情報保護學會論文誌
第14券 第2號, 2004. 4

인증된 양자 키 분배 프로토콜

이 화 연[a)†], 홍 창 호[a)], 이 덕 진[a)], 양 형 진[a),b)‡], 임 종 인[a)]
고려대학교 정보보호대학원[a)] 고려대학교 자연과학대학[b)]

Authenticated quantum key distribution protocol

Hwa-Yean Lee[a)†], Chang-ho Hong[a)], Dong-Hoon Lee[a)],
Hyung-jin Yang[a),b)‡], Jong-in Lim[a)]
Graduate School of Information Security(GSIS), Korea University[a)]
Department of Physics, Korea University[b)]

요 약

본 논문에서는 Greenberger-Horne-Zeilinger(GHZ) 상태를 이용하여 키 분배와 인증을 동시에 수행할 수 있는 인증된 양자 키 분배 프로토콜을 제안한다. 이 프로토콜에서 공유되는 키는 정직한 중재자에게는 노출되지 않으며 완전한 안전성이 보장된다. 제안된 양자 키 분배 프로토콜은 기존의 양자 키 분배 프로토콜이 지니는 안전성을 그대로 확보하면서 기존의 정보를 이용하여 상대방에 대한 신뢰를 추가로 제공한다는 장점을 가지며, 실험적으로도 기본적인 양자 연산만을 이용하기 때문에 쉽게 구현될 수 있을 것이다.

ABSTRACT

We propose a new authenticated quantum key distribution protocol. Using Greenberger-Horne-Zeilinger(GHZ) state, the users of our protocol can authenticate each other and share a secret key. In our protocol, the shared key is not revealed to the honest arbitrator, which provides the additional secrecy. Our protocol not only guarantees secrecy as the other quantum key distribution protocols, but also the users authenticates each other. In practice, our new protocol can be easily implemented because it only uses basic quantum operations.

Keywords: *GHZ, Quantum Key Distribution*

Ⅰ. 서 론

양자 암호라는 용어가 주로 양자 키 분배를 지칭하는 데에서 알 수 있듯이, 양자 키 분배 시스템은 양자 암호체계에서 가장 활발하게 연구되고 있으며 현실적으로 적용이 가능한 분야이다. 양자 키 분배 프로토콜은 1984년에 Bennett과 Brassard[1]에 의해 처음으로 제안되었으며, 이후 EPR[2], B92[3]와 같은 양자 키 분배 프로토콜[4]이 제안되었다. 1992년에 Bennett, Brassard 및 Mermin이 제안한 논문[5]에서 BB84 프로토콜과 EPR이 실질적으로 유사한 프로토콜이라는 것이 증명되어, 현재 BB84가 표준으로 널리 사용되고 있다.

양자 키 분배 프로토콜 분야의 연구는 안전성 분석[6,7,8]과 더불어 실험적 구현[9,10,11]이 활발하게 진

접수일: 2003년 12월 10일; 채택일: 2004년 3월 30일
* 본 연구는 정보통신부 대학 IT연구센터 육성·지원사업의 연구결과로 수행 되었습니다.
† 주저자, hylee@cist.korea.ac.kr
‡ 교신저자, yangh@korea.ac.kr

행되고 있으며, GHZ[12,13]상태를 이용한 다자간의 양자 키 분배[14,15]에 대한 연구 또한 관심을 끌고 있다. 이러한 다자간 양자 키 분배 프로토콜의 아이디어를 이용하면 양자 시스템에 인증 메커니즘을 도입할 수 있다. GHZ 상태를 이용하여 인증을 도입한 서명 기법[16,17] 및 양자 키 분배 프로토콜[14,15]에서는, 인증키나 비밀키가 정보를 주고받는 대상 외에 중재자에게도 동일하게 분배된다. 이는 공개된 메시지를 인증하는 경우에는 문제없지만, 비밀 통신을 원하는 사용자의 신원을 인증하거나 비밀키를 동시에 분배하려고 할 때에는 사용될 수 없다. 따라서 중재자가 키를 공유하는 사용자를 인증해주지만 키 자체에 대한 정보를 정확하게 알 수 없도록 하는 스킴이 필요하다.

