미래 전장환경에서 안전한 데이터 관리를 위한 준동형 시스템 설계

차현종* · 김진묵** · 유황빈***

요 약

미래 전장환경은 주로 네트워크 중심전의 이론을 기반으로 표현되고 있다. 미래의 전쟁에서는 적군보다 먼저 적을 인식하고, 빠르게 의사결정을 하여 정확하게 타격을 하는 것을 목표로 하고 있다. 이를 위해 C4ISR+PGM의 통합체계를 구축 중이다. 이러한 통합체계에서는 정보의 보안측면을 더욱 강화해야 한다. 특히, 보안성의 강화는 효율성의 저하로 이어진다. 때문에 보안성과 효율성이 고려되어야 한다. 이에 본 연구에서는 미래 전장환경에서의 정보공유 중에 데이터를 안전하게 관리할 수 있는 준동형 암호 시스템을 제안한다. 제안기법은 암호문 상태에서 산술연산이 가능한 준동형 암호를 사용한다. 암호문 상태에서 원하는 정보로 수정하여 정보를 전달하므로, 정보전달하는 중에 유출되더라도 공격자는 제대로 된 정보를 확인 할 수 없다.

Design of the homomorphic encryption system for secure data management in the future battlefield environment

HyunJong Cha* · JinMook Kim** · HwangBin Ryou***

ABSTRACT

Be expressed in network-centric warfare, mainly battlefield environment of the future. The purpose of the system for the war of the future, is to recognize the enemy before the enemy, and rapid decision-making, to hit accurately. For this reason , it is during the construction of the integrated system of C4ISR+PGM. In such an integrated system , it is necessary to further enhance the security aspects of the information. In particular, strengthening of security leads to a decrease of efficiency. Therefore, security and efficiency should be considered together. In this study, we provide a homomorphic encryption system that can be safely managed information environment on the battlefield of the future. The proposed method uses encryption technology of homomorphic that can be the arithmetic operations on encrypted state. It has changed from the state of the encryption. Therefore, the attacker can not know a decent information.

Key words : Future battlefile, Homomorphism, Data management

접수일(2014년 3월 10일), 수정일(1차: 2014년 3월 13일), 게재확정일(2014년 3월 14일)

★ 본 논문은 2013년도 광운대학교 교내학술연구비 지원에 의해 연구되었음.

* 광운대학교 방위사업학과
** 선문대학교 IT교육학부(교신저자)
*** 광운대학교 컴퓨터과학과

1. 서 론

과학기술이 빠르게 발전함에 따라 전쟁의 개념과 전쟁을 수행하는 수단도 변화하고 있다. 미 해군제독인 Cebrowski가 제시한 네트워크 중심전은 전장에 참여하는 요소들이 네트워크를 통해 상호 유기적으로 정보를 공유하여 작전 수행능력을 높이는 전투개념이다. 과학기술의 발전에 따라서 점차 네트워크중심전의 이론을 실제화하고 있다. 즉, 국방 선진국은 적군보다 먼저 적을 인식하고, 빠르게 의사결정을 하여 정확하게 타격을 하는 것을 목표로 하고 있다[1, 2, 3].

미래전에서 핵심이 되는 통합체계에서는 정보의 보안측면을 더욱 강화되어야 한다. 때문에 미래전의 준비과정에서 정보보호 분야를 독립적인 요소로 구분하여 연구되고 있다. 정보보호 분야는 네트워크 중심전 환경에서 적의 다양한 사이버 위협 및 공격을 탐지하거나 차단하는 기술이다. 특히 네트워크에서 공유되는 정보를 효과적으로 보호하는 기술이 필요하다. 이 분야에서는 침입탐지기술, 침입대응기술, 침입감내기술로 나뉜다[4, 5].

본 연구에서는 미래 전장환경에서의 데이터의 안전한 관리를 위해 준동형 암호 시스템을 제안한다. 제안기법은 복호화 과정 없이 암호문 상태에서 원하는 정보로 관리를 한다. 제안기법을 적용함으로써 정보전달하는 중에 유출되더라도 공격자는 제대로 된 정보를 확인 할 수 없다.

