양자암호와 포스트 양자암호에 관한 연구[1)]

김승민, 임성희, 김소희, 김윤정
서울여자대학교 정보보호학과
e-mail:swukimseungmin@gmail.com

A Study on Quantum Cryptography and Post Quantum Cryptography

Seung-Min Kim, Sunghee Lim, So-Hee Kim, Yoonjeong Kim
Dept of Information Security, Seoul Women's University

요 약

최근 양자컴퓨터의 개발로 공개키 암호 방식이 풀릴 수 있어 양자암호에 대한 연구가 활발해 지고 있다. 본 논문에서는 지금까지 설명 된 양자암호의 개념과 양자키 분배 프로토콜에 대해 살펴보고, 더 나아가 양자암호 방식 이후의 포스트 양자암호 방식과 응용에 대해 살펴본다. 또한 화폐 위조 기술이 늘어나는 만큼 위조를 할 수 없는 양자 화폐에 대해 살펴본다. 이러한 양자암호에 대한 다방면의 연구는 기존의 공개키 암호 방식을 보완하거나 대체할 만한 강화되고 새로운 암호체계에 대한 연구의 좋은 시작이 될 것이다.

1. 서론

현재 사용되고 있는 암호체계로는 RSA공개키 방식이 대표적이다. R. Rivest, A. Shamir, L. Adleman이 개발한 RSA공개키 암호체계[1]는 송신자가 공개키를 이용해 메시지를 암호화 하고 수신자는 자신만이 알고 있는 비밀키를 이용해 평문화를 한다. 이 공개키 방식의 암호를 풀기 위해서는 소인수분해를 해야 하는데 아무리 성능 좋은 컴퓨터라도 큰 수의 소인수분해는 풀기 어려워 안전한 암호체계다. 그러나 1990년대 중반, 벨연구소의 응용수학자 Peter Shor가 소인수분해를 쉽게 할 수 있는 양자알고리즘을 개발했다[2], [3]. 이는 양자컴퓨터가 개발이 되면 지금의 공개키 방식의 암호체계가 도청 위협에 직면했다는 것이다. 이 문제에 대한 대안으로 1983년 처음 Stephen Wiesner가 제안한 양자암호[4], [5]가 있다. 양자암호란 빛의 양자 역학을 이용한 암호 체계이다. 이와 함께 Wiesner는 위조 불가능한 화폐인 양자 화폐[6]를 구상했다. 양자 얽힘이라는 양자 역학적 특성을 이용한 양자 화폐는 최근 위조화폐로 문제가 되고 있는 부분에 대해 최적의 대응책으로 여겨지고 있다.

본 논문에서는 양자암호와 포스트 양자암호를 다루고 BB84 프로토콜을 포함한 양자키 분배 프로토콜들에 대한 기존 연구 결과를 살펴본다. 그리고 양자 화폐에 대해 자세히 기술한 후 향후, 양자암호통신과 포스트 양자암호, 양자 화폐의 전망을 예측해 보고 이에 따른 연구 방향을 소개한다.

1) 이 논문은 미래창조과학부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원(IITP-2016-H8501-16-1018)과 2016년도 정부(미래창조과학부)의 재원으로 한국연구재단의 지원(No. NRF-2016R1A2B4011984)을 받아 수행된 연구임.

2. 양자암호(Quantum cryptography)

1983년 Stephen Wiesner가 제안한 양자암호[5]란 양자역학의 불확정성 원리를 이용한 암호 체계이다. 양자암호의 단위는 일반적인 암호와 달리 '비트'가 아니라 '큐비트'이다. 0, 1로 정해지는 비트랑 다르게 0인지 1인지 결정할 수 없는 양자중첩된 상태다. 이러한 불확정성 원리의 성질 때문에 외부에서 도청을 시도하면 양자 상태가 하나하나 변하기 때문에 도청 사실을 알 수 있다. 즉, 양자의 상태가 0인지 1인지 모르는 상태에서 외부에서 양자를 건드리면 양자의 상태가 0과 1중 하나의 상태로 고정 된다. 이 불확정성 원리로 인한 복제 불가능한 성질을 양자 복제불가능성[7] 이라고도 하는데, 위 성질 때문에 양자를 오류 없이 정확히 측정하여 복제하는 것은 불가능 하다. 그러므로 양자암호를 안전한 암호체계라고 할 수 있다.

