TTA Standard

정보통신단체표준(국문표준)

TTAx.xx-xx.xxxx/R1 제정일: 2019년 xx월 xx일

# 다변수 이차식 기반 양자내성암호 - 제1부: 부가형 전자서명 알고리즘

# Post Quantum Cryptography based on Multivariate Quadratic Equations - Part 1: Digital Signature Algorithm with Appendix

TTA 한국정보통신기술협회
Telecommunications Technology Association

**표준초안 검토 위원회** 정보보호기반 프로젝트그룹(PG501)

**표준안 심의 위원회** xx 기술위원회(TCx)

| | 성명 | 소 속 | 직위 | 위원회 및 직위 | 표준번호 |
|---|---|---|---|---|---|
| **표준(과제) 제안** | 심경아 | NIMS | 책임연구원 | - | |
| **표준 초안 작성자** | 심경아 | NIMS | 책임연구원 | - | |
| | 박철민 | NIMS | 선임연구원 | | |
| **사무국 담당** | | TTA | | - | |

본 문서에 대한 저작권은 TTA에 있으며, TTA와 사전 협의 없이 이 문서의 전체 또는 일부를 상업적 목적으로 복제 또는 배포해서는 안 됩니다.

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 : 2019.xx

# 서 문

## 1 표준의 목적

이 표준의 목적은 임의의 길이를 갖는 메시지에 대해 전자서명을 생성 및 검증 할 수 있도록 해 주는 다변수 이차식 기반 부가형 전자서명 알고리즘의 일반적인 부분을 규정하여, 정보처리시스템 및 정보통신 망 환경에서 인증, 무결성 및 부인 방지 등의 정보보호 서비스를 제공하는 것이다.

## 2 주요 내용 요약

이 표준은 다변수 이차식 기반 부가형 전자서명 알고리즘의 키 생성, 서명 생성과 검증 과정의 일반적인 사항을 정의하고 있다.

## 3 인용 표준과의 비교

해당 사항 없음.

# Preface

## 1 Purpose

The standard is to specify the post-quantum digital signature algorithm with appendix based on mutlivariate quadratic equations for key generation, signature generation and signature verification on arbitrary length of message. This algorithm is used to provide authentication, integrity, and non-repudiation services in the information processing systems and communication environments.

## 2 Summary

The standard defines general methods of the digital signature algorithm with appendix based on mutlivariate quadratic equations that can be used for the protection of electronic documents, and for the verification and validation of those digital signatures.

## 3 Relationship to Reference Standards

None

# 목 차

# 다변수 이차식 기반 양자내성암호 - 제1부: 부가형 전자서명 알고리즘

# (Post Quantum Cryptography based on Multivariate Quadratic Equations - Part 1 : Digital Signature Algorithm with Appendix)

## 1 적용 범위

전자서명 알고리즘은 공개키 기반 구조(PKI, Public Key Infrastructure)가 뒷받침되는 정보처리시스템 또는 정보통신망 환경에서 인증, 무결성 및 부인 방지 등의 정보보호 서비스를 제공할 수 있는 암호 기술이다. 전자서명은 전자서명 알고리즘의 서명 생성 과정에서 주어진 메시지에 대해 도메인 변수와 서명자의 전자 서명키를 적용하여 생성된다. 그리고 서명 검증 과정을 통해 유효한 것으로 판정된 전자서명은 서명자를 식별하고 서명 대상 메시지의 무결성을 입증할 수 있다. 전자서명의 생성과 검증은 전자 문서를 대상으로 한다.

서명 생성 과정은 전자서명을 생성하기 위해 서명자의 개인키를 사용하는 일련의 연산으로 구성되며, 서명 검증 과정은 전자서명 생성에 사용된 개인키에 대응하는 공개키를 사용하는 또 다른 일련의 연산으로 구성된다. 여기에서 전자서명 생성에 사용되는 서명자의 개인키를 서명키라고 하며, 전자서명 검증에 사용되는 서명자의 공개키를 검증키라고 한다. 서명키는 서명자만 알 수 있도록 비밀로 관리되어야 하고 검증키는 공개키 기반 구조를 통해 모든 사용자에게 공개된다. 사용자의 서명키와 검증키의 쌍인 전자 서명키는 모든 사용자에게 공통적으로 부여된 도메인 변수와 연계하여 생성되어야 하며, 전자서명의 생성 및 검증 또한 도메인 변수를 기반으로 정의된다.

