특집 03

NIST 양자내성암호 표준공모전 제출물 분석 및 향후 연구전망

박태환 (부산대학교), 서화정 (한성대학교), 김호원 (부산대학교)

목 차

1. 서 론

최근 양자컴퓨터 기술의 발전으로 인해, 2017년 17 Q-bit 기반의 양자컴퓨터가 개발된 상황이며, 양자컴퓨터와 관련된 Shor 알고리즘 및 Grover 알고리즘의 특성으로 인해 기존 공개키 기반 암호와 대칭키 기반 암호의 보안 안전성 문제가 발생할 것으로 예상되고 있다. 이러한 문제점을 해결하고자 전 세계적으로 많은 암호학자 및 수학자들에 의해, 양자컴퓨터 환경에서도 안전성과 보안성을 제공할 수 있는 양자내성암호(Post-Quantum Cryptography) 분야의 연구가 활발히 이루어지고 있다. 이러한 연구와 더불어 미국 국립 표준 기술원(NIST, National Institute Standard Technology)에서는 2012년부터 격주로 양자내성암호 세미나를 개최하였으며, 2015년부터는 NIST PQC Workshop으로 확대하여 개최하고 있다. 이를 통해 양자내성암호에 대한 표준 공모전을 준비하여 2016년 PQCrypto 2016에서 양자내성암호 표준 공모전에 대한 발표가 있었으며, 2017년 11월 30일자로 양자내성암호 표준공모전 후보군 제출을 마감한 상태이며, 올해 4월 후보군 제출자들과 NIST 간의 워크숍이 열릴 예정이며, 최종 표준 확정은 2023년에서 2025년 사이로 예상되고 있다.

미국 NIST의 양자내성암호 표준공모전은 기존의 AES, SHA-2/SHA-3 표준 공모전과 달리 하나의 표준 암호 제정이 아닌 다양한 환경에서 다양한 유형의 안전성과 효율성을 갖춘 양자내성암호 표준 후보군 제정에 그 목적을 두고 있으며, 양자내성암호 표준 확정 이후, 응용 및 활용성 강화 측면에서 각 후보군들의 응용 및 활용성 또한 고려될 것으로 보인다. 이에 따라 미국 NIST 양자내성암호 표준 공모전 제출물들에 대한 분석과 분석 결과를 바탕으로 향후 연구 진행을 통해 연구 및 기술 경쟁력 확보가 필요할 것으로 보인다. 본 논문에서는 미국 NIST 양자내성암호 표준 공모전에 제출된 제출물들에 대한

동향 분석과 양자내성암호 유형별 대표 제출물 특성 분석 결과를 제시하며, 분석 결과를 바탕으로 향후 연구 전망을 제시하고자 한다.

2. NIST 양자내성암호 표준공모전 제출물 분석

본 장에서는 NIST 양자내성암호 표준공모전 제출물에 대해 통계적 분석과 양자내성암호 유형별 대표 제출물에 대한 분석 결과를 제시하고자 한다. 기존에 알려진 양자내성암호의 유형은 격자 기반(Lattice Based), 코드 기반(Code Based), 다변수 기반(Multivariate Based), Isogeny 기반(Isogeny Based), 해시 기반(Hash Based)이 있다. 하지만 실제 NIST 양자내성암호 표준공모전 제출물 유형에 있어서 기존에 알려진 양식이 아닌 다른 유형과 기존 공개키 암호 방식의 개선안들이 포함되어있다.

2018년 2월 기준으로 NIST 양자내성암호 표준 공모전에 총 66건이 제출되었으며, 이 중 3건은 Withdraw가 된 상태이다. 제출된 66건에 대해 양자내성암호 유형별로 분석한 경과, 격자 기반(Lattice Based)이 가장 많은 26건이 있었으며, 코드 기반(Code Based)이 20건, 다변수 기반(Multi-variate Based) 9건, 해시 기반(Hash Based) 3건, Isogeny 1건, 기타 유형 7건으로 확인되었다. 이를 통해, 격자 기반(Lattice Based)과 코드 기반(Code Based) 가장 많은 유형을 차지하고 있다는 것을 확인할 수 있다.

