텔레그램의 IGE 모드에 대한 양자안전성 검증[1)]

김성숙* 이지은* 김광조*,**

*카이스트 전산학부/ **정보보호대학원

On the Quantum Security of IGE mode in Telegram

Sungsook Kim* Jeeun Lee* Kwangjo Kim*,**

*School of Computing/ **Graduate School of Information Security, KAIST

요 약

블록암호는 일정 블록 단위로 평문을 암호화하고 있으며, 다양한 길이의 평문을 암호화를 위하여 운영 모드를 사용하는 데 널리 알려진 보안 메신저인 텔레그램은 IGE(Infinite Garble Extension)이라는 특수한 운영 모드를 사용하고 있다.

양자 컴퓨터에 대한 연구가 활발히 진행됨에 따라 현재 사용되는 블록암호들은 양자 안전성 증명에 대한 필요성이 대두되고 있다. 특히, 블록암호의 양자 안전성은 사용하는 암호 알고리즘과 운영모드에 따라 안전성이 결정된다. 본 논문에서는 암호알고리즘이 sPRF(Standard-secure PRF)일 때 IGE 운영모드가 양자 안전성을 보장하지 않음을 증명하였다.

I. 서론

일정 블록 단위의 키와 평문 및 복호문을 가지고 있는 블록암호는 매 블록 단위로 평문(암호문)을 암호화(복호화)를 하고 있으며 평문이 블록 크기에 맞지 않을 때, 패딩 데이터를 추가하여 블록 단위로 처리할 수 있도록 다양한 운용 모드(Mode of Operation)가 있다.

현재 컴퓨터에 의한 계산적 안전성을 검증한 다양한 블록 암호들이 실제 많이 사용되고 있지만, Shor의 알고리즘[1]이 발표된 이래 수년 이후 상용화가 예상되는 양자컴퓨터를 사용한 공격에 대비하여 양자 안전성을 검증하는 것이 대단히 중요하게 대두되고 있다.

블록암호의 양자 안전성은 사용하는 블록함수와 운용 모드에 따라 그 안전성이 결정되며 본 논문에서는 텔레그램에서 사용되는 IGE(Infinite Garble Extension) 모드에 대한 양자 안전성에 대해 검증하고자 한다.

텔레그램은 대표적인 보안 메신저로, 최근 스마트폰이 보급되면서 많은 사람들이 다양한 메신저를 사용하면서 개인 정보를 보호할 수 있는 암호화된 메신저에 대한 관심이 높아지고 있으며 이러한 안전성 때문에 텔레그램의 사용자들도 급격히 증가하고 있는 추세다. 텔레그램은 자체 개발된 보안성이 있는 MT프로토(MTProto)라는 프로토콜을 사용하며, 이 프로토콜에서 IGE 모드가 활용된다.

1) 이 논문은 2017년도 정부(과학기술정보통신부)의 재원으로 정보통신기술진흥센터의 지원(No.2017-0-00555, 양자 컴퓨터 환경에서 래티스 문제를 이용한 다자간 인증키교환 프로토콜 연구, 2013-0-00396, 생체모방 알고리즘(Bio-Inspired Algorithm)을 활용한 통신 기술 연구)과 2017년도 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (No. NRF-2015R1A2A2A01006812)

1.1 논문의 구성

본 논문의 구성으로 Ⅱ장에서는 양자계산, IGE모드, 안전성증명에 대해 간략히 기술하고, Ⅲ장에서는 sPRF 암호 알고리즘을 IGE 모드로 사용할 때 양자 안전성을 보장하지 않음을 양자 회로를 구현하여 증명한다. 마지막으로 Ⅳ장에서는 요약하고 추후 연구할 내용에 대해 제시한다.

II. 배경지식

2.1 양자 계산

양자 시스템은 Hilbert공간, 의 내적 $|\cdot\rangle$을 포함하고, 양자 시스템의 상태(state)는 내적이 1인 벡터 $|\psi\rangle$로 표현한다. H의 직교기저가 $= |b \ ,...,|b_{d-1}\rangle\}$일 때 양자 상태 $|\psi\rangle$를 측정하면 $\left|\langle b_i|\psi\rangle\right|^2$의 확률로 b_i가 나오며 이때 $|\psi\rangle$가 b_i로 붕괴(collapse)한다고 한다. 서로 상호작용하지 않는 두 부분계 $|\psi_1\rangle\in H_1, |\psi_2\rangle\in H_2$로 이루어진 전체 계는 분리 가능한 (separable) 양자 상태이며, 이는 텐서 곱(Tensor Product)을 이용하여 $|\psi_1\rangle\otimes|\psi_2\rangle\in H_1\otimes H_2$로 표현한다.

