텍스트, 폰트, 스크린샷, 대수학이(가) 표시된 사진

AI가 생성한 콘텐츠는 부정확할 수 있습니다.

**초록**

본 연구에서는 one-way functions를 기반으로 한 quantum public-key encryption(QPKE) 방식을 제안한다. 제안된 구성에서는 public key는 quantum 상태이며, ciphertext는 classical 상태이다.

이와 유사하게, one-way functions 또는 pseudorandom function-like states와 같은 더 약한 primitive를 기반으로 한 QPKE는 [Morimae–Yamakawa, eprint:2022/1336], [Coladangelo, eprint:2023/282], [Barooti–Grilo–Malavolta–Sattath–Vu–Walter, TCC 2023] 등의 최근 연구에서도 제안된 바 있다. 그러나 이들 방식은 중요한 한계를 가진다. 바로, quantum public key가 encryption을 수행하는 송신자에게 adversary에 의해 tamper되지 않은 상태로 전달될 수 있어야만 security가 보장된다는 점이다. 이는 secure quantum channels과 같은 비현실적인 물리적 가정을 필요로 하므로, 일반적인 공개키 암호의 목적과는 거리가 있다. 본 논문에서 제안하는 방식은 이러한 제약에서 자유롭다. 구체적으로는, unauthenticated quantum channels만을 가정하더라도 암호화된 메시지의 secrecy가 보장되며, encryption은 adversary가 tamper한 quantum public key를 사용하더라도 안전하다. 이는 one-way functions만을 기반으로, insecure한 채널 상에서 secure한 통신을 실현한다는 classical public-key encryption의 목표를 quantum 환경에서 처음으로 달성한 구성이다. 또한, 본 연구에서는 \*\*CPA(Chosen Plaintext Attack)\*\*에 대한 security를 CCA(Chosen Ciphertext Attack) security로 향상시킬 수 있는 generic compiler를 제안한다. 이 컴파일러 또한 one-way functions만을 기반으로 구현 가능하다. 결과적으로, 본 연구는 one-way functions만을 기반으로 하는 CCA-secure QPKE를 달성한다는 점에서 이론적·실용적 의의를 갖는다.

**1 Introduction**

**1.1 Background**

Quantum physics는 암호학에서 여러 가지 이점을 제공한다. 예를 들어, classical cryptography에서는 불가능한 statistically-secure key exchange가 quantum state가 전송될 경우 가능해진다 [BB84].

또한, oblivious transfer와 multiparty computation은 quantum 세계에서 one-way function (OWF)로부터만 가능하다 [BCKM21, GLSV21]. 이러한 cryptographic primitive들은 classical cryptography에서는 더 강력한 구조적 가정을 필요로 하는 것으로 여겨진다 [IR89, GKM+00].

더 나아가, (non-interactive) commitment, digital signature, secret-key encryption, quantum money, multiparty computation과 같은 여러 cryptographic task들이 다음과 같은 새로운 primitive들에 기반하여 가능함이 입증되었다: pseudorandom states generator, pseudorandom function-like states generator, one-way states generator, 그리고 EFI. 이 primitive들은 OWF보다 약한 것으로 보인다 [JLS18, Kre21, MY22b, AQY22, BCQ23, AGQY22, CX22, MY22a, KQST23].

**OWF로부터의 quantum public key encryption.**

이러한 여러 발전에도 불구하고, quantum 세계에서 오직 one-way function (또는 그보다 약한 위 primitive들)만으로 public-key encryption (PKE)이 가능한지는 여전히 미해결 문제이다. OWF로부터의 PKE는 classical cryptography에서는 black-box 방식으로는 불가능하다 [IR90].그러나 quantum state가 전송되거나, 연산이 local하면서 quantum인 경우에는 가능할 수도 있다. 실제로, 최근의 몇몇 연구들 [MY22a, Col23, BGH+23a]은 OWF 또는 pseudorandom function-like states generator에 기반하여 quantum public key를 사용하는 quantum PKE(QPKE)를 독립적으로 구성하였다. 하지만, 이러한 연구들에서 제안된 구성 방식에는 아래에서 설명할 중대한 결점이 있으며, 따라서 “QPKE from OWFs” 문제에 대한 만족스러운 해법은 아직 존재하지 않는다.

