산업융합연구 제17권 제1호 pp. 1-6, 2019
ISSN 2635-8875
https://doi.org/10.22678/JIC.2019.17.1.001

키 유출 없이 저장되고 암호화된 정보를 계산할 수 있는 암호기술에 관한 연구

문형진[1], 황윤철[2*]
[1]성결대학교 정보통신학부 조교수, [2]한남대학교 탈메이지 교양교육대학 강의전담교수

A Study on the Cryptography Technology for Computing Stored and Encrypted Information without Key Leakage

Hyung-Jin Mun[1], Yoon-Cheol Hwang[2*]
[1]Assistant Professor, Department of Information & Communication Engineering, Sungkyul University
[2]Assistant Professor, Department of Talmage Liberal Arts College, Hannam University

요 약 정보의 기밀성을 보장하기 위해 고대로부터 다양한 암호기술들이 제안되었고, 다양한 방식으로 발전하고 있다. 기하급수적으로 증가하는 컴퓨터 파워로 인해 안전성 때문에 암호화 키가 점차 증가되고, 짧은 기간에만 안전성을 보장받는 방식으로 기술이 발전되고 있다. 4차 산업혁명의 도래로 다양한 분야에 암호화기술이 요구되고 있다. 최근 동형암호를 활용한 암호화 기술이 주목받고 있다. 암호화된 정보의 연산을 위해 복호화하는 과정에서 사용된 키와 복호문의 노출로 인해 보안위협이 발생된다. 동형 암호는 암호문의 데이터를 연산하여 평문상태의 정보를 노출없이 정보를 안전하게 처리가 가능하다. 다양한 서비스에서 암호화된 개인정보가 저장된 빅데이터 처리시 동형암호을 활용할 경우 키사용과 복호화 평문의 노출이 없기 때문에 보안의 위협을 피할 수 있다.

키워드 : 정보보호, 중국인의 나머지 정리, 동형암호, 암호기술, 암호문연산, 개인식별방지

Abstract Various cryptographic technologies have been proposed from ancient times and are developing in various ways to ensure the confidentiality of information. Due to exponentially increasing computer power, the encryption key is gradually increasing for security. Technology are being developed; however, security is guaranteed only in a short period of time. With the advent of the 4th Industrial Revolution, encryption technology is required in various fields. Recently, encryption technology using homomorphic encryption has attracted attention. Security threats arise due to the exposure of keys and plain texts used in the decryption processing for the operation of encrypted information. The homomorphic encryption can compute the data of the cipher text and secure process the information without exposing the plain text. When using the homomorphic encryption in processing big data like stored personal information in various services, security threats can be avoided because there is no exposure to key usage and decrypted information

Key Words : Information Protection, Chinese Remainder Theorem, Homomorphic Encryption, Cryptographic Technology, Cryptographic Operation, Protection of Personal Identification

1. 서론

고대로부터 현대에 이르기까지 다양한 메시지를 안전

*Corresponding Author : 황윤철(dolpin98@nate.com)
Received January 31, 2019 Revised February 18, 2019
Accepted March 15, 2019 Published March 31, 2019

하게 상대방에게 전달하기 위해 다양한 방법들이 사용되었다. 노예의 머리에 메시지를 적고, 적국을 지나 동맹국에 정보를 전달하는 방식까지 정보의 노출없이 안전하게 전달하는 방법들이 역사를 통해 전해 오고 있다. 다양한 정보를 안전하게 전달, 처리하기 위해서 알아 볼 수 없는 기호나 문자를 변화하여 상대방에게 전달한다. 알 수 없는 기호나 문자를 변화하는 과정을 암호화라 하고, 이는 정보의 기밀성을 보장하기 위한 대표적인 방법이다.