2.2 Infinite Garble Extension(IGE) 모드

IGE모드는 현재 텔레그램의 MTProto에서 사용되는 모드로 1978년 Campbell[2]에 의해 처음 제안되었으며 [그림1]과 같이 동작한다.

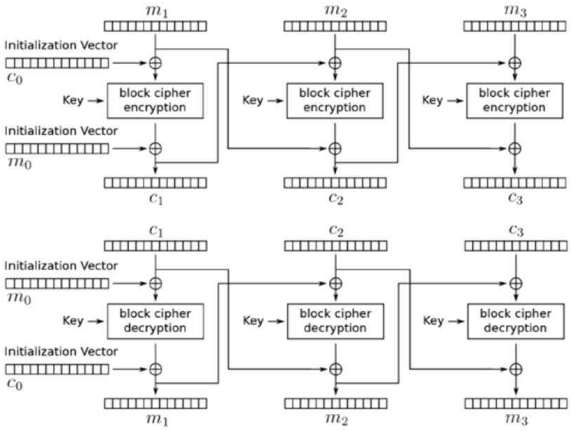
주어진 블록암호 E에서 대칭키 암호알고리즘 Π_{GE}=(Gen,Enc,Dec)은 다음과 같이 정의한다.

Gen : 블록암호E의 랜덤한 키 k를 생성한다.

Enc : 메시지 $M = m_1 m_2 \cdots m_n$에 대한 암호문 $C = c_1 c_2 \cdots c_n$이면

$c_i = Enc(k, m_i \oplus c_{i-1}) \oplus m_{i-1}$ 이다.
이 때, 초기 값인 c_0, m_0은 두 번째 랜덤한 키 k_0를 이용하여 계산$c_0 = Enc(k_0, m_0)$하거나, 임의로 선택할 수 있다.

Dec : 암호문 $C = c_1 c_2 \cdots c_n$과 k가 주어졌을 때, 복호화하면 $M = m_1 m_2 \cdots m_n$이 되고, $m_i = Dec(k, c_i \oplus m_{i-1}) \oplus c_{i-1}$으로 계산한다.



[그림1] IGE모드의 암호화 및 복호화

2.3 IND-CPA

대칭키 암호 알고리즘 Π=(Gen,Enc,Dec)는, 아래의 게임에서 다항식 시간의 공격자가 랜덤 추측(guess)보다 무시할만한(negligible) 이점(advantage)을 가질 때 IND-CPA 안전하다고 한다.

키생성 : 질의자가 랜덤 키 $k \leftarrow$Gen() 와 랜덤 비트 b를 생성한다.

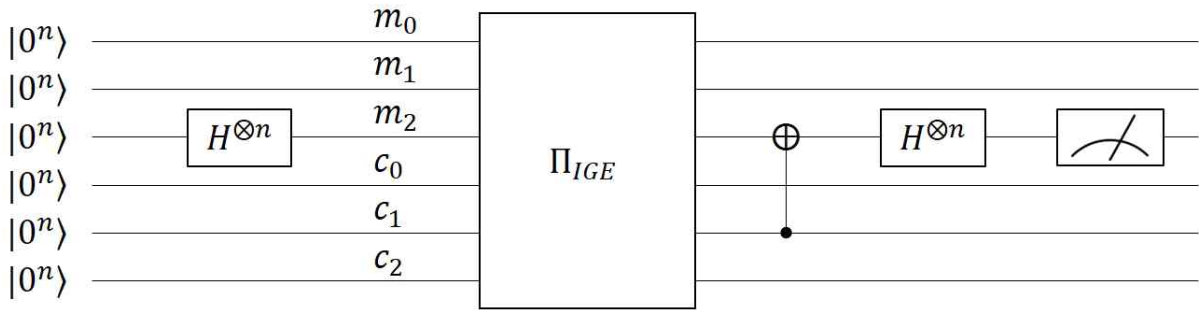
질의 : 공격자 A가 두 개의 메시지 m_0, m_1을 선택하고, 이를 질의자에게 보낸다. 질의자는 메시지를 암호화 $c^* = Enc_k(m_b)$ 하고, 이를 공격자에게 보낸다.

추측 : 공격자가 b'을 생성하고, $b = b'$일 때 공격자가 승리한다.

2.4 IND-qCPA[3]

IND-qCPA는 종래의 IND-CPA와 키생성, 추측 과정은 동일하나, IND-qCPA에서 질의 과정은, 양자 챌린지 질의와 양자 암호화 질의로 구분된다.

챌린지 질의 : 공격자 A가 두 개의 메시지 m_0, m_1를 질의자에게 제시하고, 질의자는 그 중 임의로 하나를 선택하여 암호문$c^* = Enc_k(m_b)$을 공격자에게 알려주는 것으로 IND-CPA와 동일하다.



