TTA Standard

정보통신단체표준(국문표준)

제정일: 20xx년 xx월 xx일

양자 키 분배 - 제1부: 일반

Quantum Key Distribution - Part1: General

TTA 한국정보통신기술협회
Telecommunications Technology Association

표준초안 검토 위원회 정보보호기반 프로젝트그룹(PG501)

표준안 심의 위원회 정보보호 기술위원회(TC5)

	성명	소 속	직위	위원회 및 직위	표준번호
표준(과제) 제안	김나영	국가보안기술 연구소	연구원	정보보호기반 프로젝트그룹 위원	
표준 초안 작성자	김나영	국가보안기술 연구소	연구원	정보보호기반 프로젝트그룹 위원	
	홍창호	국가보안기술 연구소	선임연구원	-	
	권오성	국가보안기술 연구소	선임연구원	-	
	정연창	국가보안기술 연구소	선임연구원	-	
	지세완	국가보안기술 연구소	선임연구원	-	
	장진각	국가보안기술 연구소	책임연구원	-	
	권대성	국가보안기술 연구소	책임연구원	-	
사무국 담당	박수정	TTA	책임	-	

본 표준 발간 이전에 접수된 지식재산권 확약서 정보는 본 표준의 '부록(지식재산권 확약서 정보)'에 명시하고 있으며, 이후 접수된 지식재산권 확약서는 TTA 웹사이트에서 확인할 수 있습니다.
본 표준과 관련하여 접수된 확약서 외의 지식재산권이 존재할 수 있습니다.

발행인 : 한국정보통신기술협회 회장
발행처 : 한국정보통신기술협회
13591, 경기도 성남시 분당구 분당로 47
Tel : 031-724-0114, Fax : 031-724-0109
발행일 : 20xx.xx

서 문

1 표준의 목적

양자 키 분배(QKD, Quantum Key Distribution)는 정당한 두 사용자가 양자를 이용하여 비밀키를 공유하는 것이다. 이 표준의 목적은 QKD의 일반적인 모델과 단계별 절차를 제시하는 것이다.

2 주요 내용 요약

이 표준은 QKD의 개념을 바탕으로 일반적 모델을 정립하고, QKD를 실현하기 위해 설계된 다양한 QKD 프로토콜을 포괄할 수 있는 단계별 절차와 안전성 요구사항을 제시한다.

3 인용 표준과의 비교

3.1 인용 표준과의 관련성

해당사항 없음

3.2 인용 표준과 본 표준의 비교표

해당사항 없음

Preface

1 Purpose

The purpose of Quantum Key Distribution(QKD) is that two legitimate users share a secret random key using quantum mechanics. The standard provides a general model and process of QKD.

2 Summary

The standard provides a general model which is based on the basic concept of QKD, stepwise process, and security requirements that would encompass the various QKD protocols.

3 Relationship to Reference Standards

- None

목 차

양자 키 분배 - 제1부 일반
(Quantum Key Distribution - Part1: General)

1 적용 범위

양자 키 분배(Quantum Key Distribution, 이하 QKD)는 정당한 두 사용자가 양자(quantum)를 이용하여 안전하게 비밀키를 공유하는 것이다. QKD는 기존 계산 복잡도에 기반한 키 공유 기법의 조건부 안전성과 달리 양자물리법칙에 기반하여 무조건부 안전성(unconditional security)을 이론적으로 보장한다. 조건부 안전성은 수학적 문제의 해결 난이도에 의존하는 것으로, 컴퓨터의 연산 능력이 증가하고 문제 해결 알고리즘이 발전함에 따라 안전성이 저하될 수 있다. 반면 무조건부 안전성은 수학적 어려움과는 상관없이 무한한 계산 능력을 가진 공격자를 가정하더라도 QKD로 공유한 비밀키의 기밀성이 손상되지 않는 정보이론적 안전성을 의미한다.

QKD는 사용하는 프로토콜과 구현방법에 따라 세부 절차가 달라진다. 이 표준에서는 구체적인 프로토콜을 정의하기 앞서 QKD의 일반적 모델을 정립한다. 그리고 다양한 QKD 프로토콜을 포괄할 수 있는 단계별 절차와 안전성 요구사항을 제시한다.