본 논문에서는 완전한 안전성을 보장하면서 제 3자가 키 공유를 원하는 쌍방의 신원을 인증해주는 양자 키 분배 프로토콜을 제안하고, 제안된 프로토콜에 대한 안전성을 분석하도록 하겠다.

Ⅱ. 인증된 양자 키 분배 프로토콜

이 논문에서는 중재자가 정직하다는 전제 아래, 중재자가 키를 공유하는 사람, 즉 비밀 메시지를 보내고자 하는 사람(갑)과 받는 사람(을)의 신원을 보증해주는 양자 키 분배 프로토콜을 제안한다. 이때 신원보증은 키 분배 과정에서 중재자가 GHZ 입자를 키 분배 이전에 확인될 수 있는 정보를 가진 갑과 을에게 전달함으로써 이루어진다고 가정한다. 즉, 중재자로부터 올바른 GHZ 입자를 받는 사람이 갑과 을이라는 확인을 하는 것이다. 기존에 제안되었던 양자 키 분배[14,15,16, 17]와는 다르게, 본 논문에서 제안하는 프로토콜은 중재자가 키 분배에 관여하지만 분배된 키에 대해서는 어떠한 정보도 알 수 없도록 한다. 또한, 기존 프로토콜에서 사용하지 못했던 정보를 모두 이용하여 채널 상에 오류가 없을 경우 100%의 효율성을 보장한다.

프로토콜은 다음과 같다. 우선 암호키 분배를 원하는 사용자(갑)가 상대방(을)과 비밀 통신을 하기를 원한다는 사실을 중재자에게 알린다. 중재자는 위와 같은 사실을 을에게 통보하고, N개의 GHZ 상태 $|\psi\rangle$를 생성한다. 중재자가 GHZ 상태를 사용하면, 프로토콜이 종료된 후에도 공유된 키가 정직한 중재자나 도청자에게 누출되지 않는다.

$$|\psi\rangle=\frac{1}{\sqrt{2}}(|000\rangle_{AaB}+|111\rangle_{AaB})$$

여기에서 A 는 갑, a는 중재자, B는 을이 갖게 되는 입자를 나타낸다.

중재자는 각각의 GHZ 상태에서 첨자가 A인 것은 갑에게, B인 것은 을에게 전송하고 나머지 하나는 자신이 보관한다. 중재자가 GHZ 상태를 갑과 을에게 분배하는 과정은 도청에 안전하다고 가정한다. 중재자가 GHZ 상태 분배시에 기존에 가지고 있는 갑, 을과 공유된 각각의 비밀 정보등을 이용하여 GHZ 입자를 암호화 하여 전달하기 때문에 갑과 을만이 올바르게 GHZ 상태를 공유할 수 있으며, 이를 통하여 갑과 을은 자신이 키를 공유하는 대상에 대한 확신할 수 있다.

갑과 을은 각각 자신의 GHZ 입자들에 무작위로 Pauli 연산 I 와 σ_x중의 하나를 선택하여 연산을 취한다. 이때 I 연산을 0으로, σ_x 연산을 1로 본다면, 을이 사용하는 연산의 수열이 바로 갑과 을이 나눠 갖게 될 키 수열이 된다. 이때, 갑이 사용한 연산의 수열을 암호키로도 사용할 수 있으나, 키 공유 요청을 받은 을이 키 수열에 대한 의구심을 갖지 않게 하기 위하여 을이 사용한 연산을 최종 암호키로 사용하도록 고안하였다. 한편, 완전한 무작위성을 만족시키려면, 갑과 을이 같은 연산자만을 사용한 경우를 키로 삼고, 나머지 비트는 에러 확인 및 정정을 위하여 사용할 수 있다.

갑과 을이 각각 Pauli 연산을 취한 이후의 GHZ 상태 변화는 다음과 같이 표현된다.