**Quantum public key를 어떻게 인증할 것인가?**

우리가 public key 암호학적 primitive를 연구할 때는, public key를 어떻게 인증할 것인가, 즉 메시지를 암호화하는 송신자가 주어진 public key가 유효하며, 그 아래에서 암호화된 메시지의 기밀성이 보장되는지를 어떻게 확인할 수 있는지를 고려해야 한다.Public key가 classical string인 경우, digital signature scheme을 사용하여 쉽게 인증할 수 있다. 그러나 public key가 quantum state인 경우에는 일반적으로 이러한 목적을 달성하기 위해 digital signature scheme을 사용할 수 없으며, 이를 어떻게 인증할 수 있을지는 불분명하다.

앞서 언급했듯이, 최근의 몇몇 연구들 [MY22a, Col23, BGH+23a]은 OWF 또는 그보다 약한 가정에서 quantum public key를 사용하는 QPKE를 실현하였다. 그러나 이들 연구에서는 quantum public key 인증 문제를 충분히 다루지 않았다. 실제로 우리가 이해하는 바에 따르면, 이러한 연구들에서 제안된 primitive들을 의미 있게 사용하기 위해서는 quantum public key를 송신자에게 손상되지 않은 채로 전달하기 위한 secure quantum channel을 사용해야 한다.

이는 PKE의 목표가 secure channel을 가정하지 않고 메시지를 전달하는 것임을 고려할 때, 중대한 결점이다. 만약 송신자가 secure channel을 통해 quantum public key를 받을 수 있다면, 처음부터 해당 채널을 이용해 메시지를 전달할 수 있기 때문에, PKE scheme을 사용할 이점이 없어진다.

**1.2 Our Result**

우리는 위 질문에 대해 긍정적인 해답을 제시한다. 우리는 오직 OWF에만 기반하여, classical PKE의 목표인 불완전한 채널 위에서의 안전한 통신을 달성하는 최초의 QPKE scheme을 실현한다. 우리는 인증되지 않은 quantum channel과 인증된 classical channel이 사용 가능한 위와 같은 설정에서 사용할 수 있는 QPKE의 개념을 정의한다. 그런 다음, 우리는 OWF로부터 그 정의를 만족하는 구성 방법들을 제안한다. 아래에서는 각 결과를 상세히 기술한다.

**정의 관련 작업.** 우리는 QPKE의 구문(syntax)을 새롭게 정의한다. 기존 정의와의 차이점은 키 생성 알고리즘이 secret key와 함께 하나의 classical verification key를 출력한다는 점이다. 또한, 이 verification key는 encryption 알고리즘에 quantum public key 및 메시지와 함께 제공되며, encryption 알고리즘은 주어진 quantum public key의 유효성을 이 verification key를 이용해 검사할 수 있어야 한다. 우리는 ciphertext가 classical이어야 함을 요구한다. 우리는 QPKE scheme이 다음의 두 가지 기본적인 보안 개념을 만족할 것을 요구한다.

• **Indistinguishability against public key tempering chosen plaintext attacks**

**(IND-pkT-CPA security).**

이는 대략적으로 말해, adversary가 변조한 public key로 메시지를 암호화하더라도, 암호문 간의 구별이 불가능함을 보장한다. 좀 더 구체적으로는, verification key vk가 주어지고, adversary가 올바르게 생성된 quantum public key의 복수 개 사본을 갖는 상황에서, adversary가 (pk’, msg\_0, msg\_1)를 생성하고, Enc(vk, pk’, msg\_b)가 주어졌을 때, 효율적인 adversary는 challenge bit b를 무작위 추측보다 유의미하게 더 높은 확률로 맞출 수 없어야 한다. IND-pkT-CPA security는 classical verification key가 classical authenticated channel을 통해 전달되는 설정을 반영한다. 따라서 모든 참여자가 올바른 verification key를 얻을 수 있다. 반면, quantum public key는 인증되지 않은 quantum channel을 통해 전달되므로 adversary에 의해 변조될 수 있다.

**• Decryption error detectability.**

우리의 설정에서는 adversary가 quantum public key를 변조하여 복호화 오류를 유도할 수 있다. 이 문제를 해결하기 위해 우리는 decryption error detectability라는 새로운 보안 개념을 도입한다. 이는 대략적으로, ciphertext의 정당한 수신자는 복호화된 메시지가 송신자가 의도한 메시지와 다를 경우 이를 인지할 수 있어야 함을 보장한다.