2 인용 표준

해당사항 없음

3 용어 정의

3.1 QKD 프로토콜(QKD protocol)
양자 키 분배를 하기 위한 통신 규약들

3.2 raw키(raw key)
양자채널을 통한 양자상태의 송·수신 결과인 키 수열

3.3 걸러진키(sifted key)
송·수신자 사이에 동일한 기저를 사용한 키 수열

3.4 공개채널(public channel)

도청자를 포함하여 외부에 완전히 공개된 채널로 非양자정보가 전송되는 채널. 공개채널로 전송되는 정보는 누구나 확인 가능하나 변조되지 않음을 가정하며 일반적으로 QKD에서 사용하는 공개채널은 고전채널(classical channel)이라 칭하기도 함

3.5 기저(basis)

양자상태를 구분 짓는 기준 좌표

3.6 비밀증폭(privacy amplification)

오류정정 과정의 공개된 정보와 이로 인해 비밀키의 유추 가능한 정보를 제거하는 단계

3.7 비밀키(secret key)

QKD를 통해 생성된 최종 키. QKD의 최종 결과물

3.8 양자채널(quantum channel)

양자의 물리적 상태를 전송하는 채널

3.9 오류정정(reconciliation)

걸러진키의 오류를 수정하는 단계

3.10 위상 부호화(phase encoding)

광자의 위상차를 이용하여 부호화함

3.11 유니버셜 해시함수(universal hash function)

일방향 함수의 일종으로 충돌이 일어날 가능성이 최대 $1/2^M$이 되는 함수를 의미함. 여기서 M은 입력메시지의 전체 길이를 표현함

3.12 편광 부호화(polarization encoding)

광자의 방향성을 이용하여 부호화함

3.13 후처리 과정(post process)

오류정정 단계와 비밀증폭 단계를 합쳐서 일컫는 과정

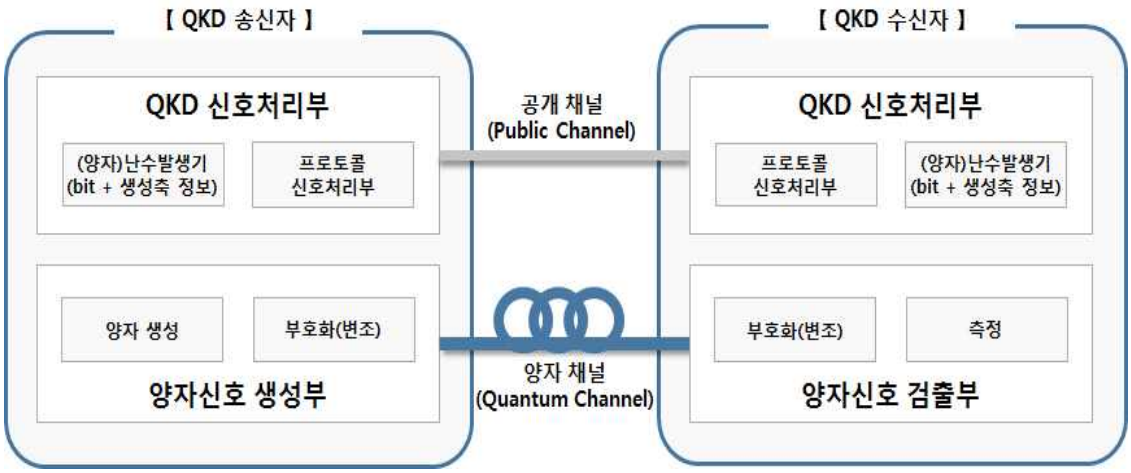
4 약어 및 기호

QKD	Quantum Key distribution

5 양자 키 분배(QKD) 일반

양자 키 분배(QKD)란 양자 역학의 특성을 활용하여 정당한 사용자들이 비밀키를 공유하는 것이다. QKD는 양자물리법칙에 기반하여 정보이론의 무조건부 안전성(unconditional security)을 보장한다.