2. 관련연구

2.1 미래 전장환경

기술의 발전에 따라서 전쟁의 개념과 수단, 도구까지 변화하고 있다. 미래전의 전장양상은 4차원적인 우주공간과 컴퓨터의 수많은 이용에 따라 사이버공간을 활용한다. 지능형 네트워크를 기반으로 정밀 유도와 타격의 중요성이 대두된다. 또한 인명피해를 최소화하기 위해 무인화 무기체계와 방호기술 등이 활용된다.

미래 전장환경에서의 다양한 무기체계들의 원활한 연동을 위해서는 분산컴퓨팅 기술과 상호운용성을 확보할 수 있는 기술이 필요하다. 또한 네트워크에 연결되어 정보를 공유하는 무기체계들의 안정성을 확보하기 위해 정보보호 기술이 요구된다. 정보의 수집과 수집된 정보를 통해 신속하고 정확한 의사결정을 할 수 있는 지휘통제체계를 위해서 정보융합 기술과 모델링 및 시뮬레이션 기술이 필요하다. 전장관리체계와 무기체계의 복합적인 정보처리와 기술의 고도화를 위해 인공지능 기술이 필요하다. 네트워크 중심전에서 필요한 국방정보기술은 (그림 1)을 통해 알 수 있다[6].

(그림 1) 미래전에 필요한 정보기술

2.2 준동형 암호 시스템

동형 암호 시스템은 대수학에서 정의된 두 집합 사이의 연산에 의한 집합을 보존하는 '준동형성'이라는 성질을 갖는 암호 시스템이다. 즉, 준동형 암호는 산술연산 중에서 대표적인 덧셈 연산과 곱셈 연산을 암호문에 적용하여 평문에 대한 연산을 수행할 수 있도록 하는 암호화 기법이다. 이러한 준동형 암호에서 사용한 연산 이외에도 논리연산이 가능한 암호를 완전 준동형 암호라 한다[7].

준동형 암호는 1978년 RSA 암호알고리즘의 개발자인 Rivest와 Adleman, Dertouzous에 의해 최초로 소개되었으며, 'Privacy Homomorphism'이라 불렀다. 이 기법은 RSA암호 알고리즘을 수정하여 제안되었지만, 안정성에 대한 검증이 이루어지지 않았고, 사회적인 주목으로 받지 못하여 사용되지 못하였다. 이를 발전시켜 1996년에 Domingo-Ferrer가 'Symmetric homomorphic encryption'을 제안하였다. 이는 덧셈, 뺄셈, 곱셈 연산이 가능하게 설계되었으나, 비밀 키를 사용자 간에 미리 공유해야 하고, 알려진 평문공격에 취약하다는 단점이 있었다. 2009년 Gentry가 1996년에 제

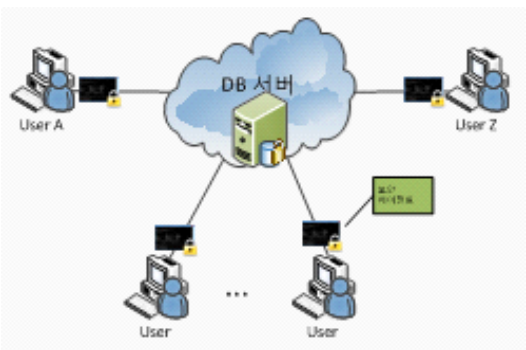
안된 기법을 발전시켜 'Fully homomorphic encryption' 기법을 제안하였다. 이 기법은 복호화에 필요한 정보와 공개키 정보를 암호문과 함께 제공한다. 암호화된 상태에서 일정 횟수까지만 연산이 가능하다[8, 9, 10].