부가형 전자서명 알고리즘은 전자 문서의 해시 코드에 공개키 연산을 적용하여 전자서명을 생성한다. 검증자는 수신된 서명 메시지와 전자서명을 대상으로 전자서명 생성에 사용된 것과 동일한 해시 함수와 서명자의 서명키에 대응하는 검증키를 사용하여 전자서명의 유효성을 확인한다.

본 표준에서는 부가형 전자서명 알고리즘의 일반적인 사용자 전자 서명키 생성 방법, 전자서명 생성과 검증 절차를 정의한다. 그러나 인증서를 포함한 사용자 전자 서명키와 도메인 변수의 관리는 공개키 기반 구조의 운용에 의존하는 사항이므로 본 표준에서는 다루지 않는다.

## 2 인용 표준

해당 사항 없음

## 3 용어 정의

### 3.1 검증키(Verification key)
전자서명을 검증하기 위하여 이용하는 전자적 정보

### 3.2 다변수 연립 이차 방정식(System of multivariate quadratic equations)
미지수가 2개 이상이고 미지수의 가장 높은 차수가 이차인 방정식으로 이루어진 연립 방정식

### 3.3 도메인 변수(Domain parameters)
특정 암호 운용 시스템(정보처리 시스템 또는 정보 통신망 환경)의 사용자들이 암호 알고리즘에 공통적으로 사용하는 변수

### 3.4 랭크(rank)
행렬에서 일차 독립인 행 벡터나 열 벡터들의 최대 개수

### 3.5 서명키(Signing key)
전자서명을 생성하기 위하여 이용하는 전자적 정보

### 3.6 아핀 변환(Affine transformation)
한 벡터 공간을 다른 벡터 공간에 대응시키고 직선과 거리의 비를 보존하는 변환. 선형 변환과 평행 이동 변환의 합성으로 이루어져 있음

### 3.7 유한체(Finite field)
덧셈에 대하여 군을 이루고, 덧셈의 항등원을 제외한 집합이 곱셈에 대하여 군을 이루는 집합

### 3.8 전자서명(Digital signature)
서명자를 확인하고 서명자가 전자 문서에 서명을 하였음을 나타내는데 이용하기 위하여 해당 전자 문서에 첨부되거나 논리적으로 결합된 전자적 형태의 정보

### 3.9 해시 함수(Hash function)
임의 길이 입력 데이터를 일정 길이 출력으로 반환하는 함수

## 4 약어

| | |
|---|---|
| MQ | Multivariate Quadratic Equations |
| EIP | Extended Isomorphism of Polynomials |
| MinRank | Minimum Rank |

## 5 기호

| | |
|---|---|
| $q$ | 소수 혹은 소수의 지수 승 |
| $F_q$ | $q$ 개의 원소를 갖는 유한체 |
| $F_q^m$ | $F_q$의 $m$개의 곱집합 |
| $F \circ G$ | 함수 혹은 아핀 변환 $F$ 와 $G$ 의 합성 |
| $M_{n\times n}(F_q)$ | 유한체 $F_q$ 에서 정의된 $n \times n$ 행렬들의 집합 |

## 6 양자내성암호

양자내성암호란 양자컴퓨터에 안전하다고 알려진 수학적 난제에 기반을 둔 공개키 암호 알고리즘을 칭하는 것으로 크게, 격자문제 기반, 다변수 이차식 기반, 코드문제 기반, 해시 함수 기반, 아이소지니(isogeny) 기반 등으로 구분되어 연구가 진행되고 있다.

