정 보 보 호 학 회 지
제 33 권 제3호, 2023. 6

양자내성암호 특허동향

강 민 성*

요 약

양자컴퓨터의 개발이 가속화됨에 따라 기존의 공개키 암호에서 양자내성암호로 시급하게 전환해야 하는 상황이다. 이러한 상황을 가장 신속하게 대응하고 있는 미국은 NIST를 통해 양자내성암호로의 전환을 위한 표준화를 진행하고 있으며, 표준화 대상 알고리즘까지 선정한 상황이다. 그 외 일본, 중국, 및 유럽의 각국도 양자내성암호 기술을 확보하기 위해 많은 투자를 하고 있다. 본 고에서는 양자내성암호의 국적 및 세부기술별 특허출원 동향을 살펴보고, 나아가 양자내성암호의 구현특허 출원 동향도 함께 분석한다.

Ⅰ. 서 론

양자 컴퓨터의 개발은 국방·안보, 제조·반도체, 의료·제약·소재, 금융, 교통·물류 등 전 산업 분야에 막대한 영향을 미칠 것으로 예측된다[1]. 이러한 양자컴퓨터의 무한한 가능성에 글로벌 빅테크들은 양자컴퓨터 개발에 막대한 투자를 하고 있으며, 가장 선두에 있는 기업이 구글과 IBM이다.

구글은 ‘19년 슈퍼컴퓨터의 경우 만년이 걸리는 연산을 53큐비트 프로세서(시카모어)로 단 200초 만에 수행할 수 있는 양자 우월(Quantum supremacy)을 달성했음을 공표하였다[2]. IBM은 ‘23년까지 1,121큐비트 양자 프로세서(콘도르)의 개발을 예고했으며, 나아가 2026년 이후에는 양자 오류 정정까지 제공하는 1만~10만 큐비트 양자 프로세서를 개발한다는 기술로드맵도 공개했다[3]. 구글과 IBM이 양자컴퓨터 개발에 적극적으로 나서고 있다는 점은 관련 특허출원으로부터도 확인할 수 있는데, 특허청 분석에 따르면 ’10년부터 ‘19년까지 양자컴퓨터 관련 특허출원(2,572건) 중에 IBM(408건)과 구글(233건)이 25%를 차지했다[1,4].

글로벌 빅테크들의 적극적인 투자로 양자컴퓨터 개발의 속도가 가속화됨에 따라 소인수 분해 문제 등을 기반으로 하는 공개키 암호를 양자내성암호로 시급하게 전환해야 하는 상황이다[5,6]. 미국은 양자내성암호로의 전환을 가장 신속하게 준비하고 있으며, ’16년부터 NIST를 통해 양자내성암호 표준화 공모전을 진행하여 양자내성암호 세분기술인 격자 기반 암호, 코드 기반 암호, 다변수 암호, 해시 기반 암호, 타원곡선 아이소제니 기반 암호 중에서 격자 기반 암호와 해시 기반 암호를 첫 번째 표준화 대상으로 선정했다[7].

본 고에서는 양자내성암호 관련 특허출원 동향을 알아본다. Ⅱ.장에서 양자내성암호 국적별, 세부기술별, 다출원인 특허출원 동향을 살펴보고, Ⅲ.장에서는 양자내성암호 구현에 관한 특허출원 동향을 분석한다. Ⅳ.장에서는 본 고의 결론을 제시한다.

Ⅱ. 양자내성암호 특허출원 동향

2장에서는 특허청에서 분석한 양자내성암호 관련 특허출원 1,268건을 국적별, 세부기술별, 및 다출원인으로 나눠서 살펴본다[8].