표 1. 연산이후 변화된 GHZ 상태

$\|\psi\rangle$에 작용시키는 연산자		변화된 GHZ 상태
갑	을	
I_A	I_B	$\|G_0\rangle=\frac{1}{\sqrt{2}}(\|000\rangle_{AaB}+\|111\rangle_{AaB})$
I_A	σ_{x_B}	$\|G_1\rangle=\frac{1}{\sqrt{2}}(\|001\rangle_{AaB}+\|110\rangle_{AaB})$
σ_{x_A}	I_B	$\|G_2\rangle=\frac{1}{\sqrt{2}}(\|100\rangle_{AaB}+\|011\rangle_{AaB})$
σ_{x_A}	σ_{x_B}	$\|G_3\rangle=\frac{1}{\sqrt{2}}(\|101\rangle_{AaB}+\|010\rangle_{AaB})$

연산이 끝나면, 갑은 자신의 GHZ 입자를 중재자에게 전달하고, 을은 갑에게 자신의 GHZ 입자를 전달한다. 즉, 갑은 을의 입자를 얻게 되고, 중재자는

표 2. 중재자의 C-NOT 연산 및 정보 공개

중재자의 C-NOT 연산 이후의 상태	중재자의 정보 공개	갑의 을 qubit 측정치
$\mid G'_0\rangle = CNOT_{aA} \mid G_0\rangle = \frac{1}{\sqrt{2}}(\mid 000\rangle_{AaB} + \mid 011\rangle_{AaB})$	O	0
	X	1
$\mid G'_1\rangle = CNOT_{aA} \mid G_1\rangle = \frac{1}{\sqrt{2}}(\mid 001\rangle_{AaB} + \mid 010\rangle_{AaB})$	O	1
	X	0
$\mid G'_2\rangle = CNOT_{aA} \mid G_2\rangle = \frac{1}{\sqrt{2}}(\mid 100\rangle_{AaB} + \mid 111\rangle_{AaB})$	O	1
	X	0
$\mid G'_3\rangle = CNOT_{aA} \mid G_3\rangle = \frac{1}{\sqrt{2}}(\mid 101\rangle_{AaB} + \mid 110\rangle_{AaB})$	O	0
	X	1

갑의 입자 및 자신의 입자를 갖게 된다. 이후, 중재자는 자신의 입자를 control qubit으로 갑의 입자를 target qubit으로 하여 C-NOT 연산을 취한다. 연산이 끝나면 중재자가 가지고 있는 모든 qubit 즉, 갑에서 받은 qubit과 자신의 qubit에 대해 von Newman 측정을 한 뒤, 그 결과가 같은 지만을 공개한다. 이때, 입자의 측정치를 공개하지 않는 이유는, 그것이 공개되었을 경우 도청자에게 모든 정보가 노출될 수 있기 때문이다.

한편, 갑은 을로부터 받은 qubit에 대해 von Newman 측정을 한다.

중재자의 정보 공개 및, 갑의 을의 qubit 측정 결과에 따라 갑은 자신의 연산자 정보를 수정한다. 예를 들어, 중재자의 공개 정보가 같은 경우(O), 갑의 측정치가 0이면, 갑은 자신의 정보를 그대로 자신의 키 비트로 사용하고, 갑의 측정치가 1이면, 갑은 자신의 정보를 바꾸어 키 비트로 사용한다. 중재자의 공개 정보가 다른 경우(X), 갑의 측정치가 0이면, 갑은 자신의 정보를 바꾸어 키 비트로 사용하고, 갑의 측정치가 1이면, 갑은 자신의 정보를 그대로 키 비트로 사용한다. 이를 정리하면 〔표 3〕과 같다.

갑과 을이 사용한 연산자는 공개되지 않기 때문에, 도청자나 정직한 중재자는 공유되는 키 수열을 알 수 없다. 이에 대한 분석은 다음 절에서 자세히 다루도록 하겠다.

