 2000년 10월 벨기에에서 만든 Rijndael이 AES로 채택되어 국제 표준 알고리즘으로 지금까지 많은 곳에서 활용되고 있다.

AES 암호 알고리즘은 SPN(Substitution-Permutation Network) 구조를 가지며, 128bit의 고정된 입력 길이에 128bit의 고정된 출력 길이를 가진다. 결정된 보안 강도에 따라 키 길이는 128bit, 192bit, 256bit 중 하나로 결정되며, 결정된 키 길이에 따라 각각 10, 12, 14라운드로 구성된다. 각 라운드는 SubBytes, ShiftRows, MixColumns, AddRoundKey의 네 개의 독립적인 함수로 이루어져 있다.

이 중, SubBytes와 MixColumns 두 개의 함수는 유한체 연산을 기반으로 설계된 함수인데, 구현 방법에 따라 많은 속도 차이가 발생한다. 유한체 연산을 구현하는 방식은 메모리가 적게 요구되지만 속도가 매우 느린 반면, 32bit 단위의 LUT(Look-Up Table) 방식으로 구현할 경우 속도는 빠르지만 많은 메모리를 요구하는 단점이 있다. 제약사항이 많아 저전력 통신이 요구되는 수중환경에서는 전자와 후자의 경우 모두 어려움이 따른다.

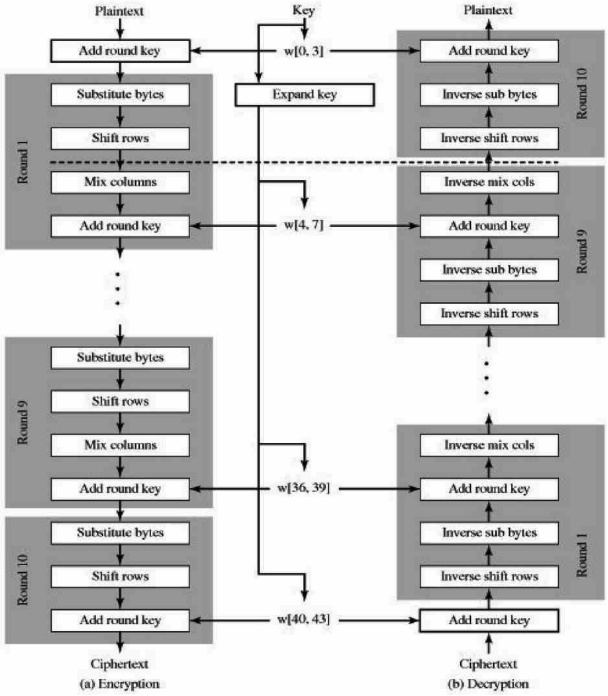

Fig. 1. AES Encryption/Decryption

2.2 ARIA (Academy, Research Institute, Agency)

ARIA(Academy, Research Institute, Agency)[5]는 네트워크 기반의 전자정부 시스템을 비롯한 정보보호 환경을 대비하여 국가보안기술연구소에서 개발된 암호 알고리즘이다. 학계, 연구소, 정부기관이 공동으로 개발하여 2004년 국가표준암호로 지정되어 정부나 공공기관 등 국내 다양한 곳에서 활용되고 있다.

ARIA 암호 알고리즘은 ISPN(Involution SPN)의 구조를 가지며, 128bit의 고정된 입력 길이에 128bit의 고정된 출력 길이를 가진다. AES와 동일한 보안강도를 가지는 ARIA 알고리즘은 결정된 보안 강도에 따라 키 길이는 128bit, 192bit, 256bit 중 하나로 결정되며, 결정된 키 길이에 따라 각각 12, 14, 16라운드로 구성된다. 각 라운드는 AddRoundKey, 치환계층, 확산계층으로 구성되어 있고, 이 중 AES의 SubBytes에서의 연산과 유사한 치환계층은 홀수 라운드와 짝수 라운드에 따라 일부 다르게 구성되어 있다. 확산계층은 ARIA를 다른 알고리즘과 구분 짓는 주요 부분으로 16X16 Involution 이진행렬을 사용한다. ARIA 암호 알고리즘은 ISPN 구조를 가지므로 AES와 달리 암호화와 복호화 과정이 동일한 것 또한 특징이다.