2.1. 양자내성암호 국적별 특허출원

특허청 분석에 따르면 양자 내성 암호 관련 특허는 ‘11년부터 ’20년까지 연평균 17.3%씩 증가해 총 1,268건 출원되었다[8]. 특히, NIST가 양자내성암호의 표준화를 선언한 ‘16년 이후 양자내성암호 특허출원의 연평균 증가율은 그림 1과 표 1에서 확인할 수 있듯이

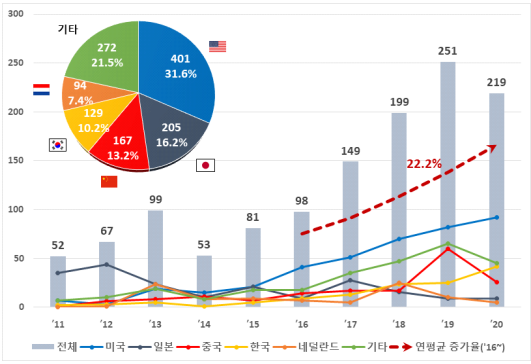
* 특허청 디지털융합심사국 인공지능빅데이터심사과 (심사관, mskang81@korea.kr)

〔표 1〕 양자내성암호 출원인 국적별 특허출원

연도	'11	'12	'13	'14	'15	'16	'17	'18	'19	'20	합계	연평균증가율('16~)
미국	7	3	19	15	21	41	51	70	82	92	401	22.4%
일본	35	44	24	10	21	9	28	16	9	9	205	0%
중국	1	6	8	11	7	14	17	17	60	26	167	16.7%
한국	2	3	5	1	5	9	13	24	25	42	129	47%
NL	0	1	24	8	9	7	5	25	10	5	94	-8.07%
기타	7	10	19	8	18	18	35	47	65	45	272	25.7%
전체	52	67	99	53	81	98	149	199	251	219	1,268	22.3%

22.3%로 가파르게 증가하고 있다.

출원인 국적별 특허는 미국 401건(31.6%), 일본 205건(16.2%), 중국 167건(13.2%), 한국 129건(10.2%), 네덜란드 94(7.4%) 순으로 출원되었으며, '16년 이후 평균 증가율은 한국 47%, 미국 22.4%, 중국 16.7%로 급격히 증가한 것으로 분석되었다. 한편, 일본과 네덜란드의 출원량은 정체하거나 다소 감소했다.



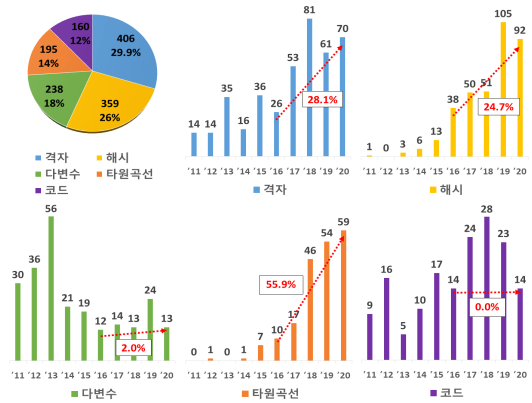
〔그림 1〕 양자내성암호 출원인 국적별 특허출원 동향.

2.2. 양자내성암호 세부기술별 특허출원

양자내성암호 세부기술별 특허는 NIST 표준화 공모전 3라운드에 진출한 격자 기반 암호(격자), 해시 기반 암호(해시), 다변수 암호(다변수), 타원곡선 아이소제니 기반 암호(타원곡선), 코드 기반 암호(코드)를 중심으로 분석했으며, 영지식 증명 기반 암호는 유의미한 특허통계가 추출되지 않아 분석에서 제외하였다.

양자내성암호 세부기술별 특허는 그림 2와 같이 '11년부터 '20년까지 격자 406건(29.9%), 해시 359건(26%), 다변수 238건(18%), 타원곡선 195건(14%), 코드 160건(12%) 순으로 출원되었다. 여기서 주목해야 할 점은 격자와 해시가 양자내성암호 전체 특허출원의 절반 이상을 차지한다는 것이며, 이후 '22년 7월 NIST에서 격자의 3개 알고리즘(CRYSTALS-KYBER, CRYSTALS-DILITHIUM, FALCON)과 해시의 1개 알고리즘(SPHINCS+)은 표준화 대상으로 선정되었다[6, 7, 9].