양자내성암호의 방식의 경우, 전자 서명 기법이 21건, KEM (Key Encapsulation Mechanism), 키 교환 및 암/복호화 유형이 45건으로 확인되었다. 이를 통해, 전자서명과 KEM/키 교환 방식이 유형의 주를 이루는 것으로 확인되었다.

NIST 양자내성암호 표준 공모전 제출 건에 대해 참여한 국가별 분포를 분석한 경과, 미국이 총 22건에 참여하였으며, 프랑스가 15건, 네덜란드가 9건에 참여한 것으로 확인되었으며, 한국의 경우, 다른 국가와의 협업 방식이 아닌 독자 제안 방식으로 5건이 제출된 것으로 확인되었으며, 해당 수치는 일본, 캐나다, 벨기에와 동일한 수치이며, 4번째로 많은 제출 건에 기여한 국가인 것으로 확인되었다. 한국에서 제출한 5건에 대해 분석한 결과, 격자 기반(Lattice Based) 2건(KEM, 암/복호화 유형), 코드 기반(Code Based) 2건(전자서명 1건, 암/복호화 1건), 다변수 기반(Multi-variate Based) 1건(전자서명)으로 확인되었다.

다음으로는 제출물의 유형별 대표 제출물에 대해 분석한 결과를 설명한다.

2.1 격자 기반(Lattice Based) 양자내성암호 대표 제출물 분석

격자 기반(Lattice Based) 양자내성암호는 격자(Lattice) 상의 문제를 해결하는 것이 NP-hard 문제임에 기반으로 보안성을 제공하는 암호시스템 유형을 말한다.

격자 기반(Lattice Based) 양자내성암호의 대표적인 제출물인 CRYSTALS-Dilithium [1]은 독일 보훔(Bochum)대와 미국 SRI international, 스위스의 IBM Research, 네덜란드 Radbound 대학, 프랑스 ENS de Lyon이 같이 제출한 격자 기반 (Lattice-Based) 전자서명 방식으로써, 격자 상에서의 short vector를 찾기 어려운 문제에 기반하고 있다. 제안 기법은 “Fiat-Shamir with Aborts” 접근 방식을 기반으로 설계되었으며, 효율성을 위해, SHAKE-128 (암/복호화 시 사용), SHAKE-256(서명 기법 시 사용)을 사용하였으

	I weak	II medium	III recommended	IV very high
q	8380417	8380417	8380417	8380417
d	14	14	14	14
weight of c	60	60	60	60
$\gamma_1 = (q-1)/16$	523776	523776	523776	523776
$\gamma_2 = \gamma_1/2$	261888	261888	261888	261888
(k, ℓ)	$(3, 2)$	$(4, 3)$	$(5, 4)$	$(6, 5)$
η	7	6	5	3
β	375	325	275	175
ω	64	80	96	120
pk size (bytes)	896	1184	1472	1760
sig size (bytes)	1487	2044	2701	3366
Exp. reps (from Eq. (5))	4.3	5.9	6.6	4.3

(그림 1) Dilithium 파라미터

며, 제안 기법의 권고 수준의 보안강도를 가질 경우, 서명의 크기는 2.7KB, 공개키는 1.5KB의 크기를 가지는 것으로 확인되었다. 제안 기법의 파라미터 및 파라미터 별 공개키/서명 크기는 아래의 그림과 같다.

Dilithium의 보안강도별 성능 평가 결과는 아래와 같으며, 서명 생성 과정이 서명 검증 과정보다 오래 걸린다는 것을 확인 할 수 있었다. Dilithium의 가장 높은 보안강도의 경우, 키 생성에 512,116 cycles(ANSI C), 292,404 cycles (AVX2)가 걸리며, 서명 생성과정의 경우, 1,677,782 cycles(ANSI C), 711,018 cycles (AVX2)가 소요되며, 검증 과정은 548,558 cycles, 288,398 cycles가 소요되는 것으로 확인되었다.

2.2 코드 기반(Code Based) 양자내성암호 대표 제출물 분석

코드 기반 (Code Based) 양자내성암호는 일반적인 Linear Code를 Decoding하는 것이 NP-hard 문제임에 기반으로 보안성을 제공하는 암호시스템의 유형을 의미한다.