근대에 들어와서 정보를 암호화하는 방법과 암호화된 정보를 복호화하는 방법을 짧은 키를 이용하여 수행하므로써 키가 암호화 기술의 안전성을 보장하게 되었다. 대칭키 암호기술로 대표적인 DES(Data Encryption Standard) 알고리즘은 56bit이 키를 가지고 있고 이를 기반으로 암호화와 복호화가 가능하다. 하지만 기하급수적으로 증가하는 컴퓨터 파워로 인해 암호화된 정보는 다양한 공격이 시도되어 안정성을 보장받지 못해 키 길이를 128bit로 확장되는 암호화기술이 제안되어 사용되고 있다. 안전성을 보장받기 위해 키의 길이가 증가되고, 짧은 기간에만 안전성을 보장받는 방향으로 대칭키 암호기술이 사용되고 있다. 웹사이트에서 비빌번호를 주기적으로 변경하는 이유도 안전성 보장을 위해 저장기간을 제한하고 있다. 즉, 암호문을 복호화하기전까지는 암호문은 키유출이 없을 경우 일정한 시간내에 안전성을 보장받는다.

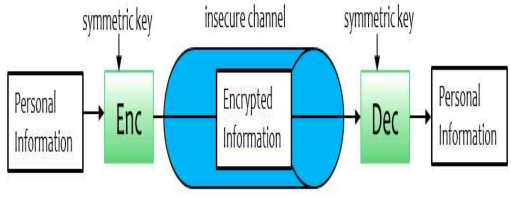
다양한 서비스를 제공하기 위해 개인정보를 수집하고, DB에 저장한다. 하지만 프라이버시 침해 가능성으로 인해 다양한 법률로 인해 저장된 정보를 접근제어 및 암호화 기술을 적용하여 보호하고 있다[1-3]. 하지만 다양한 서비스 제공을 위해 저장된 정보 연산이 필요할 경우 많은 보안위협에 노출되어 있다.

최근, 4세대 암호기술로 알려진 동형암호는 개인정보 보호 등에 활용한 개인식별방지 기술 연구가 주목받고 있다. 다양한 단말기를 통해 생성된 빅데이터의 효율적인 데이터 활용 수요가 늘어나지만 기존 암호화 기술로는 기하급수적으로 증가된 컴퓨터 파워 등으로 보안 위협이 높아지고 있다[4]. 동형암호(Homomorphic Encryption)는 평문과 암호문에서 같은 성질이 유지되어 평문에 대한 산술연산결과나 암호문에 대한 산술연산결과가 동일한 암호화 기술이다[5,6]. 완전동형암호(Fully Homomorphic Encryption)는 산술연산인 덧셈과 곱셈에 대해서 동형의 성질이 유지되는 암호화 방식을 의미한다[5,7-9].

동형암호 기술은 암호화된 개인정보를 복호화하지 않고도 통계분석이 가능하면 개인정보 유출 가능성이 작아진다. 즉, 동형암호는 암호화된 데이터를 복호화 없이 연산하는 암호다. 암호화된 개인정보 뿐만 아니라 암호화된 상태에서 통계처리나 검색, 기계학습이 가능하여 공격자에 의해 데이터를 해킹당하더라도 키 유출이 없고, 암호화되어 안전성이 보장된다. 이는 의료나 금융 분야에서 개인 빅데이터 정보를 활용시 암호화된 정보라 유출시에도 개인식별이 불가하기 때문에 완전한 암호화 기술로 인식된다[10,11]. 단지, 암호문이 기존 방식보다 수 십 배 증가하기 때문에 암호문 연산 시간이 수 백 배로 길어지는 단점이 있다. 즉, 암호화 및 연산시 효율성이 떨어지지만 연산 속도 등 컴퓨터 파워가 증가되어 시간에 대한 단점을 극복하고 있어 관련 연구가 활발하게 진행되고 있다.

2. 관련 연구

많은 시스템이나 웹사이트에서 사용가능한 패스워드 기반의 인증기술인 1세대 암호, 대칭키를 이용한 암호방식으로 데이터를 암호화하는 2세대 암호, 짝이 되는 개인키 및 공개키를 기반으로 RSA 암호알고리즘 등의 공개키 암호를 3세대 암호로 불린다. 공개키 암호기술은 대체로 대칭키를 안전하게 수신자에게 전달하기 위해 사용된다. [Fig. 1]은 2세대 암호인 대칭키를 이용하여 평문을 암호화 하고, 안전하지 않는 채널을 통해 수신자에게 전달되고, 수신자는 동일한 대칭키로 암호문을 복호화하는 과정을 나타낸 것이다.