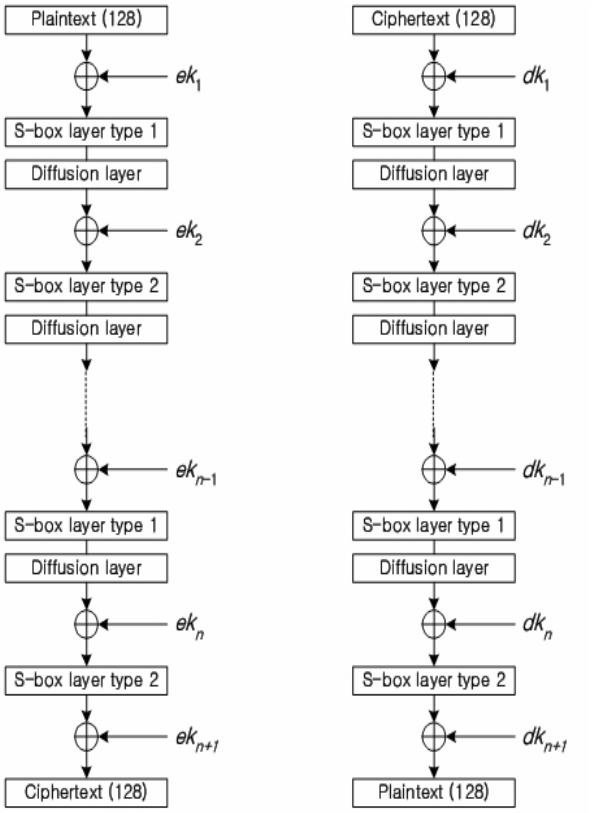

Fig. 2. ARIA Encryption/Decryption

ARIA 암호 알고리즘은 벨기에 루벤 대학으로부터도 안전성에 대한 평가를 받았으며, 하드웨어나 소프트웨어 구현 모두 효율적으로 알려져 있다. 하지만, 16X16의 확산계층에서의 연산은 작은 메모리의 저사양 기기에서는 구현상의 어려움이 있다.

2.3 LEA (Lightweight Encryption Algorithm)

LEA(Lightweight Encryption Algorithm)[6, 7]는 2012년 국가보안기술연구소에서 개발한 높은 안전성과 우수한 효율성을 제공하는 암호 알고리즘이다. LEA 암호 알고리즘은 저전력 데이터 암호화, 대용량 데이터 서버에서의 고속 데이터 암호화에 적합하도록 설계되어 있다.

32bit 단위로 동작하는 LEA 암호 알고리즘은 AES나 ARIA 알고리즘과 달리 SubBytes의 과정 없이 단순한 ARX (Addition, Rotation, XOR) 연산으로 한 라운드를 구성하여 경량 구현이 가능하다는 것이 가장 큰 장점이다. AES, ARIA 암호 알고리즘은 SubBytes 라는 치환과정에서 128 byte의 비선형 치환 테이블인 S-box를 각각 1개, 4개가 요구하지만, LEA는 치환과정이 따로 없으므로 요구되는 메모리와 코드크기가 적다. 또한, AES 암호 알고리즘은 MixColumns이라는 함수에서 유한체 행렬 곱셈이, ARIA 암호 알고리즘에서는 확산함수 부분에서 16X16 행렬 연산이 있어 연산량이 많지만 LEA 암호 알고리즘에서 사용하는 ARX 연산은 모두 프로세서가 제공하는 기본 연산을 그대로 사용할 수 있기 때문에 연산속도가 빠르게 구현이 가능하다. LEA 암호 알고리즘은 AES, ARIA 암호 알고리즘과 마찬가지로 128bit의 고정된 입력 길이에 128bit의 고정된 출력 길이를 가진다. 결정된 보안 강도에 따라 키 길이는 128bit, 192bit, 256bit 중 하나로 결정되며, 결정된 키 길이에 따라 각각 24, 28, 32라운드 수가 요구된다.