대표적인 코드 기반(Code Based) 양자내성암호 제출물에는 Classic McEliece가 있다. Classic McEliece [2]는 고 보안강도를 제공함과 동시에 IND-CCA2 보안성 제공을 위해 설계된 KEM 방식이며, Binary Goppa code를 사용하는 McEliece의 Niederreiter's dual version 기반으로 OW-CPA 보안성을 위해 설계된 PKE 기반 방식을 제공한다. 제안 방식에서는 2가지의 파라미터가 있으며, 관련 파라미터는 아래의 표과 같다.

NIST Security Level	-	1	2	3
Gen cycles (Haswell)	169,972	269,844	382,756	512,116
Sign cycles (Haswell)	765,442	1,285,476	1,817,902	1,677,782
Verify cycles (Haswell)	196,048	296,920	395,936	548,558
Gen cycles (AVX2, Haswell)	104,128	156,432	225,432	292,404
Sign cycles (AVX2, Haswell)	338,922	493,332	673,144	711,018
Verify cycles (AVX2, Haswell)	105,584	150,228	207,164	288,398

(그림 2) Dilithium 성능 평가 결과 (AVX2 SIMD 미적용/적용, Haswell 환경)

〈표 1〉 Classic McEliece 파라미터

제안방식 유형	m	n	t	l	해시함수
kem/mceliece6960119	13	6960	119	256	SHAKE256
kem/mceliece8192128	13	8192	128	256	SHAKE256

Classic McEliece의 성능 평가는 소프트웨어와 하드웨어 2종으로 제시되고 있다. 소프트웨어 성능 평가의 경우, GCC 컴파일러를 활용하여 -march=native-mtune=native-O3 -fomit-frame-pointer-fwrapv 옵션으로 컴파일된 소스에 대한 성능을 평가하였으며, 각 수행에서 31 timing의 중간 값을 성능치로 평가가 진행되었다. mceliece8192128의 경우, Encapsulation 과정에 첫 번째 수행에서는 296036 cycles, 두 번째에서는 295392cycles, 세 번째에서는 295932 cycles가 소요되는 것으로 확인되었으며, De-capsulation의 경우, 3회의 수행에 대해 각각 458556cycles, 458476 cycles, 458340 cycles가 소요되며, 키 생성 과정은 수십억 cycles가 소요되는 것으로 확인되었으며, 중간치로 각각 4010278828 cycles, 6008245724 cycles(약 2초), 4005886024 cycles가 소요되는 것으로 확인됨. 각 키 생성과정은 약 20억 cycles 정도 소요되는 것으로 확인되었다.

하드웨어 성능 평가의 경우, 중간 크기의 Altera Straix V FPGA (5SGXEA7N) 상에서 synthesize 및 성능 평가가 이루어졌다. mceliece8192128의 경우, 231MHz 동작 주파수 상에서 키 생성 과정은 1173750 cycles (5.08ms), Decoding 과정은 17140 cycles (0.074ms)가 소요되는 것으로 확인되었으며, mceliece6960119의 경우, 248MHz 동작 주파수 상에서 키 생성 과정은 966400 cycles (3.58ms), Decoding 과정은 17055 cycles (0.060ms)가 소요되는 것으로 확인 되었다. 하드웨어 면적의 경우, mceliece8192128이 227,750 레지스터 (flip-flops), 129,059 ALMs (가능한 로직 자원의 55%), 1,126 RAM blocks (가능한 on-chip RAM의 44%), 4개의 DSP 블록(가능한 DSP의 1.6%)이 필요한 것으로 확인되었고, mceliece6960119의 경우, 223,232 registers (flip-flops), 121,806 ALMs (가능한 로직 자원의 52%), 961 RAM blocks (가능한 on-chip RAM의 38%), 6 DSP blocks (가능한 DSP의 2.3%)가 필요한 것으로 확인되었다(키 생성부분과 decoding부분만 포함된 면적).

제안 기법에서의 입/출력의 크기는 아래의 표와 같다.