표 3. 중재자의 정보 공개 및 갑의 을 qubit 측정치에 따라 공유되는 키 비트

중재자의 정보 공개	갑의 을 qubit 측정치	키 비트
O	0	같은 비트
	1	다른 비트(갑의 비트 플립)
X	0	다른 비트(갑의 비트 플립)
	1	같은 비트

Ⅲ. 안전성 분석

제안된 프로토콜의 안전성을 살펴보기 위하여 도청자가 갑의 qubit을 도청하는 경우, 을의 qubit을 도청하는 경우, 그리고 갑과 을의 qubit을 모두 도청하는 경우로 나누어 살펴보기로 하겠다. 중재자가 갑과 을에게 GHZ 상태를 분배할 때 발생되는 에러 등은 privacy amplification 및 entanglement distillation[18,19,20,21,22] 등을 이용하여 보정할 수 있을 것이다. 또한 GHZ 입자는 중재자가 기존에 갑, 을과 공유된 각각의 비밀 정보를 이용하여 갑과 을에게만 전달된다고 가정한다. 즉 GHZ 상태 분배 시에는 도청자가 없다고 가정할 수 있다.

3.1 도청자가 갑의 qubit을 도청하는 경우

갑이 자신의 qubit에 연산을 취한 후, 중재자에게 그 qubit을 전달하는 과정에서 도청이 일어난 경우를 살펴보자. 도청자는 측정을 통해 그 qubit의 정보가 0인지 1인지를 파악하고 중재자에게 전달하게 된다. 측정을 통해서 양자상태가 붕괴되기 때문에 〔표 4〕를 얻는다. 〔표 4〕에서 보듯이, 도청자는 을 qubit에 대한 측정치를 알 수 없으므로 분배되는 키가 무엇인지를 알 수 없다. 도청자가 알 수 있는 것은 자신이 0을 측정하면 중재자의 정보공개가 O이고, 1을 측정하면 X가 나온다는 것뿐이다. 키를 알기 위해서는 갑의 을 qubit 측정치를 알아야만 한다.

3.2 도청자가 을의 qubit을 도청하는 경우

도청자가 을이 갑에게 보내는 qubit 정보를 도청하는 경우를 생각해 보자. 이 경우에도 3.1의 경우와 마찬가지로 〔표 5〕와 같이 정리할 수 있다. 〔표

표 4. 도청자가 갑의 qubit만을 도청하는 경우

채널에 전송되던 GHZ 상태	도청자의 갑 qubit 측정치	변화된 상태	중재자의 C-NOT 연산	중재자의 정보공개	갑의 을 qubit 측정치
$\|G_0\rangle=\frac{1}{\sqrt{2}}(\|000\rangle_{AaB}+\|111\rangle_{AaB})$	0	$\|000\rangle_{AaB}$	$\|000\rangle_{AaB}$	O	0
	1	$\|111\rangle_{AaB}$	$\|011\rangle_{AaB}$	X	1
$\|G_1\rangle=\frac{1}{\sqrt{2}}(\|001\rangle_{AaB}+\|110\rangle_{AaB})$	0	$\|001\rangle_{AaB}$	$\|001\rangle_{AaB}$	O	1
	1	$\|110\rangle_{AaB}$	$\|010\rangle_{AaB}$	X	0
$\|G_2\rangle=\frac{1}{\sqrt{2}}(\|100\rangle_{AaB}+\|011\rangle_{AaB})$	0	$\|011\rangle_{AaB}$	$\|111\rangle_{AaB}$	O	1
	1	$\|100\rangle_{AaB}$	$\|100\rangle_{AaB}$	X	0
$\|G_3\rangle=\frac{1}{\sqrt{2}}(\|101\rangle_{AaB}+\|010\rangle_{AaB})$	0	$\|010\rangle_{AaB}$	$\|110\rangle_{AaB}$	O	0
	1	$\|101\rangle_{AaB}$	$\|101\rangle_{AaB}$	X	1