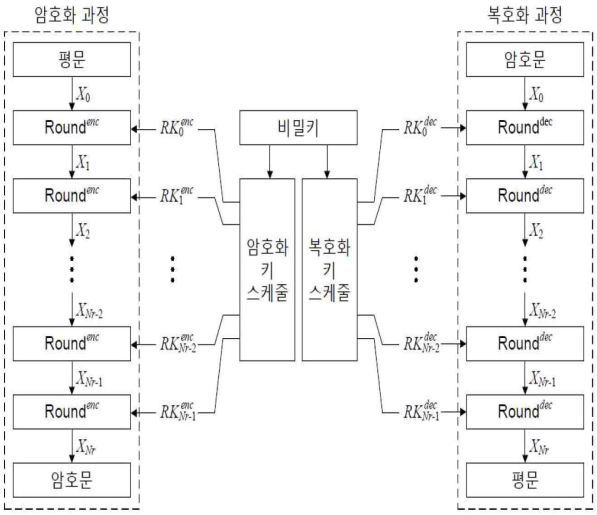

Fig. 3. LEA Encryption/Decryption

LEA 암호 알고리즘은 블록암호에 대한 알려진 모든 공격에 안전하도록 설계되었고, 국외 전문 연구기관인 벨기에 COSIC 연구소로부터 안전성을 검증받았다. 고속, 저전력 암호화가 가능하도록 설계된 알고리즘이어서 저전력 통신을 요구하는 수중통신 환경에서 다양하게 활용될 것으로 기대된다.

3. 실험 환경 및 결과

3.1 실험 환경

본 논문에서는 기존 수중환경에서 언급되고 있는 Cortex-M3 보드를 비롯하여 수중통신에 활용가능한 다양한 플랫폼에서의 실험을 통해 암호 알고리즘의 성능을 비교·분석하고자 한다. 수중 환경에 적합한 보드를 선택하기 위해서는 먼저 수중환경의 특징을 고려해야 한다. 앞서 언급했듯이 수중 환경은 지상의 환경과 다른 매질로 인해 전송 지연이나 패킷 손실 등이 발생하여 원활한 통신이 어렵다. 또한, 수중 환경의 특성상 기기를 한번 물속에 세팅하면 전력 교체나 수리가 어려운 점을 고려하여 에너지 소비가 적으면서도 효율성이 좋은 플랫폼을 위주로 고려하였다. 본 논문에서 선택한 세 가지 플랫폼은 Cortex-M3, ATmega128, Intel Edison으로 저사양부터 고사양의 플랫폼을 다양하게 선택하여 암호 알고리즘의 성능에 미치는 영향을 측정하였다. 각 플랫폼의 특징은 다음과 같다.

1) Cortex-M3

기본적인 수중 환경에서의 통신에 대한 실험을 고려할 때 물리 계층 - 데이터링크 계층에 대하여 실험환경을 구성하는데, Cortex-M3[8]는 본 연구실에서 데이터링크 계층 베이스보드로 사용하고 있다.

Cortex-M3는 ARM계열의 32bit 프로세서로 기존 ARM 기기 대비 30% 이상의 고속 및 저전력의 성능을 가지고 있어 에너지 효율성이 좋다. 동일사양 대비 저가형 기기여서 산업체의 제어 시스템이나 무선 네트워크 장비 등에 많이 활용되고 있는 보드이다. Table 1은 기기의 사양을 보여준다.

Table 1. Cortex-M3 specifications

Feature	Description
MCU	Cortex-M3(STM32F103CB)
OS	Firmware
Size	가로 30mm, 세로 30mm
Power	3.3V

2) ATmega128

ATmega128[9]은 8비트 AVR 마이크로 컨트롤러의 megaAVR 패밀리 계열중 하나의 프로세서이다. 명령어가 간단하며, 동작 속도가 빠른 것이 특징이다. ATmega128은 본 연구실에서 사용하는 Cortex-M3 보다는 저사양을 지니지만 RISC(Reduced Instruction Set Computer) 구조를 사용하여 기타 저사양 기기 대비 저전력 고성능을 가진다.