2.3 다변수 기반(Multi-variate Based) 양자내성암호 대표 제출물 분석

다변수 기반(Multi-variate-Based) 양자내성암호는 유한체에서 다변수 함수를 푸는 것이 NP-hard문제인 것에 기반으로 보안성을 제공하는 암호시스템 유형을 말하며, 대표적인 제출물

〈표 2〉 Classic McEliece의 유형별 공개키/비밀키/암호문/세션키 크기 비교

제안기법 유형	공개키 크기(byte)	비밀키 크기(byte)	암호문 크기(byte)	세션키 크기(byte)
mceliece8192128	1357824	14080	240	32
mceliece6960119	1047319	13908	226	32

은 Rainbow가 있다. 표준 공모전에 제출된 Rainbow [3]는 기존 Rainbow 전자 서명 기법을 수정 변경한 방식이다. 제안 기법의 파라미터와 파라미터 별 공개키, 개인키, 해시 크기, 서명 크기는 아래의 그림과 같으며, 제안 기법의 파라미터 중 가장 높은 보안강도를 제공하는 VIb 파라미터를 사용하는 경우, 공개키는 1,321KB, 비밀키는 922.4KB, 서명 크기는 128bit salt값을 포함하여 1,176bit가 소모되는 것으로 확인되었다.

제안 기법의 소프트웨어 성능 평가에서 가장 높은 보안강도를 제공하는 VIb 파라미터를 사용하는 경우, 키 생성과정에 49,906ms (ANSI C), 1,066ms (AVX2)이 소요되며, 서명 생성 과정은 5.077ms (ANSI C), 1.108ms (AVX2)가 걸리며, 서명 검증 과정의 경우, 3.401ms(ANSI C), 1.421ms (AVX2) 가 걸리는 것으로 확인되었다.

2.4 Isogeny 기반(Isogeny Based) 양자내성암호 대표 제출물 분석

Isogeny 기반 양자내성암호는 Order가 같은 두 타원곡선 사이에 존재하는 Isogeny를 구하는 것이 NP-hard 문제임에 기반으로 보안성을 제공하는 암호시스템 유형을 의미한다. 이번 NIST 양자내성암호 표준 공모전에는 SIKE (Supersingular Isogeny Key Encapsulation) 1건이 제출되었다.

SIKE [4]는 미국 마이크로소프트(MS)사를 중심으로 제안된 Supersingular Isogeny Key Encapsulation(SIKE) 기법을 의미하며, Supersingular Isogeny Diffie-Hellman(SIDH)를 기반으로 한 키 교환 기법에 해당된다. 제공 방식은 IND-CPA KEM과 IND-CCA KEM 방식이 있다. 제안 기법의 성능 평가의 경우, 제안 기법에 대한 성능 평가를 위해 제안자들은 GMP 라이브러리를 활용한 레퍼런스 코드, portable C 기반의 최적화 구현, x64 assembly 기반의 최적화 구현, ARM64환경에 대해 ARMv8 assembly 기반의 최적화, FPGA와 ASIC을 위한 VHDL모델(속도 최적화)을 제시하고 있다. 제안 기법에 대한 최적화 구현의 경우, F_{p^2} 상에서의 효율적 연산을 위해 Karatsuba and lazy reduction을 사용하였고, fully roled 버전의 Comba, Montgomery reduction을 사용하였음. x64 환경상에서는 MULX, ADX 명령어 이용 가능성으로 인해 Comba 곱셈보다 Schoolbook 곱셈이 더 좋은 성능을 보이는 것으로 확인되었으며, 제안 기

parameter set	parameters $(\mathbb{F}, v_1, o_1, o_2)$	public key size (kB)	private key size (kB)	hash size (bit)	signature size (bit) [1]
Ia	(GF(16),32,32,32)	148.5	97.9	256	512
Ib	(GF(31),36,28,28)	148.3	103.7	268	624
Ic	(GF(256),40,24,24)	187.7	140.0	384	832
IIIb	(GF(31),64,32,48)	512.1	371.4	384	896
IIIc	(GF(256),68,36,36)	703.9	525.2	576	1,248
IVa	(GF(16),56,48,48)	552.2	367.3	384	736
Vc	(GF(256), 92,48,48)	1,683.3	1,244.4	768	1,632
VIa	(GF(16), 76,64,64)	1,319.7	871.2	512	944
VIb	GF(31), 84,56,56)	1,321.0	922.4	536	1,176