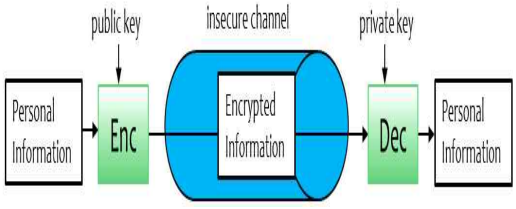


[Fig. 1] Encryption and decryption process using symmetric keys

대칭키 암호기술은 동일한 키를 송신자와 수신자가

가지고 있어야 한다. 사전에 동일한 키를 가지고 있다는 전제하에서 정보를 안전하게 전달할 수 있다. 대칭키 암호의 장점으로는 컴퓨터가 쉽고 빠르게 계산할 수 있는 연산을 위주로 암호화하거나 복호화하기 때문에 암호화 및 복호화 속도가 상당히 빨라서 대량의 정보를 암·복호화에 적합하다. 특히, 네트워크 상에서 안전하게 데이터를 송수신하는 방법으로 대칭키 암호 방식을 주로 사용한다[12].

3세대 암호기술인 수신자의 공개키를 이용하여 평문을 암호화 하고, 안전하지 않는 채널을 통해 수신자에게 전달된다. 안전하지 않는 채널을 통해 암호문이 전달되기 때문에 제 3자가 가로챌 수 있지만 암호화되어 있기 때문에 복호화할 수 있는 키를 가지고 있지 않기 때문에 암호문의 내용을 볼 수 없다. 오직 개인키를 가지고 있는 수신자만이 암호문을 복호화하여 내용을 볼 수 있다. [Fig. 2]은 3세대 암호기술인 공개키를 이용하여 안전하게 정보를 전달하는 과정을 나타낸 것이다.



[Fig. 2] Encryption and decryption process using public keys

3세대 공개키 암호기술은 소인수분해의 어려움이나 이산대수의 어려움 등을 기반으로 2개의 키를 생성하고, 암·복호화하는 기술로, 컴퓨터 파워가 증가함에 따라 정보 해독 가능성이 높아진다. 공개된 키를 가지고 짝이 되는 개인키를 유출할 가능성이 있기 때문에 키의 길이가 커지거나 안전성을 보장하는 시간을 단축할 수밖에 없다. 안전성을 위해 키의 길이 길어지는 것 만큼 암호화·복호화 시간이 많이 소요된다.

현재, 공개키 암호기술은 주로 메시지가 짧은 평문을 대상으로 전자서명이나 대칭키를 안전하게 전달하는 수단으로 활용된다. 전자서명을 하기 위해 PKI 기술을 기반으로 현재 많이 사용되고 있지만 암호화된 정보가 DB에 저장되어 통계처리나 연산을 하는데 연산속도 측면에서 어려움이 있다.

3. 암호문 연산이 가능한 암호기술

3.1 동형암호

동형암호 기술은 NoKey 암호방식으로 암호화된 상태에서도 연산이 가능한 암호방식이다. 동형암호(Homomorphic Encryption) 스킴은 1970년대 처음 이론 연구가 시작되었고 많은 연구들이 진행되고 있다. Goldwasser와 Micali, ElGama, Paillier 등이 암호화 스킴에서 암호문에 대한 동형 계산이 가능하다. Boneh et. al 는 한 번의 곱셈과 여러 번의 덧셈 연산이 가능한 스킴이 처음으로 제안하였다[13]. 동형암호는 2009년에 IBM 연구원인 Gentry에 의해 동형암호의 기술적 가능성이 증명되었다[14,15].