3. 제안 시스템

본 논문에서 제안하는 암호화된 데이터의 관리기법의 시스템 개요를 설명하고, 암호화된 데이터의 검색과 데이터의 공유방법에 대하여 설명한다.

3.1 시스템 개요

제안기법의 시스템의 구성은 (그림 2)와 같다.



(그림 2) 제안 시스템의 개요

정보의 공유를 위해서 통합관리서버에는 암호화된 데이터를 기록하며, 권한을 갖는 사용자만이 데이터에 접근할 수 있다. 서버는 데이터를 수정할 수 없고, 데이터의 저장과 삭제만 할 수 있다. 서버에 저장되는 데이터는 원활한 검색을 위한 키워드가 존재한다. 키워드는 정보의 기밀성 때문에 원문으로 저장되지 않고 암호화된 상태에서 저장된다. 즉, 암호화된 데이터와 매칭이 되는 암호화된 키워드가 존재한다. 이는 DB서버에 직접 접근이 가능한 내부자라 할지라도 복호화 내용을 확인할 수 없다. 각 사용자는 보안기능을 담당하는 보안 에이전트를 포함하고 있다.

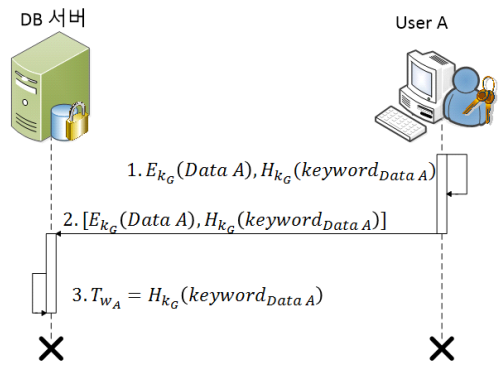
3.2 데이터의 생성

사용자는 접근권한에 대한 인증을 받고 해당하는 그룹 키를 보유하고, 데이터의 생성권한을 보유해야만 데이터를 생성할 수 있다. 데이터 생성에 대한 과정은 (그림 3)과 같이 이루어진다. 데이터의 생성에 대한 세부절차는 다음과 같다.

단계1. $E_{k_G}(Data\,A), H_{k_G}(keyword_{ata\,A})$: 사용자 A는 보유하고 있는 그룹 키로 데이터를 암호화하고, 데이터에 대한 키워드의 해쉬 값을 생성한다.

단계2. 생성한 암호문과 해쉬 값을 하나의 메시지로 만들어 전송한다.

단계3. $T_{w_A} = H_{k_G}(keyword_{Data\,A})$: 사용자 A에게서 받은 해쉬 값은 데이터와 연결되는 인덱스의 역할로 트랩도어를 생성하여 저장해둔다.



(그림 3) 암호화 데이터의 생성

3.3 데이터의 검색

사용자 A가 생성한 데이터는 암호화 상태에서 서버에 저장되어 있다. 또한 해당하는 키워드를 통해 트랩도어를 생성하여 저장 중이다. 암호화 상태의 데이터를 검색하는 시나리오는 (그림 4)와 같다.

사용자 Z는 데이터를 검색하고자 한다. 사용자 Z는 DB서버에 데이터를 검색하기 전에 접근권한에 대한 인증단계를 거쳤다. 또한 사용자 A와 같은 그룹에 속해있으므로 사용자 A와 같은 그룹 키를 보유하고 있다. 데이터의 검색에 대한 세부절차는 다음과 같다.

단계1. $E_{k_Z}(random), H_{k_G}(keyword')$: 사용자 Z는 자신의 시스템에서 생성한 난수를 자신의 키로 암호화하고, 검색하고자하는 키워드를 그룹 키로 해쉬

값을 구한다.

단계2. 난수에 대한 암호문과 검색하고자하는 키워드의 해쉬 값을 서버에 전송한다.