Table 2. ATmega128A specifications

Feature	Description
MCU	ATmega128A
OS	Firmware
Size	가로 145mm, 세로 100mm
Power	5V

3) Intel Edison

인텔 에디슨[10, 11]은 IoT 분야를 견인하기 위해 Intel이 2014년 출시한 신제품이다. 축소된 사양의 리눅스가 탑재되어 있는 고사양의 장비이다. 소비 전력을 생각하면 성능 대비 매우 낮아 저전력을 요하는 수중환경에 적합하다. 하지만 워낙 고성능의 장비이다보니 기기의 크기나 비용문제를 고려하면 센서 노드나 코디네이터 장비로 사용하기보다는 게이트웨이와 같이 고성능이 요구되는 장비로 사용하는 것이 더 적절할 것으로 고려된다.

Table 3. Intel Edison specifications

Feature	Description
MCU	Intel Quark 100 MHz
OS	Yocto Linux / RTOS
Size	가로 122mm, 세로 72mm
Power	7V - 15V

다음의 Table 4는 앞서 살펴본 세 플랫폼에 대한 비교이다. 동작 가능한 온도나 속도, 메모리를 비교해보면 사양의 차이가 있음을 확인할 수 있다.

Table 4. Compare of three platforms

	Cortex-M3	ATmega128	Intel Edison
Flash (Kbytes)	64 or 128	128	4000 (4GB)
SRAM (Kbytes)	20	4	1000 (1GB)
SPI	O (2)	O	O (1)
USART	O (3)	O	O (1)
I2C	O (2)	X	O (1)
USB	O (1)	X	O (1)
JTAG	X	O	X
Operating Temperature	-40°C to +85°C	-55°C to +125°C	0°C to 40°C
Operating Voltage	2.0V to 3.6V	4.5V to 5.5V	7V to 15V
Core	ARM 32bit Cortex-M3 CPU	Atmel® AVR®	Intel® AtomTM
Speed Grades	72 MHz	16MHz	100MHz

3.2 실험 결과

본 논문에서는 다양한 플랫폼에서 AES, ARIA, LEA 암호 알고리즘의 성능을 측정하고 비교·분석하였다. 동일한 기준을 가지기 위해 세 알고리즘 모두 32비트 단위로 구현하였고, AES 암호 알고리즘의 경우 MixColumns 함수의 유한체 연산 부분을 XTIME 기법을 사용하여 연산횟수를 줄였다. ARIA 암호 알고리즘의 경우 생성된 라운드 키를 역순으로 사용하여 복호화하는 다른 알고리즘과 달리 복호화를 위한 키 생성과정이 별도로 필요하지만, ISPN 구조를 가지므로 암호화과정과 복호화과정은 동일하다. LEA 암호 알고리즘의 경우 ARX 구조를 가지고 있어, 구현상 다른 알고리즘에 비해 간단하였고, 각 라운드를 24번 반복한 것보다 4개의 라운드를 한 번에 고려하여 6번 반복한 결과 더 효율적이어서 후자의 방법을 택해 실험하였다.

실험은 크게 2가지 방법으로 진행하였다. 첫 번째 방법은 세 가지 보드에서 AES, ARIA, LEA 알고리즘에 대한 키 생성과정, 암호화 과정, 복호화 과정을 각각 실험하여, 실제 소요시간과 Kbps(=1000bps, bps : bit per sec), CPB(Cycles per byte) 를 측정하였다. 두 번째 방법은 세 가지 보드에서 각 알고리즘에 대해 키 생성과정 및 암호화 과정, 키 생성

과정 및 복호화 과정으로 나누어 실제 소요된 시간과 Kbps, CPB를 측정하였다.

1) 키 생성 과정, 암호화 과정, 복호화 과정 실험

실제 암호 알고리즘을 적용할 경우 키를 관리하는 부분은 또 하나의 중요한 문제로 작용하게 된다. 따라서 일반적으로 보안제품이나 시스템에 암호 알고리즘을 사용할 경우, 데이터를 암호화 할 때마다 매번 키 생성을 하기보다 한 번 키 생성 과정을 거친 후 생성된 라운드 키로 암·복호화 과정에 반복해서 이용한다.

a) Cortex-M3

Cortex-M3 에서 각 부분별로 시간, Cycle, Kbps, CPB를 측정한 결과 LEA 암호 알고리즘이 모든 부분에서 가장 효율성을 보였다. ARIA 암호 알고리즘의 경우 암호화와 복호화 과정만 보면 AES 암호 알고리즘에 비해 약간의 성능을 보이지만 키 생성 부분에서 많은 시간이 요구되었다.