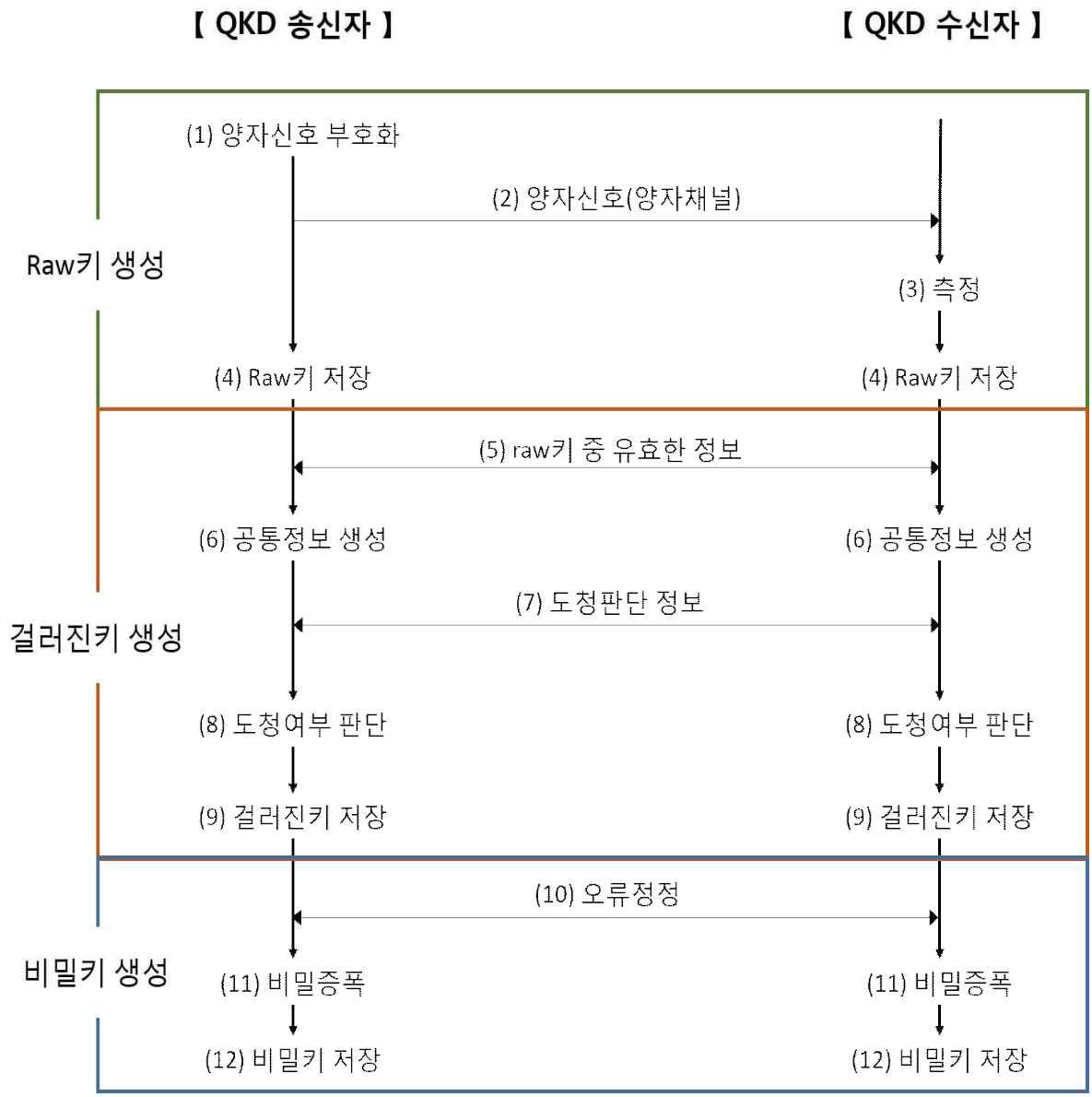
QKD를 운용하는 사용자는 송신자와 수신자로 구분할 수 있다. 송·수신자는 양자신호 생성부 혹은 검출부와 QKD 신호처리부로 이루어져 있으며 각각 양자채널(quantum channel)과 공개채널(public channel)로 연결되어 있다(그림 5-1 참조). 양자신호 생성부 혹은 검출부는 양자신호를 생성하거나 검출하는 부분으로 레이저, 반사거울, 광분할기, 광검출기 등을 포함하는 광학계로 구성되며, QKD 신호처리부는 (양자)난수발생기를 사용하여 난수를 생성하고 생성된 난수를 활용해 키분배와 후처리 과정을 진행한다. 실제 QKD 구현 시 광자를 양자상태로 사용하는 경우 양자채널은 광섬유 및 자유공간 등으로 구현될 수 있으며, 공개채널은 이더넷(ethernet) 및 무선 통신을 사용할 수 있다