2.1 양자키 분배(Quantum Key Distribution, QKD)

RSA와 같은 고전 암호 프로토콜들을 보면, 키를 안전한 방법으로 나눠 갖고, 안전한 네트워크를 통해 통신한다. 양자의 세계에서도 역시 마찬가지이다. 따라서 안전한 키 교환 방법이 필요하고, 양자암호에서 역시 안전한 양자키 교환방법이 필요하다.

양자적인 방법으로 암호키를 배분하는 경우, 기밀성을 보장하는 것은 양자역학의 관측이론 때문이다. 양자비트는

도청자에게 도청될 수 없도록 되어있으며, 설령 도청이 가능하더라도 복제가 불가능하다. 이를 non-cloning theorem 이라 한다. 임의의 유니터리 연산을 이용하여 양자비트 $|\psi>$를 표적비트 $|s>$에 복사한다고 가정할 때, 다른 양자비트 $|\varnothing>$에 대해서도 적용하면 다음과 같다[8].

$$|\psi> \otimes |s>$$

$$U(|\psi> \otimes |s>) = |\psi> \otimes |\psi>$$

$$U(|\varnothing\rangle \otimes |s>) = |\varnothing\rangle \otimes |\varnothing\rangle$$

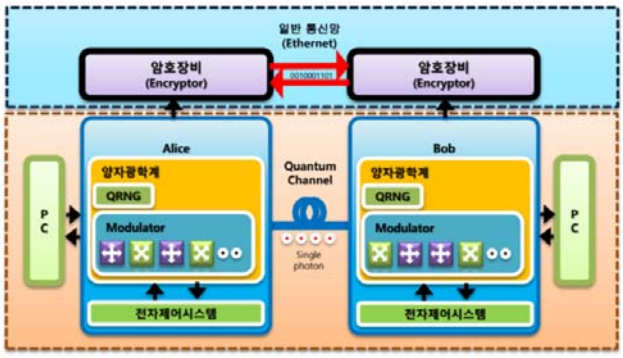
두 식의 내적을 구하면

$$<s| \otimes <\varnothing| U^{-1} U |\psi> \otimes |s> = <\varnothing|\psi> \quad [좌변]$$

$$<\varnothing| \otimes <\varnothing| \psi> \otimes |\psi> = \langle \varnothing|\psi\rangle^2 \quad [우변]$$

$$\langle \varnothing|\psi\rangle = \langle \varnothing|\psi\rangle^2$$

$\langle \varnothing|\psi\rangle = 1$ or 0 일 때에만 복제가 가능하다. 일반적으로 양자는 $0 < |\langle \varnothing|\psi\rangle| = |c^* a + d^* b| < 1$ 인 상태로 존재하므로 양자비트는 복제가 불가능하다.



<그림 1> 양자채널과 public채널을 이용하는 전체 흐름도[2]