IND-pkT-CPA security는 quantum public key를 변조할 수는 있지만 ciphertext는 수동적으로 관찰만 하는 adversary를 고려한다. classical PKE의 경우, 보안의 황금 기준은 IND-CCA security로, 이는 adversary가 임의의 (잘못 형성된 것일 수도 있는) ciphertext에 대한 복호화 결과를 볼 수 있는 능동적 adversary를 고려한다. 따라서 우리는 QPKE에 대해서도 이에 상응하는 보안 개념을 정의한다. Section 1.3에서는 이러한 보안 개념이 자연스러운 응용 시나리오에서 왜 중요한지를 논의한다.

**• Indistinguishability against public key tempering chosen ciphertext attacks**

**(IND-pkT-CCA security).**

이 개념은 IND-pkT-CPA security와 유사하지만, adversary가 challenge ciphertext를 제외한 임의의 ciphertext에 대해 복호화 결과를 반환하는 decryption oracle에 접근할 수 있다는 점에서 다르다. 추가로, adversary는 challenge ciphertext가 \perp로 복호화되는지를 나타내는 1비트 정보를 얻을 수 있도록 허용된다. 이는 classical PKE에서는 중복된 정보이다. 왜냐하면 decryption correctness에 의해 challenge ciphertext는 항상 challenge message로 복호화되며, 이는 \perp가 아니기 때문이다. 반면, QPKE의 경우 adversary가 challenge ciphertext를 생성하는 데 사용된 public key를 변조한 경우, decryption correctness가 더 이상 보장되지 않을 수 있으므로, 이 1비트 정보가 adversary에게 더 많은 능력을 제공할 수 있다.

**IND-pkT-CPA 보안을 만족하는 OWF 기반의 구성.**

우리는 OWF로부터 구성 가능한 digital signature scheme에 기반하여 IND-pkT-CPA security를 만족하는 QPKE scheme을 제안한다. 우리의 구성은 Aaronson, Atia, Susskind [AAS20]에 의해 제시된 distinguishing과 swapping 간의 duality, 그리고 Hhan, Morimae, Yamakawa [HMY23]에 의한 그 암호학적 응용에서 영감을 얻었다. 제안하는 구성은 quantum public key와 classical ciphertext를 갖는다. 또한 우리는 decryption error detectability를 추가하는 일반적인 변환 기법도 제안하며, 이 변환은 digital signature scheme만을 사용한다.

**IND-pkT-CCA 보안으로의 업그레이드.**

우리는 IND-pkT-CPA 보안을 IND-pkT-CCA 보안으로 업그레이드하면서도 decryption error detectability를 유지하는 일반적인 compiler를 제안하며, 이는 오직 OWF만을 사용한다. 이러한 CPA에서 CCA로의 일반적인 compiler를 구성하는 것은 classical PKE에 있어서 오랜 미해결 문제임을 언급할 가치가 있으며, 따라서 우리는 이 compiler를 구성하는 데에 public key가 quantum이라는 사실을 결정적으로 활용한다. 우리가 제안한 IND-pkT-CPA secure한 구성을 이 compiler에 적용함으로써, 우리는 OWF에만 기반하면서 IND-pkT-CCA security와 decryption error detectability를 만족하는 QPKE scheme을 얻는다.

**재활용 가능한 변형.**

앞서 정의한 QPKE는 각 quantum public key가 오직 하나의 메시지를 암호화하는 데 사용되며, 이후 소모될 수 있다고 가정한다. 이에 우리는 quantum public key가 주어졌을 때, encryption 알고리즘이 ciphertext와 함께 메시지를 여러 번 암호화하는 데 사용할 수 있는 classical 상태를 출력하는 recyclable QPKE 개념을 도입한다. 그리고 우리는 classical ciphertext를 가지는 어떤 표준적인 IND-pkT-CPA (또는 IND-pkT-CCA) 보안 QPKE scheme도, decryption error detectability를 유지하면서 IND-pkT-CPA (또는 IND-pkT-CCA) 보안을 만족하는 recyclable QPKE로 변환될 수 있음을 보인다. 이 변환은 OWF로부터 구성 가능한 CPA (또는 CCA) 보안의 classical symmetric key encryption scheme만을 사용한다. 따라서 이 변환을 앞서 제시한 결과들과 결합함으로써, 우리는 OWF에 기반한 decryption error detectability를 만족하는 recyclable IND-pkT-CCA QPKE scheme을 얻는다.