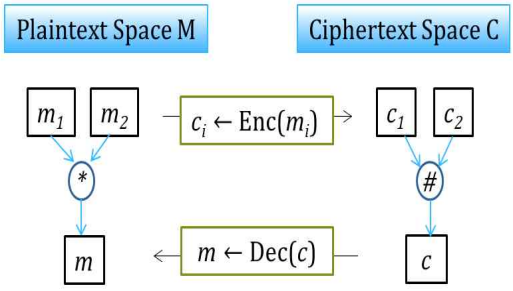
한국스마트인증은 2018년 5월에 동형암호 기술를 활용하여 홍채인증 기술을 개량 발전시켜 홍채인증 시간을 2초에서 0.25초로 단축한 시스템을 선보였고, 코리아크레딧뷰(KCB)는 금융분야에서 50만 명의 신용데이터를 동형암호을 이용하여 암호화하여 머신러닝을 활용해 신용평가 모형의 신뢰성과 정확성, 안전성을 보여주었다[4].

다양한 정보를 수집하고, DB에 저장되어 있지만 다양한 해킹이나 공격으로부터 안전성을 보장받기 위해 암호문 상태로 저장할 수 밖에 없다. 하지만 암호화된 정보로 저장될 경우 DB에서 원하는 정보를 검색할 경우 키워드 검색이 어렵기 때문에 수집된 정보를 암호화하기 전에 정보의 키워드를 추출하여 따로 저장하는 방법 등의 방법을 사용하지만 이는 정보주체의 동의를 따로 구해야 하는 문제가 제기된다.

다양하고 대용량의 정보를 한 곳에 저장하기 보다는 클라우드 컴퓨팅을 활용하여 정보를 다양한 노드에 저장하고 있기 때문에 정보의 연산을 위해서는 암호화된 정보를 다운받고, 복호화키를 찾아서 로컬 노드에서 복호화하여 로컬 서버에 저장하고, 이를 연산하고 다시금 암호화키로 암호화하여 클라우드 컴퓨팅 저장소에 저장하는 여러 단계의 절차가 있고, 각 과정마다 보안 위협이 존재한다. 복잡하고 보안위협으로부터 해결하기 위한 다양한 방법이 제시되었지만 근본적인 해결책이 되지 않았다. 이 문제 해결책으로 제시된 동형암호를 이해하기 위해 Table 1에서 용어에 대한 설명을 제시한다.

<Table 1> Notation

Notation	Meaning
m	message
$Enc()$	encryption function
$Dec()$	decryption function
$\mathrm{mod}p$	remainder by mod p



[Fig. 3] Concept of Homomorphic Encryption

[Fig. 3] 는 동형암호의 기본 개념을 나타낸 그림이다. 동형암호는 하나의 연산에 대해 식(1)과 같이 만족한다. 덧셈과 곱셈의 연산에 식(2)(3)를 동시에 만족할 때 완전동형암호이다.

$$E(m_1 * m_2) = E(m_1) * E(m_2) \quad (1)$$
$$E(m_1 + m_2) = E(m_1) + E(m_2) \quad (2)$$
$$E(m_1 \cdot m_2) = E(m_1) \cdot E(m_2) \quad (3)$$

3.2 동형암호를 이용한 암호문 연산방식

2개의 메시지(m_1, m_2)를 연산한 결과 $m_1 + m_2 = m$ 일 때 다음과 같은 결과가 있다.

$$E(m_1) = [c_1(\mathrm{mod}p), d_1(\mathrm{mod}q)] \quad (4)$$
$$E(m_2) = [c_2(\mathrm{mod}p), d_2(\mathrm{mod}q)] \quad (5)$$
$$\begin{aligned} & E(m_1 + m_2) \\ &= [c_1 + c_2(\mathrm{mod}p), d_1 + d_2(\mathrm{mod}q)] \\ &= [c_1(\mathrm{mod}p), d_1(\mathrm{mod}q)] + [c_2(\mathrm{mod}p), + d_2(\mathrm{mod}q)] \\ &= E(m_1) + E(m_2) \end{aligned} \quad (6)$$

각 메시지마다 암호화를 한 결과는 식(4),(5)과 같다[10]. 식(6)를 보면 2개의 메시지의 연산한 메시지의 암호문과 각각의 메시지의 암호문을 연산한 결과가 같음을 보여주고 있다. 동형암호를 이용하면 암호문을 복호화하지 않고, 암호문 간의 연산으로 평문의 연산된 결과를 암호화하지 않아도 된다. 즉, 키를 이용한 복호화 없이 평문의 연산이 가능하다.