현재, 소인수분해 문제와 이산로그문제를 다항식 시간 안에 풀어주는 Shor 알고리즘과 검색의 복잡도를 반 이하로 줄여주는 Grover 알고리즘이 양자알고리즘으로 알려져 있다. 양자내성암호는 알려진 양자알고리즘에 안전하고, 기반이 되는 수학적 난제를 풀어주는 효율적인 전용 양자알고리즘이 존재하지 않은 암호를 의미한다.

## 7 다변수 이차식 기반 난제

본 표준에서 제안하는 다변수 이차식 기반 전자서명알고리즘의 안전성은 다변수 연립 이차 방정식의 난제인 MQ-문제, EIP-문제와 MinRank-문제의 어려움에 기반한다. 이 장에서는 다변수 연립 이차 방정식의 난제인 MQ-문제, EIP-문제와 MinRank-문제의 정의에 대해 기술한다.

### 7.1 MQ-문제

MQ-문제는 유한체 위에서 정의된 다변수 연립 이차 방정식의 해를 구하는 문제이다. 유한체 $F_q$ 상에서 정의된 변수 $x_1, \dots, x_n$에 대한 $m$개의 이차식 $P(x_1, \dots, x_n) = (P^{(1)}(x_1, \dots, x_n), \dots, P^{(m)}(x_1, \dots, x_n))$과 $y = (y_1, \dots, y_m) \in F_q^m$가 주어져 있을 때, $P^{(1)}(x_1', \dots, x_n') = y_1, \dots, P^{(m)}(x_1', \dots, x_n') = y_m$을 만족하는 해 $(x_1', \dots, x_n') \in F_q^n$을 구

하는 문제이다. 이 문제는 $\mathbb{F}_2$를 포함한 유한체 위에서 NP-complete임이 증명이 되었다. 그러나, $n$이 $m$ 보다 아주 크거나 아주 작은 경우, 다항식 시간에 풀 수 있는 알고리즘이 알려져 있다.

### 7.2 EIP-문제

특별한 다변수 이차 이상의 연립 방정식의 집합인 $C$에 속한 $F$와 가역인 아핀 변환 $S$, $T$에 대해서 $P = S \circ F \circ T$로 만들어진 $P$가 주어져 있을 때, $P = S' \circ F' \circ T'$을 만족하는 다른 $F' \in C$와 아핀 변환 $S'$, $T'$을 찾는 문제이다.

### 7.3 MinRank 문제

자연수 $k$에 대해, $(M_1, ..., M_k)$를 $M_{n \times n}(F_q)$의 행렬들이 주어져 있을 때, 자연수 $r$에 대해, MinRank 문제는, 랭크가 $r$ 이하인 선형 결합을 찾는 것이다. 즉, 다음 식을 만족하는 $F_q^k$의 원소인 벡터 $\lambda = (\lambda_1, ..., \lambda_k)$를 찾는 문제이다.