Table 5. Experiment 1 on Cortex-M3

			time(μs)	Cycles	Kbps	CPB
AES	KeyGen	Enc	67	4,824	1910.45	301.5
		Dec	0	0	0	0
		Enc+Dec	67	4,824	1910.45	301.5
	Enc		282	20,304	453.90	1,269
	Dec		372	26,784	344.09	1,674
ARIA	KeyGen	Enc	169	12,168	757.39	760.5
		Dec	155	11,160	825.81	697.5
		Enc+Dec	288	20,736	444.44	1,296
	Enc		213	15,336	600.94	958.5
	Dec		276	19,872	463.77	1,242
LEA	KeyGen	Enc	64	4,608	2,000.00	288
		Dec	0	0	0	0
		Enc+Dec	64	4,608	2,000.00	288
	Enc		25.9	1,865	4,942.08	116.6
	Dec		24.3	1,750	5,267.49	109.4

b) ATmega128

ATmega128에서 각 부분별로 시간, Cycle, Kbps, CPB를 측정한 결과 AES 암호 알고리즘이 모든 부분에서 가장 효율성을 보였다. LEA 암호 알고리즘에서 사용되는 Addition 과정은 $\mathrm{mod} 2^{32}$의 유한체 덧셈 연산인데, 다른 보드와는 달리 프로세서가 제공하는 기본 연산을 사용하지 못해서 시간이 오래 걸린 것으로 예상된다. 따라서, 단순센싱 기능에 적합한 ATmega128을 사용할 경우에는 LEA 암호 알고리즘의 효율성이 떨어질 것으로 예상된다.

Table 6. Experiment 1 on ATmega128

			time(μs)	Cycles	Kbps	CPB
AES	KeyGen	Enc	798	12,783	160.40	799.0
		Dec	0	0	0	0
		Enc+Dec	798	12,783	160.40	799.0
	Enc		129	2,076	992.25	129.8
	Dec		168	2,689	761.90	168.1
ARIA	KeyGen	Enc	841	13,463	152.20	841.4
		Dec	97	1,553	1,319.59	97.1
		Enc+Dec	938	15,016	136.46	938.5
	Enc		188	3,010	680.85	188.1
	Dec		188	3,008	680.85	188
LEA	KeyGen	Enc	2803	44,851	45.67	2,803.2
		Dec	0	0	0	0
		Enc+Dec	2803	44,851	45.67	2,803.2
	Enc		1289	20,635	99.30	1,289.7
	Dec		1221	19,543	104.83	1,221.4

c) Intel Edison

Intel Edison에서 각 부분별로 시간, Cycle, Kbps, CPB를 측정한 결과 고성능의 장비여서 그런지 전체적으로 좋은 성능을 보였다. ARIA 암호 알고리즘의 경우 전체적으로 다른 알고리즘에 비해 성능이 떨어졌고, AES와 LEA 암호 알고리즘을 비교하면 암호화 키 생성 부분만 볼 경우에 AES가 조금 더 효율성을 보이지만, 암호화나 복호화하는 과정만 각각 고려할 경우 LEA 암호 알고리즘이 조금 더 좋은 성능을 보였다. 본 실험은 키 생성과정, 암호화 과정, 복호화 과정을 각각 측정함으로써 일반적으로 보안 적용시 하나의 세션동안 같은 키를 반복해서 사용하는 상황을 고려하여 실행하였고, 이와 같은 상황을 고려할 경우 LEA 암호 알고리즘이 더 좋은 효율을 보일 것으로 예상된다.