양자내성암호 세부기술별 특허출원의 연평균 증가율은 타원곡선 55.9%, 격자 28.1%, 해시 24.7%, 순으로 증가했으나, 다변수와 코드는 정체 중인 것으로 분석된다. 타원곡선 특허출원의 연평균 증가율이 가장 높게 나타난 것은 타원곡선의 SIKE 알고리즘이 NIST의 양자내성암호 표준화 후보로 선정된 점과 관련이 있을 것으로 추측된다[2]. 하지만, 최근 SIKE 알고리즘의 안전성에 대한 취약점이 드러났고[6, 9], 이에 따라 증가하고 있는 타원곡선의 특허출원 경향이 앞으로도 지속될지 지켜봐야 할 것으로 판단된다. 한편, 코드의 경우 NIST의 양자내성암호 표준화 후보로 3개 알고리즘(BIKE, Classic McEliece, HQC)이 선정되었고,



〔그림 2〕 양자내성암호 세부기술별 특허출원 동향.

지금까지 상기 알고리즘들에 대한 특별한 안전성 취약점이 보고되고 있지 않다[6,9]. 따라서, 이러한 표준화 상황이 향후 코드 기반 암호의 특허출원에 어떠한 영향을 미칠지 지켜봐야 할 것으로 판단된다.

2.3. 양자내성암호 세부기술별 다출원인

앞서 2.1절에서는 미국 국적 출원인의 양자내성암호 특허출원이 큰 비중을 차지하고 있는 것으로 분석되었다. 반면에, 양자내성암호 세부기술별 다출원인을 살펴보면 표 2와 같이 미국 외에도 일본, 한국, 네덜란드, 중국 등 다양한 국적의 출원인들이 순위권에 배치되어 있다. 특히, NIST 표준화 대상으로 가장 많이 선정된 격자 관련 특허는 네덜란드의 필립스(54건)와 일본의 후지쯔(28건)가 미국의 IBM(27건)보다 많이 출원했으며, 한국의 크립토-랩이 25건을 출원했다는 점도 눈에 띈다.

한편, 해시와 타원곡선 관련 특허는 미국의 인텔이 각각 108건 및 58건으로 가장 많이 출원했고, 다변수 관련 특허는 일본의 소니가 69건으로 가장 많이 출원했다. 또한, NIST 표준화 대상 후보로 선정된 코드에서는 한국의 조선대가 10건으로 가장 많이 출원했다.

Ⅲ. 양자내성암호 구현특허 출원 동향

3장에서는 양자내성암호의 구현과 관련된 특허출원 동향을 분석한다. 특허출원 통계의 산출범위는 표 3과 같이 지식재산 선진 5개국(한국, 미국, 일본, 유럽, 중국)에 2010년부터 2022년까지 출원되어 공개 및 등록

〔표 3〕 양자내성암호 구현 특허출원 산출범위 및 기준

국가	한국, 미국, 일본, 유럽, 중국
검색구간	2011년~2020년(미공개건 제외)
자료 구분	공개·등록특허
검색 DB	KIWEE(한국특허기술진흥원 검색시스템)
주요 특허분류 (CPC, IPC)	H04L(보안통신), G09C(암호)
주요 키워드	격자, 다변수, 코드 주요 알고리즘, 회로·모듈·하드웨어 구현

된 특허이다. 검색기준은 한국특허기술진흥원의 특허검색시스템(KIWEE)에서 보안(H04L) 및 암호(G09C) 관련 특허분류와 격자, 다변수, 코드 주요 알고리즘들을 회로·모듈·하드웨어 등으로 구현했다고 기재한 특허이다. (주의! 해당 특허통계에서 특정 특허의 포함 또는 누락으로 인한 일부 노이즈가 포함되어 있음. 또한 해당 특허통계 및 관련 분석은 특허청의 공식 의견이 아니며 심사관 개인의 학술연구용으로 산출 및 도출된 것으로, 이를 인용 및 활용하기 위해서는 반드시 저자와 사전협의가 필요)

양자내성암호 구현특허는 그림 3과 표 4에서 확인할 수 있듯이 '11년 이후 연평균 10.0%씩 증가해 총 546건 출원되었으며, 이는 격자, 다변수, 코드 특허출원의 전체(804건)의 67.9%를 차지한다. 특히, NIST가 양자내성암호의 표준화를 선언한 '16년 이후를 살펴보면 출원된 양자내성암호 구현특허는 337건으로 전체(470건)의 71.7%를 차지한다.