2.2 BB84 프로토콜[5]과 다양한 프로토콜

이러한 안전한 양자키 분배를 위해 1984년 Bennet과 Brassard가 처음으로 BB84 프로토콜을 제시했다. 먼저 BB84프로토콜은 2가지의 편광필터(✣,⊠)와 4가지의 편광($|\leftrightarrow\rangle$, $|\updownarrow\rangle$, $|\nwarrow\rangle$, $|\nearrow\rangle$)을 사용한다. 앨리스(Alice)와 밥(Bob)이 양자키를 나누어갖고 이를 이용해 통신을 하고자 한다. 먼저 앨리스는 두 종류의 편광필터를 무작위로 선택하여 $4n$ 비트데이터의 광자를 송신하고, 밥도 두 종류의 편광검출기를 무작위로 사용하여 편광방향을 관측한다. 이때, 앨리스와 밥은 양자채널을 통해 통신하며, 비트가 0일 때 90° 또는 45°의 편광을, 1일 때 0° 또는 135°의 편광을 보낸다. 이어서 후처리로, 앨리스와 밥은 0 또는 1의 비트 상태는 공개하지 않은 채로 각자의 편광필터의 배열순서만 고전(public)채널로 주고받는다. 앨리스와 밥의 편광상태가 일치하지 않는 경우를 모두 제거하여 일치하는 경우만을 남긴다. 편광필터와 편광검출기가 일치하는 확률은 1/2이므로 동일한 $2n$개의 비트를 공유가능하다. 이중 편광상태가 같은 n개의 비트를 무작위로 추출하여 고전채널로 주고받는다. 중간에 도청자가 도청을 하지 않았다면 앨리스와 밥이 주고받은 비트가 n개로 모두 동일해야한다. 이 n개의 비트를 one-time-pad로 사용하면 된다. 만약 도달하는 양자의 개수가 달리지게 되었다면 도청을 의심하면 된다.

그 외 2-state 프로토콜[9]과 6-state 프로토콜, EPR 프로토콜 등이 소개되었다[10]. 2-state 프로토콜은 기존의 4가지의 편광($|\leftrightarrow\rangle$, $|\updownarrow\rangle$, $|\nwarrow\rangle$, $|\nearrow\rangle$)필터를 이용해 새로운 두 개의 state를 만든 후(p_0, p_1) 이를 이용해 양자키 분배를 하는 프로토콜이다[9].

3. 포스트 양자암호(Post Quantum Cryptography)

현재의 암호 기술, 특히 공개키 기반 알고리즘들은 수학적인 난제들에 기반을 하고 있다. 그러나 양자컴퓨터의 등장과 함께 나타난 새로운 양자 알고리즘들로 인해 더 이상 현재의 암호기술들은 안전할 수 없게 되었다. 그 중 하나가 1994년에 발표된 Shor의 알고리즘이다[3]. Shor의 알고리즘으로 인해 이산로그, 소인수분해 문제가 쉽게 계산이 가능하다. 이의 대안으로 미국 및 유럽에서 활발하게 연구되고 있는 것 중 하나가 포스트 양자암호(Post Quantum Cryptography)이다. 포스트 양자암호는 다변수다항식, 부호, 격자, 해쉬에 기반을 둔 수학적 문제들에 기초하며 안전성을 말하고 있다. 그러나 이들 역시 각각 장단점이 존재하고, 개선의 여지가 있다. 현재 ECC(Elliptic Curve Cryptosystem)나 RSA는 안전성 증명에 대해 잘 나와 있는 반면, 포스트 양자암호는 그 안전성에 대해 연구가 많이 부족한 상태이다. 포스트 양자암호는 RSA와 속도면에서 유사하지만 공개키, 서명, 암호문의 파라미터들의 크기가 훨씬 크다는 단점을 가지고 있다. 각 기반 포스트 양자암호의 기반에 대해 알아보고 장단점을 알아보며 기반의 역사를 살펴보자[11].

다변수 다항식 기반 문제는 MQ문제(Multivariate Quadratic solve)에 기반을 하고 있다. One way function 구성은 쉽게 가능하나 암호체계에 적용하기 위해선 사용자가 역상을 구할 수 있어야한다. 역상을 구하기 쉽게 설계된 구조의 트랙도어를 사용하는데, 공격자 역시 역상을 구하기 쉬워지므로 1차함수를 앞뒤로 사용해 2차식의 구조를 숨김으로서 내부 구조를 랜덤해 보이도록 감춘다. 장점으로는 one way function의 결과물이 몇 개의 유한체의 원소로 이루어져있으므로 암호문의 크기가 매우 작고, 단순 다항식 계산으로 속도가 빠르다. 단점으로는 랜덤한 다항식의 모든 계수를 제시해서 공개키를 이루므로 공개키의 크기가 매우 크다.