표 5. 도청자가 을의 qubit을 도청하는 경우

채널에 전송되던 GHZ 상태	도청자의 을 qubit 측정치	변화된 상태	중재자의 C-NOT 연산	중재자의 정보공개	갑의 을 qubit 측정치
$\|G_0\rangle=\frac{1}{\sqrt{2}}(\|000\rangle_{AaB}+\|111\rangle_{AaB})$	0	$\|000\rangle_{AaB}$	$\|000\rangle_{AaB}$	O	0
	1	$\|111\rangle_{AaB}$	$\|011\rangle_{AaB}$	X	1
$\|G_1\rangle=\frac{1}{\sqrt{2}}(\|001\rangle_{AaB}+\|110\rangle_{AaB})$	0	$\|110\rangle_{AaB}$	$\|010\rangle_{AaB}$	X	0
	1	$\|001\rangle_{AaB}$	$\|001\rangle_{AaB}$	O	1
$\|G_2\rangle=\frac{1}{\sqrt{2}}(\|100\rangle_{AaB}+\|011\rangle_{AaB})$	0	$\|100\rangle_{AaB}$	$\|100\rangle_{AaB}$	X	0
	1	$\|011\rangle_{AaB}$	$\|111\rangle_{AaB}$	O	1
$\|G_3\rangle=\frac{1}{\sqrt{2}}(\|101\rangle_{AaB}+\|010\rangle_{AaB})$	0	$\|010\rangle_{AaB}$	$\|110\rangle_{AaB}$	O	0
	1	$\|101\rangle_{AaB}$	$\|101\rangle_{AaB}$	X	1

표 6. 도청자가 갑과 을의 qubit 모두를 도청하는 경우

채널에 전송되던 GHZ 상태	도청자의 측정치		변화된 상태	중재자의 C-NOT 연산	중재자의 정보공개	갑의 을 qubit 측정치
	갑	을				
$\|G_0\rangle=\frac{1}{\sqrt{2}}(\|000\rangle_{AaB}+\|111\rangle_{AaB})$	0	0	$\|000\rangle_{AaB}$	$\|000\rangle_{AaB}$	O	0
	1	1	$\|111\rangle_{AaB}$	$\|011\rangle_{AaB}$	X	1
$\|G_1\rangle=\frac{1}{\sqrt{2}}(\|001\rangle_{AaB}+\|110\rangle_{AaB})$	0	1	$\|001\rangle_{AaB}$	$\|001\rangle_{AaB}$	O	1
	1	0	$\|110\rangle_{AaB}$	$\|010\rangle_{AaB}$	X	0
$\|G_2\rangle=\frac{1}{\sqrt{2}}(\|100\rangle_{AaB}+\|011\rangle_{AaB})$	0	1	$\|011\rangle_{AaB}$	$\|111\rangle_{AaB}$	O	1
	1	0	$\|100\rangle_{AaB}$	$\|100\rangle_{AaB}$	X	0
$\|G_3\rangle=\frac{1}{\sqrt{2}}(\|101\rangle_{AaB}+\|010\rangle_{AaB})$	0	0	$\|010\rangle_{AaB}$	$\|110\rangle_{AaB}$	O	0
	1	1	$\|101\rangle_{AaB}$	$\|101\rangle_{AaB}$	X	1

5]에서 보이듯, 도청자는 갑과 을이 같은 키 비트의 정보를 갖고 있는지 그렇지 아닌지는 파악할 수 있지만, 분배되는 키 비트 자체를 알 수는 없다. 왜냐하면, 갑과 을은 자신이 선택한 연산자 정보(I (0) 또는 $\sigma_x(1)$)를 공개하지 않기 때문에 GHZ 상태 정보를 안다고 하더라도 어떠한 키가 분배가 되는지는 알 수 없다.

3.3 도청자가 갑과 을의 qubit 모두를 도청하는 경우

도청자가 GHZ 상태가 분배된 후에, 갑이 중재자에게 전송하는 GHZ 입자와 을이 갑에게 전달하는 GHZ 입자를 모두 도청하는 경우를 생각해 보자. GHZ 상태가 분배될 때, 중재자가 갑과 을의 신원을 확인하여 본인에게 GHZ 입자를 전달함으로써 GHZ 상태가 제대로 분배된다는 것을 확인하게 되면 갑과 을은 서로를 인증할 수 있다.

도청자가 갑과 을의 GHZ 입자를 도청했을 때를 정리하면 [표 6]을 얻을 수 있으며, 3.2의 경우와 마찬가지로 같은 연산을 쓴 경우 즉, $|G_0\rangle$와 $|G_3\rangle$, $|G_1\rangle$과 $|G_2\rangle$의 구분이 불가능하기 때문에 도청자는 공유되는 키 비트가 0인지 1인지를 판단할 수 없다.