(그림 5-1) QKD 구성도

QKD의 절차는 크게 raw키 생성, 걸러진키 생성, 비밀키 생성 단계로 구분할 수 있다. 두 사용자는 양자채널을 통해 부호화 된 양자신호를 송·수신하여 raw키를 생성하고, 공개채널을 이용하여 사용된 정보를 확인한 후 걸러진키를 생성한다. 이렇게 생성된 걸러진키에 후처리 과정을 적용하여 비밀키를 생성한다.

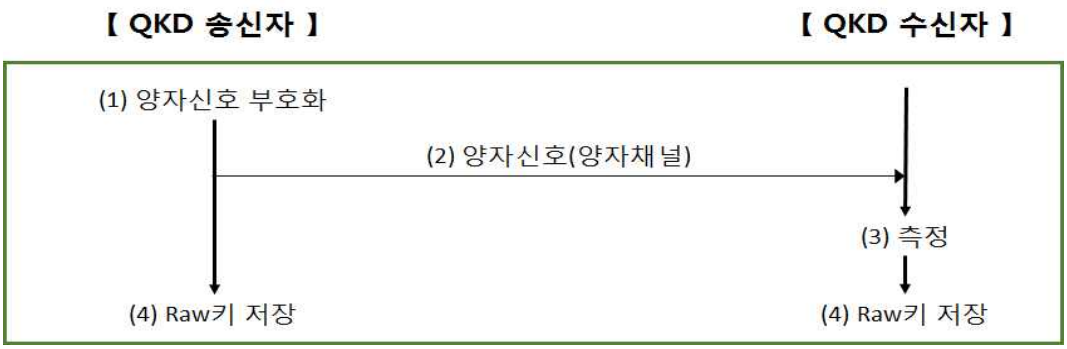
QKD의 raw키 생성, 걸러진키 생성, 비밀키 생성 단계는 QKD 프로토콜과 후처리 알고리즘에 따라 세부절차가 다를 수 있다. 따라서 각 단계의 구체적인 세부절차는 특정 QKD 프로토콜을 다루는 연계 표준에서 제시한다. 이 표준에서는 다양한 QKD 프로토콜을 포괄할 수 있는 공통적인 내용으로 raw키 생성, 걸러진키 생성, 비밀키 생성 단계의 일반적인 절차를 제시한다(그림 5-2 참조). 각 단계별 내용은 하위절에서 설명한다.



(그림 5-2) QKD 절차도

5.1 Raw키 생성

정당한 송신자가 부호화(encoding)된 양자신호를 양자채널을 통해 전송하고 수신자는 측정기저를 통해 수신된 양자신호를 측정하여 raw키를 저장하는 단계이다. 양자신호는 프로토콜에 따라 수신자만 측정(BB84[1], B92[2] 등)하거나, 송·수신자 모두 측정을 수행(Ekert91[4] 등)할 수 있다. Raw키 생성 단계의 세부 절차는 QKD 프로토콜에 따라 결정되며, 다양한 QKD 프로토콜을 포괄하는 일반적인 raw키 생성 단계는 다음과 같이 진행된다.



- Raw키 생성 단계

(1) 송·수신자는 양자신호를 부호화한다.

(2) 송신자는 부호화된 양자신호를 양자채널을 통해 수신자에게 전달한다.

(3) 수신자는 송신자가 전달한 양자신호를 측정한다. 그리고 경우에 따라 송신자도 측정을 수행한다.

(4) 송·수신자는 인코딩 정보, 측정정보를 raw키로 저장한다.