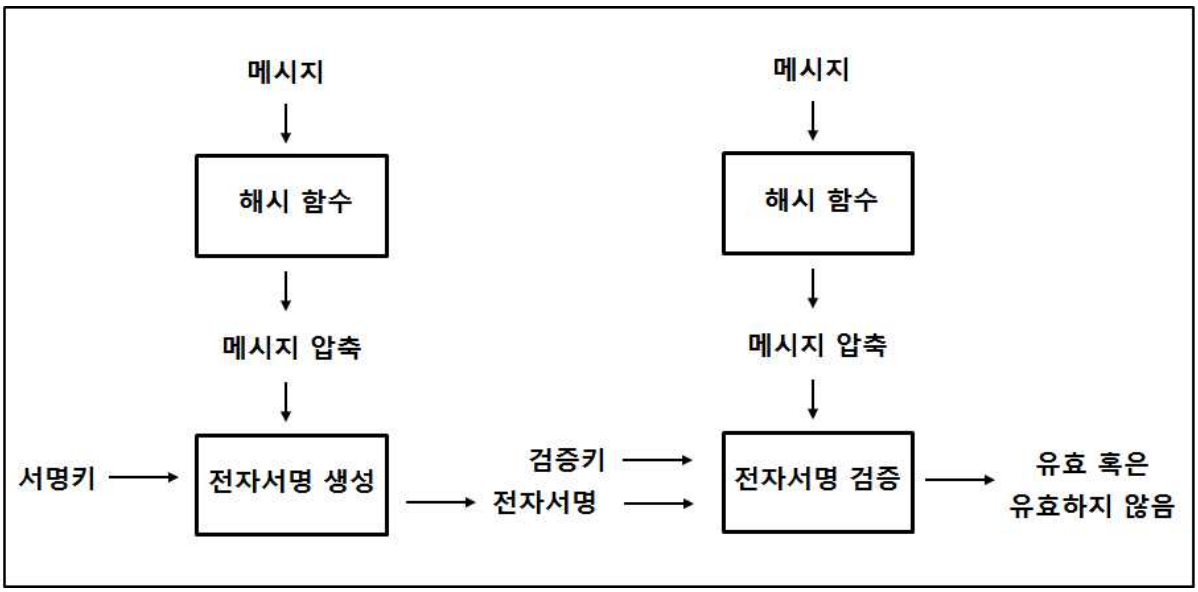
$$Rank( \sum_{i=1}^{k} \lambda_i M_i ) \leq r$$

유한체에서 이 문제는 NP-complete임이 증명되어 있다.

## 8 부가형 전자서명 알고리즘

본 장에서는 부가형 전자서명 알고리즘의 일반적인 서명키, 검증키 생성 알고리즘, 서명 생성 알고리즘과 서명의 검증 알고리즘을 기술한다.

그림 1. 전자서명 알고리즘 수행 과정



### 8.1 키 생성 알고리즘

키 생성 알고리즘은 사용자의 서명키와 검증키를 생성하는 알고리즘으로 도메인 파라미터와 필요하다면 사용자가 선택한 랜덤 값을 입력 값으로 주고 서명키와 검증키를 출력 값으로 주는 알고리즘이다.

### 8.2 전자서명 생성 알고리즘

전자서명을 생성 알고리즘은 키 생성 알고리즘에서 생성한 서명키와 메시지를 입력 값으로 이용하여 서명을 생성하여 메시지와 서명 값을 출력하는 알고리즘이다.

### 8.3 전자서명 검증 알고리즘

전자서명 검증 알고리즘은 사용자 검증키, 메시지와 전자서명 값을 입력 값으로 이용하여 특정한 검증 식을 통해 서명의 유효성을 판정한 결과를 출력하는 알고리즘이다.

# 부 록 Ⅰ-1

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

# 지식재산권 확약서 정보

## Ⅰ-1.1 지식재산권 확약서

해당 사항 없음

※ 상기 기재된 지식재산권 확약서 이외에도 본 표준이 발간된 후 접수된 확약서가 있을 수 있으니, TTA 웹사이트에서 확인하시기 바랍니다.

# 부 록 Ⅰ-2

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

# 시험인증 관련 사항

## Ⅰ-2.1 시험인증 대상 여부

해당 사항 없음

## Ⅰ-2.2 시험표준 제정 현황

해당 사항 없음

# 부 록 Ⅰ-3

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

## 본 표준의 연계(family) 표준

해당 사항 없음

# 부 록 Ⅰ-4

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

## 참고 문헌

해당 사항 없음

# 부 록 Ⅰ-5

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

# 영문표준 해설서

해당 사항 없음

# 부 록 Ⅰ-6

(본 부록은 표준을 보충하기 위한 내용으로 표준의 일부는 아님)

## 표준의 이력

| 판수 | 채택일 | 표준번호 | 내용 | 담당 위원회 |
|---|---|---|---|---|
| 제1판 | 2019.12.XX | 제정<br>TTAK.KO-12.00xx | - | 정보보호 기반 프로젝트그룹 (PG501) |