부호기반 암호는 오류정정부호에 기반을 두고 있다. Random linear code를 만들어 노이즈가 섞였을 때 이를 수신자가 디코딩하는 것을 NP hard에 기초한다. 효율적인 디코딩 알고리즘이 주어진 코드를 이용해 출발점에는 코드를 뒤섞어서 내부를 알고 있는 사용자는 알 수 있지만 내

부를 모르는 공격자는 복호화가 불가능 한 것이다. 속도가 빠른 장점과 공개키 크기가 굉장히 크다는 단점을 가졌다.

격자기반 암호는 초기 SVP나 CVP등의 격자기반문제에 기반 했다. SVP는 기저를 통해 공개키를 주고받을 때 격자 상에서 최단길이의 벡터를 찾아내는 문제이며, CVP는 격자 밖 벡터로부터 가장 가까운 격자원소를 찾는 문제이다. 이들은 매우 어려운 문제였지만 암호화나 서명으로 쓰기에는 효율성이 낮았다. 그러다 2005년 암호체계에서 쓰기 용이한 LWE문제가 제시 되었다. 기존의 격자기반 문제만큼 어렵다는 것이 증명되었지만 행렬을 공개키에 적용해야 했기 때문에 크기가 너무 컸다. 이후, 2010년 Peikert에 의해 행렬대신 다항식을 사용하는 RLWE가 제시되었다. 2015년에 Joppe W. Bos외 3명이 RLWE 키교환을 사용하는 TLS cipher suite을 만들었고 openssl로 소프트웨어 구현으로 기존의 ECDH기반 TLS cipher suite과 성능을 비교하였다. 공개키 크기와 암호문의 크기가 여전히 크지만 합리적인 수준으로 내려왔다. 암·복호화 속도가 매우 빠르며 보안모델을 통해 안전성 증명이 잘 나타나 있다[12]. 그 외에 Alkim, Ducas, Pöppelmann, Schwabe에 의해 RLWE와 함께 BCNS의 여러 측면을 개선하여 New Hope 키 교환 프로토콜을 구현하였다[13]. 속도는 ECC를 이용한 Diffie hellman 키교환을 사용했을 때보다 비슷한 정도이며, 정도의 안전성을 보장한다. New Hope의 구현으로 최근 구글이 시험용 크롬에서 시연을 한 적이 있다.

해쉬 기반 암호는 안전한 해쉬 함수를 만들면 충돌 쌍을 찾음이 어렵다는 것이 기반을 둔다. 위 3개의 기반 암호체계와는 다르게 수학적 난제에 기반하고 있지 않다. 장점으로는 속도가 매우 빠르며, 공개키 크기를 작게 만들 수 있다. 단점으로는 공개키 암호화 방식을 만들기 어렵다는 것에 있다.

4. 양자 화폐(Quantum Money)

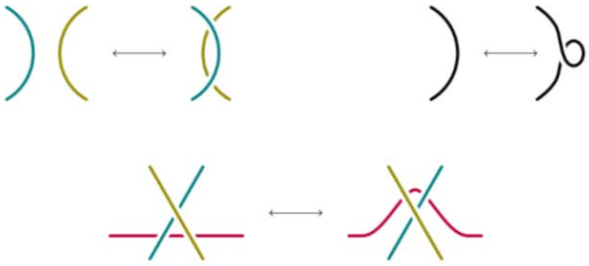
나날이 화폐를 위조하는 기술이 발전해 가고 있다. 또한 전자 금융거래에서 정보를 위조하거나 도청하는 일도 빈번해 지고 있다. 오프라인이던 온라인이던 개인정보가 중요해진 시대에 이러한 화폐 위조나 전자 금융거래 해킹은 매우 위험하다. 이에 대한 대안으로는 1983년 Wiesner가 양자암호와 함께 제안한 양자 화폐(Quantum money)이다[4].