5.2 걸러진키 생성

무작위적인 raw키 중에서 유효한 정보를 이용하여 걸러진키를 생성하는 단계이다. 걸러진키 생성 역시 raw키 생성 단계와 마찬가지로 QKD 프로토콜에 의존하여 세부 절차가 결정된다. 다양한 QKD 프로토콜을 포괄하는 일반적인 걸러진키 생성 단계는 다음과 같이 진행된다.

- 걸러진키 생성 단계

(5) 송·수신자는 raw키에서 공통정보를 추출하기 위한 유효한 정보를 공개채널로 공유한다.

(6) 송·수신신자는 단계 (5)에서 공유한 정보를 이용하여 공통정보를 생성한다.

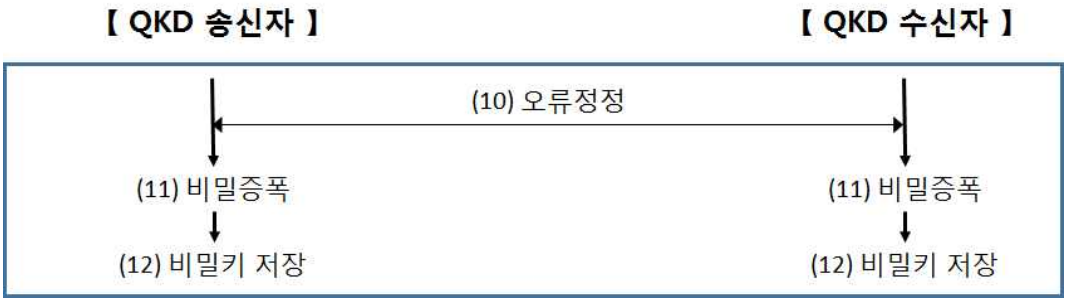
(7) 송·수신자는 도청확인을 위해 공통정보의 일부를 공개채널로 공유한다.

(8) 송·수신자는 단계 (7)에서 공유한 공통정보(도청판단 정보)를 이용하여 도청여부를 판단한다.

(9) 도청이 없음이 확인된 경우, 송·수신자는 도청확인을 위해 공유한 정보를 제외한 공통정보를 걸러진키로 저장한다. 도청이 확인된 경우, 송·수신자는 모든 정보를 폐기한 후 raw키 생성 단계부터 다시 시작한다.

5.3 비밀키 생성

걸러진키에 후처리 알고리즘을 적용하여 비밀키를 생성한다. 후처리 알고리즘은 오류정정과 비밀증폭 단계로 구성되며, 오류정정 기법은 Cascade[6], WINNOW[7], LDPC[8] 등을 사용할 수 있고 비밀증폭 기법은 유니버셜 해시 함수를 사용할 수 있다.



- 비밀키 생성 단계

(10) 송·수신자는 걸러진키를 일치시키기 위해 비트오류정정 기법을 이용하여 오류를 정정한다.

(11) 송·수신자는 오류 정보 및 오류정정 과정에서 유출된 정보를 비밀증폭 과정으로 제거한다. 비밀증폭의 일반적 방법은 일방향의 특성을 가진 유니버셜 해시 함수(universal hash function)를 이용하는 것이다. 이 때, 두 사용자가 사전에 공유한 인증키로 유니버셜 해시 함수를 구성하여 서로의 신원을 확인하는 인증을 수행할 수 있다.

(12) 송·수신자는 위의 모든 과정 수행 결과를 비밀키로 저장한다.

6 QKD의 안전성 요구사항

QKD 프로토콜의 절차 수정은 QKD 프로토콜 안전성에 영향을 미칠 수 있고 생성되는 비밀키의 안전성을 저하시킬 수 있다. 그러므로 송·수신자는 QKD 프로토콜과 후처리 알고리즘의 각 절차를 충실히 이행해야 한다. (그림 5-2)에서 제시된 QKD 절차의 이론적 안전성 요구사항은 다음과 같다.

6.1 Raw키 생성

- Raw키 생성 시 사용되는 정보는 무작위성이 보장되어야 한다.
- Raw키 생성에 관련된 정보는 걸러진키 생성 단계 전까지 공개되지 않아야 한다.

6.2 걸러진키 생성

- 걸러진키 생성 시 공개되는 정보는 변조가 불가능해야 한다.
- 걸러진키 생성과정을 통해 도청 여부가 확인되어야 한다.