동형암호를 이용하면 다수의 개인정보를 가공하고자 할 때 개개인의 정보를 일일이 확인하지 않고, 각 개인의 정보에 대해 암호화된 모든 정보를 복호화하므로써 개인정보를 평문의 연산과 동일하게 된다. 이를 통해 저장된 개인정보의 평문 상태를 요청없이도 가공이 가능하다. n명의 개인의 정보(m_i)를 각각 암호화(C_i)하여 덧셈 연산을 한 결과는 식(7)와 같다. 각각의 암호문은 키를 이용하여 암호화되어 있어 복호화키를 알지 못하면 정보를 알 수 없다.

$$\begin{aligned} & C_1 + C_2 + \cdots + C_n \\ &= (m_1 + Key \times a_1) + (m_2 + Key \times a_2) \\ &+ \cdots + (m_n + Key \times a_n) \\ &= C \end{aligned} \quad (7)$$

$$C = (m_1 + m_2 + \ldots + m_n) + Key \times (a_1 + a_2 + \ldots + a_n) \quad (8)$$

식(8)은 암호문이 연산된 결과로 나온 암호문은 복호화하면 최종적으로 다수의 개인정보의 덧셈 연산을 한 결과를 key로 암호화한 암호문과 식(7)의 암호문과 동일함을 알 수 있다.

4. 결론

ICT 의 발달로 인해 다양한 정보가 생성되고, 안전하게 정보 소비자에게 전달할 필요성이 높아지고 있다. 특히, 4차 산업혁명에서 정보의 안전한 전달, 정보의 안전한 관리 등 보안의 중요성이 높아지고 있다. 특히, 클라우드 컴퓨팅 환경에서 기관 등에 저장된 정보의 관리 및 다양한 서비스를 제공하기 위한 정보의 연산이 필요하다[16]. 기관은 사용자의 다양한 기기를 통해 수집된 정보의 관리가 중요하다. 특히 이렇게 수집된 정보를 기반

으로 사용자에게 개인별 서비스를 제공해야 한다.

하지만, 개인별 서비스를 제공을 목적으로 수집된 개인정보를 일괄적인 키를 이용하여 복호화하고, 처리하는데 어려움이 많다. 암호화되어 저장된 정보의 연산 등이 필요한 환경에서 동형암호의 필요성이 제기된다. 동형암호기술을 활용하면, 모바일 단말기에 제공되는 개인별 광고, 개인의 건강정보, 개인의 자산이나 주식과 같은 경제정보 등을 안전하게 보호하기 위해 암호화하면서도 더 나은 서비스를 위해 암호화된 정보를 연산하여 개인에게 다양한 개인별 서비스를 제공할 수 있다[17].

본 연구에서는 동형암호의 개념과 기존암호 방식과의 차이점, 동형암호 적용 방식 등에 대해 언급하였다. 또한 차세대 기술인 블록체인 기술에서 대칭키 암호 알고리즘과 공개키 암호 알고리즘을 활용되고 있다. 블록체인 기술에서 블록에 담겨져 있는 암호화된 정보의 연산 필요성과 동형암호의 활용 측면에 대한 연구가 필요하다.

향후 연구로는 정보의 연산과정에서 발생 가능한 노이즈를 줄이고, 실제 시스템에 적용시 키 생성과 암호화하는 시간을 줄일 수 있는 알고리즘 개발이 필요하다.

REFERENCES

[1] Hyung-Jin Mun, Kun-Hee Han. (2016). A Study on Design for Efficient Personal Policy of Service based RBAC. *Journal of Digital Convergence, 14(2),* 191-196. doi:10.14400/JDC.2016.14.2.191

[2] Hyung-Jin Mun, Jung-Seok Suh. (2008). Sensitive Personal Information Protection Model for RBAC System. *Journal of the Korea Society of Computer and Information, 13(5)*, 103-110.