양자 화폐는 발행처가 각 화폐마다 고유 번호를 붙이고 그에 대응하는 정보를 발행처에 저장해 놓고 양자 화폐를 증명할 때 사용한다. 이후 1982년, Bennett과 Brassard가 처음으로 Wiesner 가 제시한 양자 화폐에 대한 연구를 시도했다. 그러나 Bennett 등이 제안한 양자 화폐는 발행처 외부의 사람은 절대 위조를 하지 못한다는 강력함이 있지만, 거래하는 사람들은 거래 시 은행과 화폐 대조를 해야 하므로 이는 신용카드보다 약한 화폐가 되었다. Wiesner의 양자 화폐는 은행만이 고유의 키를 갖고 있으므로 개인키 양자 화폐(priviate-key quantum money)라고도 불렸다[14]. 그 후 2009년 처음으로 Aaronson[15]이 양자 오라클[16]이 사용되는 공개키 양자 화폐(public-key quantum money)와 양자 오라클이 사용되지 않는 공개키 양자 화폐를 제안했으나 금방 취약점이 보였다. 그래서 많은 저자들이 붕괴되지 않을 공개키 양자 화폐에 대한 연구를 발표했다. 2010년 Farhi 등[17]이 knot를 기반한 양자 화폐를 제안했다(<그림 2>). 이는 양자 오라클을 필요로 하지 않고 발행처와 증명을 할 필요가 없는 양자 화폐 방식이다. Knot란 3차원 상에서의 원을 표현한 것이다. Knot를 이용한 양자 화폐는 라이데마이스터 변형(<그림 3>)이라는 선

<그림 2> knots 에서의 양자 화폐[17]

다이어그램의 중첩을 이용한 양자 화폐방식이다. 이는 어떻게 중첩이 되더라도 같은 knot이기 때문에 한 knot로도 다양한 중첩을 이뤄낼 수 있다. 또한 첫 knot의 불변성은 Alexander 다항식(polynomial)이라고 불린다. 따라서 발행처는 이 방식으로 양자 화폐를 만들기 위해서 다양하게 중첩되는 모든 다이어그램을 준비해야 하고, Alexander 다항식의 계수를 측정해야 한다. 그리고 거래하는 상인들은 라이데마이스터 변형으로 불변하는 knot의 중첩을 증명하고 Alexander 다항식의 계수를 측정해야 한다. 따라서 이 방식은 아직 어떠한 위조 방식을 찾지 못했다. 이후 2012년에는 Gavinsky[18] 의 고전적인 증명을 기반으로 한 양자 화폐와 Aaranson 등[19]의 공간벡터의 숨겨진 부분공간을 기반으로 한 양자 화폐에 대해 제안되었다.

최근에 양자컴퓨터를 비롯한 양자기계의 실현이 다가오고 있다[20]. 따라서 [3]에서와 같이 전자금융 거래 시 여러 단계를 거칠 필요 없이 자신의 양자컴퓨터 및 휴대기기를 통해 양자 화폐를 발행받아 금융거래 및 전자상거래를 하는 시대가 올 것이라 생각한다.



<그림 3> 방향이 없는 선형 다이어그램의 라이데마이스터 변형[17]

5. 결론 및 연구 방향

본 논문에서는 양자암호와 BB84 프로토콜을 포함한 양자키분배 프로토콜들, 포스트 양자암호, 양자 화폐에 대한 전반적인 내용을 살펴보고 이에 대한 전망을 생각해 보았

다. 앞으로 BB84프로토콜뿐만 아니라 그 이후에 나온 양자키분배 프로토콜에 대해 자세히 살펴보고 현재 암호체계에 대한 대안으로 양자키분배 방식을 어떻게 적용시킬 수 있는지에 대한 연구를 진행할 예정이다. 그리고 포스트 양자암호 중 격자암호 이용에 대한 심층적인 연구를 통해, 현재 암호체계의 대안으로 양자암호 외에 다양하면서 안전한 암호 체계가 있음을 알고 실용화 할 수 있는지에 대한 연구를 진행할 예정이다. 또한 양자컴퓨터의 발전함에 따라 기존의 화폐의 위조의 위험성에 대해 살펴보고 양자 화폐를 실제로 적용할 수 있는지에 대한 연구를 계속 진행할 예정이다.