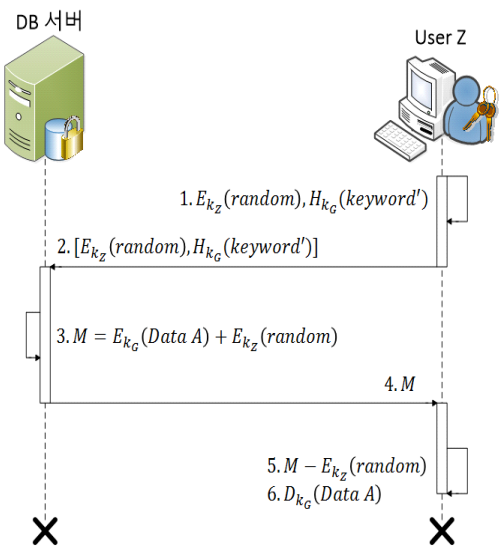
단계3-1. 서버는 전송받은 해쉬 값을 자신이 보유하고 있는 트랩도어와 비교하여 같은 데이터를 추출한다. 같은 해쉬 값이 없으면 데이터가 없으므로 시나리오를 종료한다.

단계3-2. $M = E_{k_G}(Data\,A) + E_{k_Z}(random)$: 사용자 Z에게서 받은 해쉬값과 같은 것이 있다면 해당하는 데이터를 사용자 Z에게 전송할 준비를 한다. 사용자 Z에게서 받은 암호화된 난수와 저장된 데이터를 연산한다.

단계4. 서버는 사용자 A가 생성한 데이터의 암호문과 사용자 Z가 생성한 난수의 암호문의 연산 값인 M을 사용자 Z에게 전송한다.

단계5. $M - E_{k_Z}(random)$: 서버에게서 받은 암호문의 연산 값인 M에 사용자 Z가 생성한 난수의 암호문을 역 연산한다.

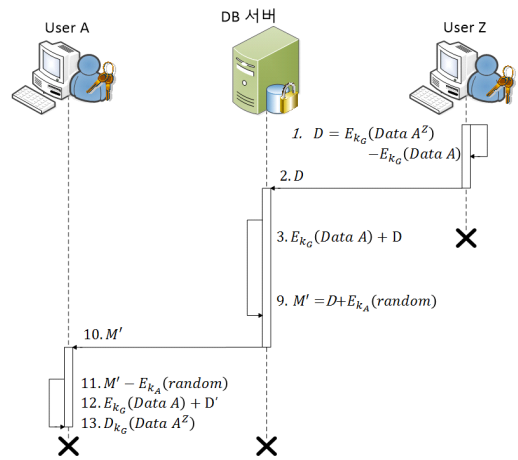
단계6. $D_{k_G}(Data\,A)$: 사용자 Z는 보유하고 있는 그룹 키로 암호문을 복호화하여 평문을 얻을 수 있다.



(그림 4) 암호화 데이터의 검색

3.4 데이터의 수정 및 공유

데이터의 수정과 사용자 A에게 공유하는 시나리오는 (그림 5)와 같다.



(그림 5) 암호화 데이터의 수정과 공유

사용자 A와 사용자 Z는 서버에 접근권한에 대한 인증을 받아서 데이터에 접근이 가능하다. 사용자 A와 사용자 Z는 같은 그룹에 속해있기 때문에 같은 그룹 키를 보유하고 있다. 서버에는 사용자 A가 생성한 데이터의 암호문이 저장되어 있다. 이 데이터에 대해 사용자 Z는 읽기권한 뿐만 아니라 수정 권한도 갖고 있다. 서버에 저장되어 있는 사용자 A가 생성한 암호화 데이터를 사용자 Z는 검색하여 받은 상태이다.

데이터의 수정에 대한 세부절차는 다음과 같다.

단계1. $D = E_{k_G}(Data\,A\,') - E_{k_G}(Data\,A)$: 사용자 Z는 사용자 A가 생성한 데이터를 수정하여 $Data\,A^Z$를 생성하고, 그룹 키로 암호화하였다. 이후 원래 데이터의 암호문과 연산하였다.

단계2. 연산한 결과 값을 서버에게 전송한다.