Table 7. Experiment 1 on Intel Edison

			time(μs)	Cycles	Kbps	CPB
AES	KeyGen	Enc	4.4	280	29,090.90	17.50
		Dec	9.0	1140	14,222.22	71.25
		Enc+Dec	13.4	1420	9,552.24	88.75
	Enc		4.7	560	27,234.04	35.00
	Dec		4.0	675	32,000.00	42.19
ARIA	KeyGen	Enc	11.0	2325	11,636.36	145.31
		Dec	8.0	1920	16,000.00	120.00
		Enc+Dec	19.0	4245	6,736.84	265.31
	Enc		8.7	2900	14,712.64	181.25
	Dec		8.5	2895	15,058.82	180.94
LEA	KeyGen	Enc	5.0	965	25,600.00	60.31
		Dec	0	0	0	0
		Enc+Dec	5.0	965	25,600.00	60.31
	Enc		3.0	420	42,666.67	26.25
	Dec		3.5	525	36,571.43	32.81

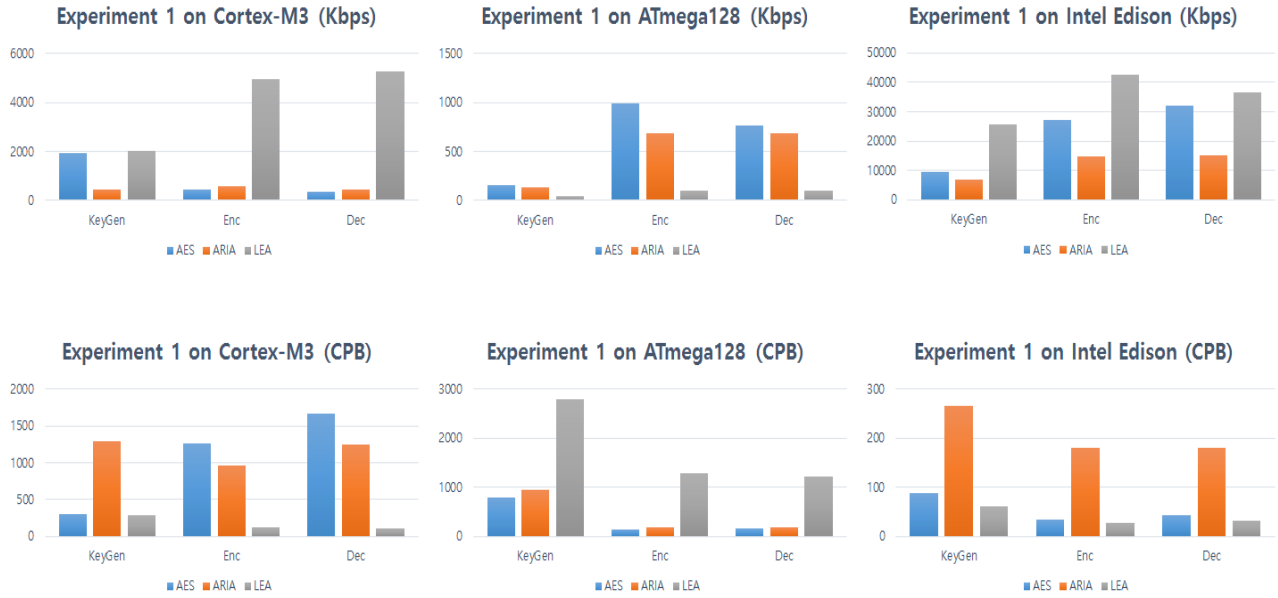

Fig. 4. Result of experiment 1 on boards

세 플랫폼에서 32비트 단위로 연산하도록 구현한 AES, ARIA, LEA 알고리즘에 대해 측정한 결과 32비트 연산을 지원하는 Cortex-M3와 Edison에서는 LEA 알고리즘이 우수한 성능을 보였지만, 8비트 연산을 지원하는 ATmega128에서는 LEA가 효율성이 낮음을 확인하였다. 세 알고리즘 모두 32비트 연산을 하도록 하였으나, 실제 내부에서 연산되는 부분에서 AES와 ARIA 암호 알고리즘은 8비트 단위의 연산의 조합으로 구성되었기 때문으로 예상된다.