[1] 128 bit salt included

(그림 3) Rainbow 파라미터 별 키/서명 크기

Scheme	KeyGen (stack)	Encaps (stack)	Decaps (stack)	static library	
				speed (-03)	size (-0s)
Reference Implementation					
SIKEp503	512	762	1528	107,450	96,386
SIKEp751	2880	1332	2280	107,450	96,386
SIKEp964	3744	2262	2936	107,450	96,386
Optimized Implementation					
SIKEp503	8,040	8,632	9,464	122,612	60,020
SIKEp751	13,864	14,024	14,680	167,508	61,404
Additional implementation using x64 assembly					
SIKEp503	8,120	8,520	8,952	132,688	62,488
SIKEp751	14,032	14,176	14,944	188,720	67,080

(그림 4) SIKE S/W 속도 메모리 사용량 평가 (단위: 1,000 cycles, bytes)

법에서 사용하는 소수 $p = 2^{e_2}3^{e_3} - 1$에 대해 최적화된 Montgomery reduction을 구현하여 사용하였다. x64 Assembly로 최적화 구현된 SIKEp751의 경우, 키 생성과정에 30,919(1000 cycles)이 소요되며, En-capsulation과 De-capsulation 과정은 총 103,852(1000 cycles)가 소요되는 것으로 확인되었다. 제안 기법에 대한 레퍼런스, 최적화 및 x64 assembly 구현물의 메모리 사용량은 아래의 그림과 같음. SIKE의 메모리 사용량에서 stack 사용량은 레퍼런스 코드가 가장 적게 소모되는 것으로 확인되었고, static library 크기의 경우, 최적화 구현 결과물이 가장 적게 소모되는 것(-Os 컴파일 옵션)으로 확인되었다.

2.5 해시 기반(Hash Based) 양자내성암호 대표 제출물 분석

해시 기반 양자내성암호는 해시 함수의 안전성에 기반으로 보안성을 제공하는 전자서명 시스템 유형을 의미한다. 대표적인 제출물로는 SPHINCS+ [5]가 있다. SPHINCS+는 기존에 연구된 SPHINCS와 유사한 과정을 수행하지만, 기존 대비 Multi-target 공격에 대한 방어가 가능하며, Tree-less WOTS+ 수행 및 FORS key pair를 사용함으로써 $k2^a$ bit message digest에 대한 서명이 가능하며, Verifiable index selection 기

	n	h	d	$\log(t)$	k	w	bitsec	sec level	sig bytes
SPHINCS$^+$-128s	16	64	8	15	10	16	133	**1**	8 080
SPHINCS$^+$-128f	16	60	20	9	30	16	128	**1**	16 976
SPHINCS$^+$-192s	24	64	8	16	14	16	196	**3**	17 064
SPHINCS$^+$-192f	24	66	22	8	33	16	194	**3**	35 664
SPHINCS$^+$-256s	32	64	8	14	22	16	255	**5**	29 792
SPHINCS$^+$-256f	32	68	17	10	30	16	254	**5**	49 216

(그림 5) SPHINCS+ 파라미터

	public key size	secret key size	signature size
SPHINCS$^+$-128s	32	64	8 080
SPHINCS$^+$-128f	32	64	16 976
SPHINCS$^+$-192s	48	96	17 064
SPHINCS$^+$-192f	48	96	35 664
SPHINCS$^+$-256s	64	128	29 792
SPHINCS$^+$-256f	64	128	49 216

(그림 6) SPHINCS+ 키, 서명 크기(단위:byte)

능을 제공한다. 제안 기법의 파라미터 값 및 파라미터별 키, 서명크기는 아래의 그림과 같다.