단계3. 서버는 연산 값을 받아 저장하고 있는 데이터와 역연산을 한다. 이는 데이터의 수정에 대한 기록을 남기기 위해 서버가 형상관리를 하는 것이다.

이렇게 수정 값을 서버에 적용시켰다. 이후 사용자 A는 자신이 생성한 데이터를 다시 검색하려한다. 단계4~단계8까지는 3.2의 데이터검색 단계이므로 생략한다. 이후에 수정된 데이터를 사용자 A가 받아서 복호화하는 세부절차는 다음과 같다.

단계9. $M' = D + E_{k_A}(random)$: 서버는 사용자 Z가 보내온 D와 사용자 A가 보낸 난수의 암호문을 연산한다.

단계10. 연산 결과를 사용자 A에게 전송한다.

단계11. 자신이 서버에게 보냈었던 난수의 암호문을 역연산하여 사용자 Z가 서버에 보낸 데이터를 구한다.

단계12. 자신이 보유하고 있는 원래 데이터와 서버에서 받은 데이터를 역연산하여 사용자 Z가 수정한 데이터의 암호문을 구한다.

단계13. 그룹 키로 복호화하여 수정된 데이터를 구한다.

4. 시스템 구현

제안하는 시스템은 기존의 암호알고리즘을 이용할 수 있다. 암호문의 연산은 크게 행렬 연산과 두 암호문의 유사도 값 연산으로 나눌 수 있다.

4.1 행렬 연산

두 개의 암호문을 연산하기 위해서 행렬 연산을 수행한다. 행렬에서 크기가 같으면 대응하는 원소끼리 서로 더하거나 뺄 수 있다. 곱셈의 경우 앞 행렬의 열의 수와 뒤 행렬의 행의 수가 같아야 가능하다. 행렬 연산은 두 개의 이미지 간에 유사도 측정하는데 주로 사용된다. 블록 암호 알고리즘의 경우에는 블록의 개수가 정해져있기 때문에 행렬연산에 적합하다.

주어진 두 $m \times n$ 행렬 A와 B에 대해 덧셈 A+B과 뺄셈 A-B는 (1)과 (2)와 같이 각 성분의 합과 차로 정의한다.

$$(A+B)_{ij} = A_{ij} + B_{ij} \quad (1)$$

$$(A-B)_{ij} = A_{ij} - B_{ij} \quad (2)$$

4.2 차이 값 연산

두 암호문의 차이를 값으로 연산하기 위해 필요한 연산이다. 이는 상관관계를 기반으로 두 개의 이미지 또는 영상 간의 유사도를 측정하는 것과 비슷하다. 이미지 또는 영상의 비교에서 상관관계 기반의 매칭은 일반적으로 지역 내 각 픽셀의 차이를 계산한다. 즉, 블록 암호문의 경우 픽셀의 값을 비교하는 것과 같은 원리가 된다. 때문에 이미지 또는 영상의 유사성 비교하는 여러 방법 중에서 절대 차의 합(SAD:Sum of Absolute Differences) 공식을 수정하여 (3)과 같이 적용한다. I_1은 비교를 할 첫 번째 암호문을 뜻하면 I_2는 두 번째 암호문을 뜻한다.

$$I_1(i,j) - I_2(x+i, y+j) \quad (3)$$

4.3 두 암호문의 차이 값 연산

암호문의 연산은 행렬연산과 차이 값 연산이 함께 사용된다. 또한 덧셈연산을 하면 역연산인 뺄셈 연산도 있어야 한다. 다음의 (그림 6)은 암호문 연산부분을 슈도코드로 표현한 것이다.

```
read ciphertext1, ciphertext2
read Size ← length of ciphertext1,2

for i=0 to Size
    if operation == ADD than
        Result[i] ← chipertext1[i]+chipertext2[i]
    else
        Result[i] ← chipertext1[i]-chipertext2[i]
End for

Return Result
```

(그림 6) 두 암호문의 차이 값 계산

두 암호문의 차이 값 계산은 두 개가 암호문의 각 바이트단위로 비교하면서 계산되어야 한다. 연산은 덧셈과 뺄셈으로 구성된다.