만약 중재자가 을의 정보를 획득할 수 있다면, 중재자는 모든 GHZ 상태 정보를 획득할 수 있게 되므로 분배되는 모든 키를 정확하게 알 수 있다. 이를 막기 위하여 중재자는 정직하여 도청의 시도를 하지 않는다는 가정이 필요하다. 중재자가 포함된 키 분배 스킴[14,15,16,17]에서는 중재자가 정직하든 그렇지 않든지 간에 아무런 제약 없이 분배되는 키의 내용을 알 수 있다. 그러나 본 논문에서 새롭게 제안하는 양자 키 분배 프로토콜에서는 정직한 중재자라면 분배되는 키를 알 수 없도록 하여 기밀성을 높였다고 할 수 있다.

Ⅳ. 결 론

위에서 살펴보았듯이, 새롭게 제안된 양자 키 분배 프로토콜은 중재자가 정직하고 초기에 GHZ 상태가 안전하게 분배된다면, 기존에 제안된 양자 키 분배 프로토콜과 마찬가지로 도청에 대해 안전하다.

본 논문에서 새로 제안한 양자 키 분배 프로토콜은 제 3자인 중재자가 키를 공유하고자 하는 쌍방을 GHZ 상태 분배 시에 인증하기 때문에 신뢰를 제공하고, 도청자는 물론 정직한 중재자도 키 분배의 내용을 알지 못한다는 특성을 지닌다. 인증된 양자 키 분배 프로토콜은 경우에 따라 다양하게 변화시켜서 이용할 수 있을 뿐만 아니라, 구현상으로도 Pauli operation만을 이용하고 측정 후 고전 정보를 이용한 연산으로 변환시킬 수 있기 때문에 쉽게 구현될 수 있을 것이다.

참 고 문 헌

[1] C. H. Bennett and G. Brassard, in Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing (IEEE, New York , 1984), p. 175.

[2] Artur K. Ekert, "Quantum cryptography based on Bell' s theorem", Phys. Rev. Lett. 67, 661 (1991).

[3] Charles H. Bennett, "Quantum Cryptography Using Any Two Nonorthogonal States", Phys. Rev. Lett. 68, 3121 (1991).

[4] 이화연, 조규형, 양형진, "양자 키분배 프로토콜", 정보보호학회지 12권 5호 p. 1 (2002)

[5] Charlse H. Bennett, Gilles Brassard, N.David Mermin, "Quantum cryptography without Bell's theorem", Phys. Rev. Lett 68, 5, pp557-559 (1992)

[6] Dominic Mayers, "Unconditional security in Quantum Cryptography", quant-ph/9802025 (1998)

[7] Hoi-Kwong Lo and H.F.Chau, "Unconditional security of Quantum key distribution over arbitrarily long distances", science vol 283 pp2050~2056(1999)

[8] Peter W. Shor, John Preskill, "Simple proof of security of the BB84 quantum key distribution protocol", Phys. Rev. Lett. 85, 441-444 (2000)

[9] W. T. Buttler, R. J. Hughes, P. G. Kwiat, S. K. Lamoreaux, G. G.

Luther, G. L. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons, "Practical free-space Quantum key distribution over 1km", Phys. Rev. Lett vol 81 pp.3283-3286 (1998)

[10] W. T. Buttler, R. J. Hughes, S. K. Lamoreaux, G. L. Morgan, J. E. Nordholt, and C. G. Peterson, "Daylight Quantum key distribution over 1.6km", Phys. Rev. Lett. 84, 5652-5655 (2000)

[11] C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P. M. Gorman, P. R. Tapster, J. G. Rarity, "A step towards global key distribution", NATURE vol 419 pp450 (2002)

[12] D. M. Greenberger, M. A. Horne, A. Shimony, and A. Zeilinger, "Bell's theorem without inequalities" Am. J. Physics 58, 1131(1990)

[13] Dik Bouwmeester, Jian-Wei Pan, Matthew Daniell, Harald Weinfurter, and Anton Zeilinger, "Observation of There-Photon Greenberger-Horne-Zeilinger Entanglement", Phys. Rev. Lett. 82, 1345-1349 (1999)

[14] Eli Biham, Bruno Huttner and Tal Mor, "Quantum cryptographic network based on quantum memories" Phys. Rev. A 54, 2651-2658(1996)

[15] Guihua Zeng and Wieiping Zhang, "Identification in quantujm key distribution", Phy. Rev. A 61, 022303 (2000)

[16] Guihua Zeng and Christoph H. Keitel, "Arbitrated quantum-signature scheme", Phys. Rev. A. 65, 042312 (2002).