SPHINCS+의 성능평가는 Intel x86-64환경 상에서 수행되었다(-O3 옵션). 성능 평가는 아래의 그림과 같으며, 다양한 해시함수를 사용하여 성능 측정하였다. 특히 Haraka의 경우, AES 암호 활용이 필요한 구조로써, Intel AES-NI 기반의 하드웨어 가속기 활용 성능 또한 제시하고 있다.

2.6 기타 유형의 양자내성암호 대표 제출물 분석

기타 유형의 양자내성암호로는 메르센 소수를 활용한 Mersenne-756839 기법 [6]과 기존의 RSA 공개키 암호에 대해 양자컴퓨터 환경에 따른 소수 및 파라미터 크기 확장을 통한 암/복호화 및 서명 기법 [7, 8]들을 제시하고 있다. 하지만 이러한 새로운 유형의 경우, 안전성 관점에서 많은 연구가 되어 있지 않기 때문에 양자컴퓨터 환경 상에서의 안전성에 대한 연구가 필요할 것

	key generation	signature generation	verification
SPHINCS$^+$-SHAKE256-128s	617 619 732	8 610 599 004	10 222 936
SPHINCS$^+$-SHAKE256-128f	19 348 784	580 904 788	24 826 884
SPHINCS$^+$-SHAKE256-192s	907 587 276	17 586 416 344	15 036 680
SPHINCS$^+$-SHAKE256-192f	28 200 752	757 001 640	40 338 224
SPHINCS$^+$-SHAKE256-256s	1 210 939 356	13 842 403 104	20 889 204
SPHINCS$^+$-SHAKE256-256f	75 031 996	1 664 510 764	41 469 276
SPHINCS$^+$-SHA-256-128s	307 425 484	4 606 958 168	5 514 124
SPHINCS$^+$-SHA-256-128f	9 625 644	302 359 220	12 901 012
SPHINCS$^+$-SHA-256-192s	576 727 832	12 239 247 980	10 740 192
SPHINCS$^+$-SHA-256-192f	17 902 436	487 388 724	26 456 352
SPHINCS$^+$-SHA-256-256s	1 095 050 628	12 893 347 756	19 141 296
SPHINCS$^+$-SHA-256-256f	68 819 608	1 558 148 364	38 316 192
SPHINCS$^+$-Haraka-128s	917 405 356	16 992 635 344	19 360 272
SPHINCS$^+$-Haraka-128f	28 814 020	1 056 761 824	45 964 624
SPHINCS$^+$-Haraka-192s	1 244 530 184	38 062 259 596	27 243 200
SPHINCS$^+$-Haraka-192f	42 782 840	1 276 694 620	69 760 728
SPHINCS$^+$-Haraka-256s	1 817 324 180	28 860 355 888	42 380 420
SPHINCS$^+$-Haraka-256f	113 876 252	3 172 247 452	76 203 004

(그림 7) SPHINCS + 성능 평가 결과 (단위: cycles)

으로 보인다.

3. 양자내성암호 향후 연구전망

앞선 장에서 살펴본 미국 NIST 양자내성암호 표준 공모전에 제출한 유형별 대표적인 제출물 분석 결과를 바탕으로 향후 양자내성암호 연구는 다양한 사물인터넷용 디바이스 환경 상에서의 최적화 구현 연구 및 하드웨어 최적화 구현 연구가 필요할 것으로 보이며, 유형별 부채널 공격 관점 상에서의 안전도와 대응방안 연구 또한 동시에 필요할 것으로 보인다. 이러한 구현 및 공격 관점에서의 연구 이후에는 연구결과물들에 대해 각종 응용 단에서의 적용 및 적용 시 발생할 수 있는 문제 해결을 위한 연구가 필요할 것으로 보인다.

4. 결 론

본 논문에서는 최근 미국 NIST 양자내성암호 표준 공모전 1차 라운드 제출물에 대한 유형/방식 등 통계적 분석 결과와 양자내성암호 유형별 대표적인 제출물에 대한 분석 결과를 제시하고 있다. 이러한 분석 결과를 바탕으로 향후 양자내성암호 연구에 대한 연구전망을 제시하였다. 본 논문의 결과는 향후 양자내성암호 연구 분야에서의 연구 기술력 및 국가 경쟁력 확보에 있어서 기초자료로써, 많은 도움이 될 것으로 기대된다.