**1.3 Discussion**

**Pure State Public Keys VS Mixed State Public Keys.**

우리가 제안하는 QPKE scheme의 quantum public key는 mixed state이다. 최근의 몇몇 연구들 [Col23, BGH+23a]에서는 QPKE의 quantum public key가 순수한 quantum state일 것을 명시적으로 요구한다. 그 이유는 이 논문의 주요 관심사인 quantum public key certification 문제와 관련이 있다. Barooti 등 [BGH+23a]은, 주어진 quantum public key가 pure state일 경우에는 송신자가 SWAP test를 통해 그 유효성을 검사할 수 있지만, mixed state일 경우에는 불가능하다고 주장하였다. 그러나 우리가 이해한 바에 따르면, 이 주장은 최소한 하나의 손상되지 않은 quantum public key가 adversary가 전혀 개입할 수 없는 secure quantum channel을 통해 전달되어야 한다는 암묵적인 전제를 포함한다. 이는 QPKE의 가치를 저해하는 바람직하지 않은 가정이다. [BGH+23a]에서 제안된 구성 방식에서, secure transmission 없이 주어진 quantum public key의 유효성을 송신자가 어떻게 확인할 수 있는지는 명확하지 않다.

우리는 quantum public key가 pure state인지 mixed state인지는 중요하지 않다고 본다. 진정으로 중요한 것은, 송신자가 quantum secure channel과 같은 바람직하지 않은 가정을 하지 않고도 주어진 quantum public key의 유효성을 확인할 수 있는가 하는 점이다. 우리가 제안한 QPKE scheme은 mixed state quantum public key를 사용하지만, 송신자가 어떠한 비현실적인 가정 없이도 quantum public key의 유효성을 확인할 수 있는 수단을 제공한다. 또한, 이 구성을 pure state quantum public key를 사용하는 방식으로 손쉽게 확장할 수 있으며, 해당 변형은 Appendix A에 제시한다.

**1.4 Related Works**

QPKE가 더 약한 가정으로부터 실현 가능하다는 가능성은 처음으로 Gottesman [Got]에 의해 제기되었으나, 그는 구체적인 구성은 제시하지 않았다. QPKE의 최초의 구체적인 구성은 Kawachi, Koshiba, Nishimura, Yamakami [KKNY05]에 의해 제안되었다. 이들은 quantum public key를 갖는 QPKE 개념을 형식적으로 정의하고, 두 quantum state를 구별하는 문제로부터 이를 만족하는 구성을 제시하였다. 최근에는 Morimae와 Yamakawa [MY22a]가, [KKNY05]에서 정의한 QPKE는 거의 자명하게 어떤 classical 또는 quantum symmetric key encryption으로부터도 실현될 수 있음을 지적하였다. 이 두 논문에서 제안된 구성은 모두 mixed state quantum public key를 사용한다. 이후, Coladangelo [Col23]와 Barooti 등 [BGH+23b]은 독립적으로 pure state quantum public key를 사용하는 QPKE가 OWF 혹은 그보다 약한 가정으로부터 구성 가능한지를 연구하였다.

위의 연구들에서 다룬 QPKE의 정의는 본질적으로 송신자가 손상되지 않은 quantum public key를 확보할 수 있다는 것을 전제로 한다. 우리가 이해한 바로는, 이는 secure quantum channel 또는 tamper-proof quantum hardware와 같은 바람직하지 않은 물리적 설정 가정을 필요로 하며, 이는 quantum public key가 pure state인지 mixed state인지와는 무관하다. 우리가 고려하는 자연스러운 설정에서는 adversary가 quantum public key가 전송되는 quantum channel에 개입할 수 있기 때문에, 단순히 해당 channel 위의 quantum public key를 자신이 생성한 것으로 교체함으로써 이전의 구성들에 대해 쉽게 공격할 수 있다. 이러한 adversarial한 행위를 고려하지 않는다면, 송신자가 손상되지 않은 quantum public key를 수신한다는 전제를 둬야 한다.

우리의 연구는 오직 classical authenticated channel만을 가정하고, 이는 classical PKE와 동일한 가정이며 digital signature scheme을 통해 구현 가능한, 이러한 자연스러운 설정 하에서 보안을 만족하는 QPKE scheme을 최초로 제안한 것이다. 기존의 구성들이 우리와 같이 classical authenticated channel만을 활용하여 동일한 문제를 해결할 수 있을지는 불분명하다. 아래에서는 최근 연구들에서 OWF로부터 제안된 QPKE 구성들을 검토한다.