5. 결 론

본 논문에서는 미래 전장환경에서에서 네트워크를 이용하여 정보를 공유할 때 암호화된 데이터를 전송함으로써 정보의 기밀성을 보장하는 준동형 암호 시스템을 제안하였다. 특히, 최초의 데이터만을 공유하

고 이후의 데이터에서 추가나 수정이 되었을 때, 암호문상태에서 연산이 가능하도록 수정되거나 추가된 부분만을 전송한다. 공격자는 중간에 데이터를 탈취하여 복호화를 하더라도 수정된 부분만이 암호화되어 있기 때문에 정상적인 내용을 확인할 수 없다.

본 연구는 미래 전장환경에서 정보의 기밀성과 접근제어기술을 연계하여 국방정보화의 기초 연구로 참고할 수 있다. 그리고 네트워크 중심전 등의 이점을 최대화하기 위해서는 이동성을 갖는 사용자를 위한 연산 복잡도가 낮은 기법에 대한 연구가 필요하다.

참고문헌

[1] Biff Sturk, Rick Painter ,'C2 Constellation & ConstellationNet', Air Force C2 & ISR Center, 2003.

[2] David S. Albert, John J. Garstka, Frederick P. Stein ,'Net Centric Warfare', DoD CCRP, 2000.

[3] DoD CIO, 'Net-Centric Data Strategy', U.S. DoD, 2003.

[4] 안유성, "사이버공격에 대비한 국방체계 발전방안 연구", 정보보호학회지, 제23권, 제2호, pp.48-54, 2013.

[5] 최중섭, 이경구, 김홍근, "침입감내기술 연구 동향", 정보보호학회지, 제13권, 제1호, pp.56-63, 2003.

[6] 안무정, 손수민, 이대영, "NCW 실현을 위한 전략과 이행방안", 정보과학회지, 제26권, 제11호, pp.40-46, 2008.

[7] N. S. Jho, K. Y. Jang, “Trend and Issue on Homomorphic Encryption”, Weekly IT Brief(2011), Vol. 1522, pp. 15-25, 2011.

[8] Rivest, Adleman, Dertouzos, "On data bank and privacy homomorphisms", Proceedings of the 19th Annual Symposium on Foundations of Secure Computation-FSC 1978, pp169-180, 1978.

[9] J.Domingo-Ferrer, "A New privacy homo -morphism and applications", Information Processing letters, vol.60, no.5, pp.277-282, 1996.

[10] Craig Gentry, "Fully homomorphic encryption using ideal lattices", in Proceedings of the 41st ACM Symposium on Theory of Computing - STOC 2009, pp.169-178, 2009.

[저 자 소 개]

차 현 종 (Hyun-Jong Cha)

2005년 광운대학교 컴퓨터소프트웨어학과 공학사
2008년 광운대학교 컴퓨터과학과 공학석사
2011년 광운대학교 방위사업학과 공학석사
2011년~현재 광운대학교 방위사업학과 박사과정

email : chj826@kw.ac.kr

김 진 묵 (Jin-Mook Kim)

1988년 배재대학교 전자계산학과 공학사
2000년 배재대학교 컴퓨터공학과 공학석사
2006년 광운대학교 컴퓨터과학과 공학박사
2006년~2008년 선문대학교 컴퓨터공학과 연구교수
2008년~현재 선문대학교 IT교육학부 조교수

email : calf0425@sunmoon.ac.kr

유 황 빈 (Hwang-Bin Ryou)

1968년 인하대학교 전자공학과 학사
1975년 연세대학교 전자공학과 공학석사
1984년 경희대학교 전자공학과 공학박사
1981년~현재 광운대학교 컴퓨터소프트웨어학과 교수

email : ryou@kw.ac.kr