6.3 비밀키 생성

- 비밀키 생성 단계 중 오류정정을 위해 공개되는 정보는 변조가 불가능해야 한다.
- 오류정정 단계에서 공개된 정보는 반드시 제거해야 한다.
- 공개된 내용을 통해 비밀키 정보의 유추가 불가능해야 한다.

7. 양자 키 분배(QKD) 세부절차

QKD는 일반적으로 raw키 생성, 걸러진키 생성, 비밀키 생성 단계로 진행되며, 각 단계는 특정 QKD 프로토콜과 후처리 알고리즘의 선택에 따라 세부절차가 정해진다. QKD 절차에서 raw키 생성 단계와 걸러진키 생성 단계의 세부 절차는 QKD 프로토콜에 따라 결정된다. 대표적인 QKD 프로토콜은 BB84[1], B92[2], 6-state[3], Ekert91[4], BBM92[5] 프로토콜 등이 있으며, 각각 프로토콜은 구현 기법에 따라 단방향과 양방향 기법, 편광 부호화와 위상 부호화 등 다양하게 구성될 수 있다. 그러므로 QKD에 필요한 구체적인 프로토콜이 정해지면 그에 대응하는 raw키 생성 단계와 걸러진키 생성 단계의 세부절차가 결정된다. 한편, 비밀키 생성 단계는 QKD 프로토콜과 상관없이 오류정정, 비밀증폭, 비밀키 저장 순서로 진행된다. 그러나 오류정정, 비밀증폭과정은 후처리 알고리즘에 의존한다. 후처리 알고리즘 중 오류정정 기법은 Cascade[6], WINNOW[7], LDPC[8] 등을 사용할 수 있으며, 비밀증폭 기법은 유니버셜 해시함수를 사용할 수 있다. 일반적으로 QKD 프로토콜은 raw키 생성 단계 및 걸러진키 생성 단계와 직접 연관이 있으며, 비밀키 생성 단계와 함께 안전성 증명이 완성된다. 따라서 비밀키 생성 단계는 QKD 프로토콜 진행 후 반드시 수반되어야 한다. 각 단계의 구체적인 세부절차는 이 표준의 범위를 벗어나므로 특정 프로토콜을 다루는 연계 표준에서 제시한다.

부 록 Ⅰ-1

지식재산권 확약서 정보

해당 사항 없음

부 록 Ⅰ-2

시험인증 관련 사항

해당 사항 없음

부 록 Ⅰ-3

본 표준의 연계(family) 표준

해당 사항 없음

부 록 Ⅰ-4

참고 문헌

[1] C.H. Bennett, G. Brassard, “Quantum cryptography: Public key distribution and coin tossing”, *P*roceedings of IEEE International Conference on Computer, Systems and Signal Processing, 175, 8, 1984.

[2] C.H. Bennett, “Quantum cryptography using any two nonorthogonal states”, Phys. Rev. Lett. 68, 3121, 1992.

[3] D. Bruss, “Optimal eavesdropping in quantum cryptography with six states”, Phys. Rev. Lett. 81, 3018, 1998.

[4] A.K. Ekert, “Quantum cryptography based on Bell’s theorem”, Phys. Rev. Lett. 67, 661, 1991

[5] C.H. Bennett, G. Brassard, N.D. Mermin, “Quantum cryptography without Bell’s theorem”, Phys. Rev. Lett. 68, 557, 1992.

[6] F. Bessette, L. Salvail, “Secure key reconciliation by public discussion”, Advances in Cryptology-Proc. Eurocrypt '93, 410, 1994

[7] W.T. Buttler, S.K. Lamoreaux, J.R. Torgerson, G.H. Nickel, C.H. Donahue, C.G. Peterson, “Fast, efficient error reconciliation for quantum cryptography”, Phys. Rev. A 67, 52303, 2003

[8] D. Pearson, “High-speed QKD reconciliation using forward error correction”, Quantum Communication, Measurement and Computing, 04, 299, 2004

부 록 Ⅰ-5

영문표준 해설서

해당 사항 없음

부 록 Ⅰ-6

표준의 이력

판수	채택일	표준번호	내용	담당 위원회
제1판				