[3] Hyung-jin Mun, Keon-myung Lee, Yong-zhen Li, Dong-heui Lee, Sang-ho Lee. (2006). Design of a Policy based Privacy Protection System using Encryption Techniques. *Journal of the Korea Institute of Information Security & Cryptology*, 16(2), 33-43.

[4] DongaScience. (2018.11.19.). Identifying homophobic code technology for safe data utilization. http://dongascience.donga.com/news.php?idx=25155.

[5] Jong-Hyuk Im, Mun-Kyu Lee. (2015). Implementation and performance comparison of batch homomorphic encryption applications over the integers. *The Journal Of Korean Institute Of Next Generation Computing,* 11(6), 19-28.

[6] Minseok Oh. (2018). Strengthening Big Data Privacy through homomorphic encryption, *Proceedings of the Korea Information Processing Society Conference*, 139-141.

[7] Myoung In Jeong. (2013). Technical Trend of Fully Homomorphic Encryption. *The Journal of the Korea Contents Association*, 13(8), 36-43. doi:10.5392/JKCA.2013.13.08.036

[8] Sehwan Kim, Hyunsoo Yoon. (2014). A Survey of applying Fully Homomorphic Encryption in the Cloud system. *Journal of the Korean Institute of Information Security and Cryptology*, 24(5), 941-949 doi:10.13089/JKIISC.2014.24.5.941

[9] Jae-Heon Kim, Sang-Kyung Yoo, Sang-Han Lee. (2013). Fully Homomorphic Encryption Scheme without Key Switching. *The Journal of Korean Institute of Communications and Information Sciences*, 38(5), 428-433. doi:10.7840/kics.2013.38C.5.428

[10] Rivest-Adleman-Dertouzos, On data banks and privacy homomorphism, FOSC'78.

[11] Hyunsung Kim, Sung-Woon Lee. (2013). Homomorphic Encryption Scheme and Applications for Cloud Computing Security, *Journal of Security Engineering*, 10(2), 213-224.

[12]Jun Seok Lee. (2009). A Study on the Multicast Security System in Multiple Core Environment. *Journal of Industrial Convergence*, 7(1), 21-31.

[13] D. Boneh, E.-J. Goh, K. Nissim. (2005, Feb). Evaluating 2-DNF formulas on ciphertexts, *In Proc. Theory of Cryptography Conf. (TCC) '05,* 325-341, Cambridge, U.S.A.

[14] Gentry, C., & Boneh, D. (2009). A fully homomorphic encryption scheme, 20(09). Stanford: Stanford University.

[15] C. Gentry. (2009, May). Fully homomorphic encryption using ideal lattices. *In Proc. 41st*

ACM Symp. Theory of Computing (STOC). 169-178, Bethesda, U.S.A.

[16] Hyun-Jong Cha, Ho-Kyung Yang, Kang-Im Choi, Hwang-Bin Ryou, Hyo-Young Shin. (2015). Design of the secure data management system using homomorphic encryption. *Jouranl of Information and Security*, 15(4), 97-103.

[17] Armknecht, F., Boyd, C., Carr, C., Gjøsteen, K., Jäschke, A., Reuter, C. A., & Strand, M. (2015). A Guide to Fully Homomorphic Encryption. *IACR Cryptology ePrint Archive*, 1192.

문형진(Hyung-Jin Mun) [종신회원]

・2008년 2월 : 충북대학교 전자계산학과(이학박사)
・2017년 3월 ~ 현재 : 성결대학교 정보통신공학부 조교수

・관심분야 : 정보보안, 네트워크 보안, 빅데이터분석
・E-Mail : jinmun@gmail.com

황윤철(Yooncheol Hwang) [정회원]

・2008년 2월 : 충북대학교 전자계산학과(이학박사)
・2005년 9월 ~ 2007년 2월 : 충북대학교 IT 누리 초빙교수
・2017년 9월 ~ 현재 : 한남대학교 탈메이지 교양교육대학 강의전담교수

・관심분야 : 네트워크 및 웹보안, IDS, ITS, Fusion IT Technology
・E-Mail : dolpin98@nate.com