참 고 문 헌

[1] V. Lyubashevsky, L. Ducas, E. Kiltz, T. Lepoint, P. Schwabe, G. Seiler, D. Stehle, Crystals-dilithium, Tech. rep., National Institute of Stan- dards and Technology, available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions (2017).

[2] D. J. Bernstein, T. Chou, T. Lange, I. von Maurich, R. Misoczki, R. Niederhagen, E. Persichetti, C. Peters, P. Schwabe, N. Sendrier, J. Sze- fer, W. Wang, Classic mceliece, Tech. rep., National Institute of Standards and Technology, available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions (2017).

[3] J. Ding, M.-S. Chen, A. Petzoldt, D. Schmidt, B.-Y. Yang, Rainbow, Tech. rep., National Institute of Standards and Technology, available at https://csrc.nist.gov/projects/post-quantum-cryptography/ round-1-submissions (2017).

[4] D. Jao, R. Azarderakhsh, M. Campagna, C. Costello, L. D. Feo, B. H. A. Jalali, B. Koziel, B. LaMacchia, P. Longa, M. Naehrig, J. Renes, V. Soukharev, D. Urbanik, Sike, Tech. rep., National Institute of Standards and Technology, available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions (2017).

[5] A. Hulsing, D. J. Bernstein, C. Dobraunig, M. Eichlseder, S. Fluhrer, S.-L. Gazdag, P. Kampanakis, S. Kolbl, T. Lange, M. M. Lauridsen, F. Mendel, R. Niederhagen, C. Rechberger, J. Rijneveld, P. Schwabe, Sphincs+, Tech. rep., National Institute of Standards and Technology, available at https://csrc.nist.gov/projects/post-quantum-cryptography/round-1-submissions (2017).

[6] D. Aggarwal, A. Joux, A. Prakash, M. Santha, Mersenne-756839, Tech. rep., National Institute of Standards and Technology, available at https://csrc.nist.gov/projects/post-quantum-cryptography/ round-1-submissions (2017).

[7] D. J. Bernstein, J. Fried, N. Heninger, P. Lou,

L. Valenta, Post-quantum rsa-encryption, Tech. rep., National Institute of Stan- dards and Technology, available at https://csrc.nist.gov/projects/ post-quantum-cryptography/round-1-submissions (2017).

[8] D. J. Bernstein, J. Fried, N. Heninger, P. Lou, L. Valenta, Post-quantum rsa-signature, Tech. rep., National Institute of Stan- dards and Technology, available at https://csrc.nist.gov/projects/ post-quantum-cryptography/round-1-submissions (2017).

저 자 약 력

박 태 환

이메일 : pth5804@pusan.ac.kr

- 2013년 부산대학교 정보컴퓨터공학부 (학사)
- 2013년~현재 부산대학교 전기전자컴퓨터공학과 (석, 박사 통합과정)
- 관심분야 : 암호화 S/W 구현, IoT 디바이스 보안, 양자내성 암호

서 화 정

이메일 : hwajeong84@gmail.com

- 2010년 부산대학교 컴퓨터공학과 (학사)
- 2012년 부산대학교 컴퓨터공학과 (석사)
- 2016년 부산대학교 컴퓨터공학과 (박사)
- 2015년 4월~5월 싱가포르 난양공대 인턴쉽
- 2016년 1월~2017년 3월 싱가포르 과학기술청 연구원
- 2017년 4월~현재 한성대학교 조교수
- 관심분야 : 정보보호, 암호화 구현, IoT

김 호 원

이메일 : howonkim@pusan.ac.kr

- 1993년 경북대학교 전자공학과 학사 졸업
- 1995년 포항공과대학교 전기전자공학과 석사 졸업
- 1999년 포항공과대학교 전기전자공학과 박사 졸업
- 2008년 한국전자통신연구원 정보보호연구단 선임연구원/팀장
- 2008년 3월~현재 부산대학교 전기컴퓨터공학부 정교수
- 관심분야 : 스마트그리드 보안, RFID/USN 정보보호 기술, PKC 암호, VLSI 설계, Embedded system 보안, IoT 보안