[그림 2] IGE 모드를 이용하는 블록 암호에 대한 양자 공격 회로

암호화 질의 : 공격자가 암호화 오라클에 질의를 할 때 메시지가 중첩된 상태로 질의를 하며, 중첩된 상태의 암호문을 받는다.

$$\sum_{m,c}\psi_{m,c}|m,c\rangle \rightarrow \sum_{m,c}\psi_{m,c}|m,c\oplus\ nc_k(m)\rangle$$

2.5 Standard-secure PRF(sPRF)[4]

종래의 질의를 하는 어떤 양자 공격자도 PRF와 truly random function을 잘 구별할 수 없을 때, PRF는 standard-secure PRF이다.

2.6 Quantum-secure PRF(qPRF)[4]

양자 질의를 하는 어떤 양자 공격자도 PRF와 truly random function을 잘 구별할 수 없을 때, PRF는 quantum-secure PRF이다.

III. sPRF를 사용한 IGE모드의 안전성

이 장에서는 블록암호가 sPRF로 증명이 되어도 IGE모드를 사용할 때 양자 공격에 안전(IND-qCPA)하지 않은 경우를 제시한다. 아래의 sPRF를 사용한 블록암호가 Simon 알고리즘[5]을 이용하면 완벽하게 키를 찾아낼 수 있다.

3.1 sPRF인 블록암호[6]

$$BC_k(x) := E_{(k)}(droplastbit(x\oplus(k\,\|\,1)\times lastbit(x)))\ \|\ t_{H(k)_2}(x\oplus(k\,\|\,1)\times lastbit(x))\oplus lastbit(x),$$
$$E:\{0,1\}^{n-1}\times\{0,1\}^{n-1}\rightarrow\{0,1\}^{n-1}\ standard\ \text{secure}\ PRF$$
$$t:\{0,1\}^n\times\{0,1\}^n\rightarrow\{0,1\}\ standard\ \text{secure}\ PRF$$
$$H:\{0,1\}^n\rightarrow\{0,1\}^n\times\{0,1\}^n\ random\ \text{oracle}$$
$$k\xleftarrow{\$}\{0,1\}^{n-1}$$

위 블록암호는 sPRF이지만 qPRF는 만족하지 않으며, $k\,\|\,1$)주기를 가지고 있다. 자세한 설명은 [6]을 참조한다.

3.2 IGE 모드를 사용한 블록암호 공격

Π_{GE} 가 위의 C를 사용한 암호일 때, IND-qCPA의 공격자는 Π_{IGE}에 양자 질의가 가능하다. 즉, 공격자는 모든 메시지를 중첩된 상태로 BC_k에 질의를 할 수 있다.

먼저 공격자가 메시지와 암호문이 저장될 양자 레지스터 M, C를 준비한다. 메시지를 중첩된 상태로 M에 저장하고, C에는 $|0^{3n}$ 으로 초기화 하여 저장한다.

다음으로 공격자는 Π_{IGE}에 암호화 질의를 하고, 상응하는 결과가 C 레지스터에 저장된다. 암호화 질의 과정은 [그림 2]에 표시되어 있으며, 아래와 같은 계산과정을 거친다.

메시지 레지스터가 Hadamard 게이트 통과 후 Π_{IGE}를 적용하면 정규화된 (normalized) 상태는 다음과 같다.

$$|M,C\rangle = \sum_{m_2}|m_0\rangle|0^n\ \ |m_2\rangle|c_0\rangle\ |BC_k(c_0)\oplus m_0\rangle|BC_k(BC_k(c_0)\oplus m_0\oplus m_2)\rangle$$

$y := BC_k(c_0)\oplus m_0$로 두면,

$\sum_{m_2}|m_0\rangle|0^n\rangle|m_2\rangle|c_0\rangle|y\rangle|BC_k(y\oplus m_2)\rangle$이고,

CNOT 게이트를 이용하여 c_1을 m_2에 XOR 하면 아래와 같이 식(1)을 얻을 수 있다.

$$\sum_{m_2}|m_0\rangle|0^n\rangle|m_2\oplus y\rangle|c_0\rangle|y\rangle|BC_k(y\oplus m_2)\rangle \quad \text{식(1)}$$

BC_k가 $(k\,\|\,1)$주기를 가지므로, 식(1)에 $BC_k(y\oplus m_2)=BC_k(y\oplus m_2\oplus(k\,\|\,1))$을 적용하여 정리하면 식(2)를 얻는다.