참고문헌

[1] R. Rivest, A. Shamir, L. Adleman, “A Method for Obtaining Digital Signature and Public-Key Cryptosystems”, Communications of the ACM, 1978

[2] 한상욱, “QKD 프로토콜 및 시스템 개요”, 제 1회 양자통신 및 양자컴퓨터 기초 단기강좌, 한국통신학회 양자통신연구회, 2016

[3] Peter W. Shor, “Algorithms for Quantum Computation: Discrete Logarithms and Factoring”, 35th Annual Symposium on Foundations of Computer Science, 1994

[4] Stephen Wiesner, “Conjugate coding”, ACM Sigact News, 1983

[5] Charles H. Bennett, Gilles Brassard, “Quantum cryptography : Public key distribution and coin tossing”, International Conference on Computer System and Signal Processing, IEEE, 1984

[6] Charles H. Bennett, Gilles Brassard, Seth Breidbart, Stephen Wiesner, “Quantum Cryptography, or Unforgeable Subway Tokens”, Advances in Cryptology, 1983

[7] 김재완, “양자암호”, 네이버 캐스트 http://navercast.naver.com/contents.nhn?rid=20&contents_id=6439

[8] 좌천홍신, 길전선장, *양자정보이론*, 청범출판사, 2008

[9] Charles H.Bennett, “Quantum Cryptography Using Any Two Nonorthogonal States”, Physical Review Letter, 1992

[10] Nicolas Gisin, Gr´egoire Ribordy, Wolfgang Tittel and Hugo Zbinden, “Quantum Cryptography”, Reviews of modern physics 74.1 (2002): 145.

[11] 윤아람, “양자 알고리즘 및 현대 암호 안전성 분석에 관한 연구”, 2016년 암호연구회 제2차 워크샵, 2016년 9월

[12] Joppe W. Bos, Craig Costello, Michael Naehrig, Douglas Stebila, “Post-quantum key exchange for the TLS protocol from the ring learning with errors problem”, IEEE security and privacy, 2015

[13] Erdem Alkim, Léo Ducas, Thomas Pöppelmann, Peter Schwabe, “Post-quantum key exchange - a new hope”, Cryptology ePrint Archive, Report 2015/1092, 2015. http://eprint. iacr. org, 2015.

[14] Scott Aaronson, Edward Farhi, David Gosset, Avinatan Hassidim, Jonathan Kelner, Andrew Lutomirski, “Quantum money”, Communications of the ACM, 2012

[15] Scott Aaronson, “Quantum copy-protection and quantum money”, 24th Annual IEEE Conference on Computational Complexity, 2009

[16] Mihir Bellare, Phillip Rogaway, “Random oracles are practical: A paradigm for designing efficient protocols”, Proceedings of the 1st ACM conference on Computer and communications security, 1993

[17] Edward Farhi, David Gosset, Avinatan Hassidim, Andrew Lutomirski, Peter Shor, “Quantum money from knots”, 3rd Innovations in Theoretical Computer Science Conference, 2012

[18] Dmitry Gavinsky, “Quantum money with classical verification”, 27th Annual IEEE Conference on Computational Complexity, 2012

[19] Scott Aaronson, Paul Christiano, “Quantum money based on hidden subspaces“, 44th annual ACM symposium on Theory of computing, 2012

[20] 방은주, “구글 ‘양자컴퓨터 드림 실현 멀지 않았다’”, 전자신문 2016년 9월 5일 기사, http://www.etnews.com/20160905000480