2) 키 생성 및 암호화 과정, 키 생성 및 복호화 과정 실험

두 번째 실험은 키 생성 및 암호화 과정, 키 생성 및 복호화 과정을 통합하여 세 보드에서 Kbps와 cpb를 측정하였다. 측정 결과 1)의 실험과 유사한 결과를 보였다. 키 생성 및 암호화 과정 기준으로 8비트 연산을 지원하는 ATmega128에서는 약 4배정도의 시간이 더 소모되었고, 32비트 연산을 지원하는 Cortex-M3와 Intel Edison에서는 각각 6.7배, 4.2배정도 우수한 효율을 보였다.

a) Cortex-M3

Table 8. Experiment 2 on Cortex-M3

		time(μs)	Cycles	Kbps	CPB
AES	KeyGen+Enc	321	23,112	398.75	1,444.50
	KeyGen+Dec	398	28,656	321.61	1,791.00
ARIA	KeyGen+Enc	331	23,832	386.71	1,489.50
	KeyGen+Dec	466	33,552	274.68	2,097.00
LEA	KeyGen+Enc	757	54,504	169.09	3,406.50
	KeyGen+Dec	737	53,064	173.68	3,316.50

b) ATmega128

Table 9. Experiment 2 on ATmega128

		time(μs)	Cycles	Kbps	CPB
AES	KeyGen+Enc	1,157	18,518	110.63	1,157.38
	KeyGen+Dec	1,275	20,410	110.39	1275.63
ARIA	KeyGen+Enc	1,029	16,464	124.39	1,029.00
	KeyGen+Dec	285	4,570	449.12	285.63
LEA	KeyGen+Enc	4,092	65,482	31.28	4,092.63
	KeyGen+Dec	4,024	64,390	31.81	4,024.38

c) Intel Edison

Table 10. Experiment 2 on Intel Edison

		time(μs)	Cycles	Kbps	CPB
AES	KeyGen+Enc	8.00	860	16,000	53.75
	KeyGen+Dec	12.50	1,865	10,240	116.56
ARIA	KeyGen+Enc	18.00	5,230	7,111	326.88
	KeyGen+Dec	14.00	4,835	9,143	302.19
LEA	KeyGen+Enc	6.70	1,395	19,104	87.19
	KeyGen+Dec	7.50	1,480	17,067	92.50

4. 결론 및 향후 연구방향

수중 음파통신은 매질의 특성에 의해 제약 사항이 많아 지상에서의 연구에 비해 많이 미흡한 상황이지만, 다양한 발전 가능성으로 연구가 계속되고 있다. 이에 따라 중요한 정보를 보호하기 위한 보안 적용은 필수적으로 강조되어야 한다. 본 논문에서는 수중 음파통신에서 수집되는 중요한 정보에 대한 보안을 적용하기 위한 방안의 시작으로, 데이터의 기밀성을 제공할 수 있는 암호 알고리즘 AES, ARIA, LEA에 대해 활용가능한 다양한 플랫폼에서 성능을 측정하였다. 측정결과 경량암호로 개발된 LEA 알고리즘의 경우 32비트 연산을 지원하는 플랫폼에서는 뛰어난 효율을 보였으나, 8비트 연산을 지원하는 환경에서는 낮은 효율을 보임을 확인하였다. LEA 암호 알고리즘은 최근 국내에서 개발된 신생 알고리즘으로 알려진 공격들에 대해 안전할 뿐만 아니라 메모리 및 속도 측면에서 높은 효율성을 보이는 점을 고려할 때, 32비트 연산을 지원하는 환경에서 활용 가치가 매우 클 것으로 기대된다. 8비트 연산을 지원하는 환경에서 효율이 떨어지는 것은 8비트 단위로 $\mathrm{mod} 2^{32}$ 위에서의 덧셈 연산하는 것이 어렵기 때문이다. 향후, $\mathrm{mod} 2^{32}$ 위에서의 덧셈 연산을 8비트 연산단위로 효율적으로 할 수 있는 방안에 대한 연구와 실제 수중 통신에 사용되는 통신 프로토콜에 암호 알고리즘을 적용하고 그에 따른 문제점들을 보완하는 방안에 대해 연구를 진행하고자 한다.