$$m_0 \ |0^n \ |m_2 \oplus y\rangle |c_0\rangle |y \ | \ C_k(y \oplus m_2 \oplus (k \| 1))\rangle$$

$$= \sum_{m_2} |m_0\rangle |0^n\rangle |m_2 \oplus y \oplus (k \| 1)\rangle \\ |c_0\rangle |y\rangle |BC_k(y \oplus m_2)\rangle \quad \text{식(2)}$$

$:= m \oplus y$일 때, 식(1)과 식(2)는 다음과 같이 표현된다.

$$\sum_{\gamma} |m_0\rangle |0^n\rangle |\gamma\rangle |c_0\rangle |y\rangle |BC_k(\gamma)\rangle \quad \text{식(3)}$$

$$\sum_{\gamma} |m_0\rangle |0^n\rangle |\gamma \oplus (k \| 1)\rangle |c_0\rangle |y\rangle |BC_k(\gamma)\rangle \quad \text{식(4)}$$

따라서 공격자는 다음과 같은 상태를 얻을 수 있다.

$$\sum_{\gamma} |m_0\rangle |0^n\rangle (|\gamma\rangle + |\gamma \oplus (k \| 1)\rangle) |c_0\rangle |y\rangle |BC_k(\gamma)\rangle$$

이 후, Hadamard 게이트를 통과하면,

$$\sum_{\gamma} \sum_{z} ((-1)^{\gamma \odot z} + (-1)^{\gamma \oplus (k \| 1) \odot z}) \\ |m_0\rangle |0^n\rangle |z\rangle |c_0\rangle |y\rangle |BC_k(\gamma)\rangle$$

$$= \sum_{\gamma} \sum_{z} (-1)^{\gamma \odot z} (1 + (-1)^{(k \| 1) \odot z}) \ (\odot \text{는 내적}) \\ |m_0\rangle |0^n\rangle |z\rangle |c_0\rangle |y\rangle |BC_k(\gamma)\rangle$$

최종적으로 공격자가 측정 시 $z \odot (k \| 1) = 0$을 만족하는 경우 벡터 z를 얻을 수 있고, 그렇지 않으면 값이 0으로 수렴한다. n개의 독립된 벡터 z_i를 얻을 때까지 위의 과정을 반복하면 Gaussian 소거법에 의해 비밀키 k를 복구할 수 있으며 Π_{GE}가 IND-qCPA를 만족하지 못함을 알 수 있다.

IV. 결론

양자 컴퓨터의 개발에 대비하여 양자 안전성에 대해 다양한 분야[7]에서 연구가 활발히 진행되고 있다.

본 논문에서는 텔레그램에서 사용되고 있는 IGE 모드의 IND-qCPA에 대해 알아보았다. IGE모드에 사용한 블록암호가 sPRF인 경우에는 안전하지 않음을 반례를 통해 제시하였으며, 제시된 블록암호를 사용할 경우 Simon 알고리즘을 이용하여 비밀키를 복원할 수 있음을 제시하였다.

추후 과제로는 IGE 모드가 sPRF인 블록암호를 사용할 경우 양자 안전성을 만족하진 못하지만, qPRF인 블록암호를 사용할 경우에 대한 양자 안전성 등이 요구된다.

[참고문헌]

[1] Peter W. Shor. "Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer." *SIAM Journal on Computing*, 26(5):1484 - 1509, October 1997.

[2] Carl M. Campbell. "Design and specication of cryptographic capabilities." *IEEE Communications Society Magazine*, 16(6):15-19, November 1978.

[3] Dan Boneh and Mark Zhandry. "Secure signatures and chosen ciphertext security in a quantum computing world." In *Proceedings of the 33rd Annual International Cryptology Conference (Crypto 2013)*, pages 361 - 379, Santa Barbara, CA, USA, August 2013.

[4] Mark Zhandry. "How to construct quantum random functions." In *Proceedings of the 53rd Annual Symposium on Foundations of Computer Science (FOCS 2012)*, pages 679 - 687, New Brunswick, NJ, USA, October 2012.

[5] Peter W. Shor. "Algorithms for quantum computation: Discrete logarithms and factoring." In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science (FOCS 1994)*, pages 124 - 134, Santa Fe, NM, USA, November 1994.

[6] Mayuresh V. Anand, Ehsan E. Targhi, Gelo N. Tabia, and Dominique Unruh. "Post-quantum security of the CBC, CFB, OFB, CTR, and XTS modes of operation." In *Proceedings of the 7th International Workshop on Post-Quantum Cryptography (PQCrypto 2016)*, pages 44 - 63, Fukuoka, Japan, February 2016.

[7] Dan Boneh and Mark Zhandry. "Quantum-secure message authentication codes." In *Proceedings of Annual International Conference on the Theory and Applications of Cryptographic Techniques*. Springer, Berlin, Heidelberg, 2013.