[17] Hwayean Lee, Changho Hong, Hyunsang Kim, Jongin Lim, HyungJin Yang, "Arbitrated quantum signature scheme with message recovery", Physics Letters A 321, Issue5-6, p.295-300 (2004)

[18] Nicolas Gisin, Gregoire Ribordy, Wolfgang Tittel, and Hugo Zbinden, "Quantum cryptography", Rev. Mod. Phys. 74, 145-195(2002)

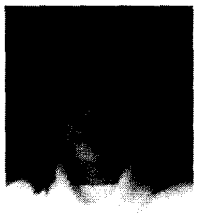
[19] Charles H. Bennett, David P. DiVincenzo, John A. Smolin, and William K. Wootters, "Mixed-state entanglement and quantum error correction", Phys. Rev. A 54, 3824-3851 (1996)

[20] A. Ambainis, A.Smith, and Ke Yang, "Extracting Quantum Entanglement (General Entanglement Purification Protocols)", 17th Annual IEEE conference on Computational Complexity (CCC2002) p103

[21] M. Murao, M. B. Plenio, S. Popescu, V. Vedral, and P. L. Knight, "Multipartite entanglement purification protocols", Phys. Rev. 57, R4075 (1998)

[22] Ping-Xing Chen and Cheng-Zu Li, "Distilling multipartite pure state from a finite number of copies of multipartite mixed states', Phys. Rev. A 69, 012308 (2004)

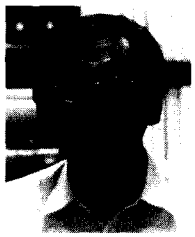
〈著者紹介〉



이 화 연 (Hwa-Yean Lee)
2001년 2월: 고려대학교 수학과 학사
2003년 2월: 고려대학교 정보보호대학원 석사
2003년 3월~현재: 고려대학교 정보보호대학원 박사과정
〈관심분야〉 양자암호, 암호프로토콜

홍 창 호 (Chang-ho Hong)
2001년 2월: 고려대학교 자연과학대학 물리학과 학사
2003년 2월: 고려대학교 응용물리대학원 응집물리학과 석사
2003년 3월~현재: 고려대학교 정보보호대학원 박사과정
〈관심분야〉 양자암호, 암호프로토콜

이 덕 진 (Dong-Hoon Lee)
2003년 2월: 고려대학교 자연과학대학 물리학과 학사
2003년 3월~현재: 고려대학교 정보보호대학원 석사과정
〈관심분야〉 양자 암호, 암호 프로토콜



양 형 진 (Hyung-jin Yang)
1990년 8월~1990년 10월: 미국 Oak Ridge 국립 연구소, Computer Consultant
1990년 12월~1991년 12월: 미국 신시내티대학교 박사후 연구원
1999년 1월~1999년 12월: 미국 매릴랜드대학교 교환교수
1992년 3월~현재: 고려대학교 자연과학대학 물리학과 교수
2001년 3월~현재: 고려대학교 정보보호대학원 겸임교수
〈관심분야〉 양자암호, 암호프로토콜

임 종 인(Jong-in Lim)
1980년 2월: 고려대학교 수학과 학사
1982년 2월: 고려대학교 수학과 석사
1986년 2월: 고려대학교 수학과 박사
1986년~2001년 1월: 고려대학교 수학과 교수
1999년~현재: 고려대학교 정보보호기술연구센터 센터장, 한국정보보호진흥원 사외이사
2000년~현재: 고려대학교 정보보호대학원 원장, 정보통신부 정보보호 자문위원
2003년 4월: 국가정보원/국가보안기술연구소 정보보안/암호정책 자문위원
2003년 11월~현재: 국무총리산하 개인정보보호심의위원회 위원
〈관심분야〉 사이버법률, 포렌식, 프라이버시, 암호기술, 양자 암호 등등