References

[1] I. F. Akyildiz, D. Pompili, and T. Melodia, “Underwater acoustic sensor networks: research challenges,” *Ad Hoc Networks*, Vol.3, No.3, pp.257-279, 2005.

[2] Z. Jiang, “Underwater acoustic networks - issues and solutions,” *International Journal of Intelligent Control and Systems*, Vol.13, No.3, pp.152-161, 2008.

[3] Nist Special Publication 800-57, Recommendation for Key Management - Part 1 : General, March, 2007 [Internet], http://csrc.nist.gov.

[4] J. Daemen and V. Rijmen, “The Design of Rijndael: AES-the Advanced Encryption Standard,” Springer Science & Business Media, 2013.

[5] A. Biryukov, C. De Canniere, J. Lano, S. B. Ors, and B. Preneel, “Security and performance analysis of ARIA,” *Final Report, KU Leuwen ESAT/SCD-COSIC*, Vol.3, p.4, 2004.

[6] D. Hong, J. K. Lee, D. C. Kim, D. Kwon, K. H. Ryu, and D. G. Lee, “LEA: A 128-bit block cipher for fast encryption on common processors,” in *Information Security Applications*, Springer International Publishing, pp.3-27, 2014.

[7] D. Hong, J. K. Lee, D. C. Kim, D. Kwon, K. H. Ryu, and D. G. Lee, “LEA: A 128-bit block cipher for fast encryption on common processors,” in *Information Security Application,* Springer International Publishing, pp.3-27, 2013.

[8] J. Yiu, “*The definitive guide to the ARM Cortex-M3*,” Newnes, 2009.

[9] A. A. ATmega, *128L-8-bit AVR Microcontroller with 128K Bytes In-System Programmable Flash*, *Rev.* 2467M-AVR-11/04.

[10] Intel Edison Platform [Internet], http://www.intel.com/content/www/us/en/do-it-yourself/edison.html.

[11] Arduino Platform [Internet], http://www.arduino.cc.

[12] Jin-Young Lee, Nam-Yeol Yun, and Soo-Hyun Park, “Design and Implementation of MAC Protocol for Underwater Mobile Ad-hoc Networks,” *Journal of the Institute of Electronics and Information Engineers*, Vol.51, No.4, pp.76-89, April, 2014.

윤 채 원

e-mail : chwyun91@kookmin.ac.kr
2014년 국민대학교 수학과(학사)
2014년~현 재 국민대학교 금융정보보안학과 석사과정
관심분야 : 네트워크 보안, 정보보호, Underwater Acoustic Network Security

이 재 훈

e-mail : guderian88@kookmin.ac.kr
2013년 국민대학교 수학과(학사)
2013년~현 재 국민대학교 금융정보보안학과 석·박사통합과정
관심분야 : 네트워크 보안, IoT보안

이 옥 연

e-mail : oyyi@kookmin.ac.kr
1988년 고려대학교 수학과(학사)
1990년 고려대학교 수학과(석사)
1996년 Univ. of Kentuchy 수학과(박사)
1999년~2001년 ETRI 선임연구원
2001년~현 재 국민대학교 수학과 교수
관심분야 : 무선이동통신 보안, 암호알고리즘, 네트워크 보안

신 수 영

e-mail : sy-shin@kookmin.ac.kr
1998년 한국방송통신대학교 교육학과(학사)
2003년 덕성여자대학교 정보통신(이학석사)
2007년 국민대학교 비즈니스IT(정보통신)(이학박사)
2008년~현 재 국민대학교 특수통신연구센터 부센터장/전임연구교수
관심분야 : 무선통신 MAC, Underwater Acoustic Network, 통신 표준

박 수 현

e-mail : shpark21@kookmin.ac.kr
1988년 고려대학교 전산과학과(학사)
1990년 고려대학교 수학과 전산학전공(석사)
1998년 고려대학교 컴퓨터학과(박사)
2002년~현 재 국민대학교 정보시스템 전공 교수
관심분야 : IoT / M2M 인프라네트워크, Underwater Acoustic Network