주요 발행국에 출원된 양자내성암호 구현특허는 그림 4와 같이 중국특허청(CNIPA) 172건(32%), 미국특허청(USPTO) 168건(31%), 일본특허청(JPO) 84(15%),

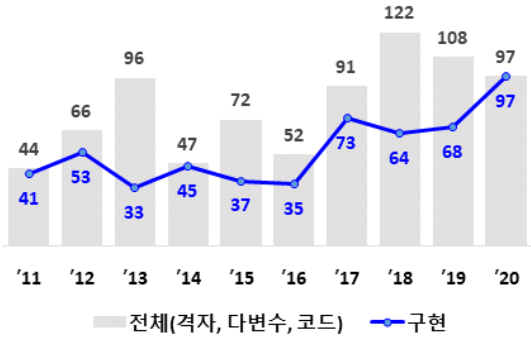
〔표 2〕 양자내성암호 기술별 다출원인

순위	격자			해시			다변수			타원곡선			코드		
	출원인	국적	출원건	출원인	국적	출원건	출원인	국적	출원건	출원인	국적	출원건	출원인	국적	출원건
1	PHILIPS		54	INTEL		108	SONY		69	INTEL		58	조선대		10
2	FUJITSU		28	GSC SECRYPT		38	NETWORK-1 TEC.		22	ISARA		38	NTT		9
3	IBM		27	CIVIC TECH.		32	SCUT		17	PHILIPS		30	ENVEIL		8
4	크립토-랩		25	ADV. NEW TEC.		28	PHILIPS		16	RUBAN Q. TEC.		26	RENESAS		7
5	MITSUBISHI		18	RUBAN Q. TECH.		28	THOMSON LICENSING		13	MITSUBISHI		18	BARKAN. ELAD		6

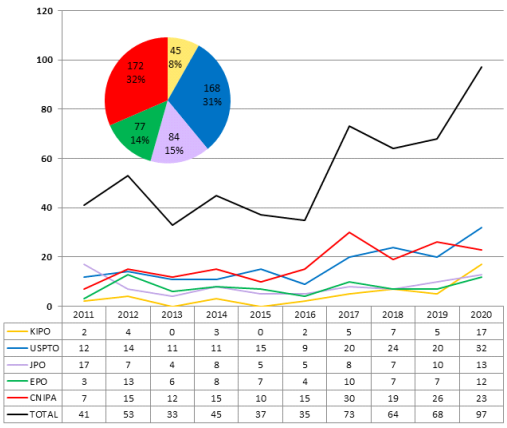
〔표 4〕 양자내성암호 구현 특허출원

연도	'11	'12	'13	'14	'15	'16	'17	'18	'19	'20	합계
구현	41	53	33	45	37	35	73	64	68	97	546
전체*	53	66	96	47	72	52	91	122	108	97	804
비율	77.4%	80.3%	34.4%	95.7%	51.4%	67.3%	80.2%	52.5%	63.0%	100.0%	67.9%

* 참고문헌 〔8〕 특허청 보도자료(23.01.09.)에서 격자, 다변수, 코드 특허출원의 합계



〔그림 3〕 양자내성암호 구현특허 출원 동향.



〔그림 4〕 양자내성암호 구현특허 발행국별 출원 동향.

유럽특허청(EPO) 77(14%), 한국특허청(KIPO) 45건(8%) 순으로 출원되었다. 이를 통해 중국과 미국의 양자내성암호 시장이 활성화되고 있다는 점을 알 수 있다.

마지막으로 양자내성암호 구현특허 다출원인을 살펴보면, 표 5와 같이 대부분 일본 대기업인 소니(64건), 파나소닉(21건), 후지쯔(18건), KDDI(15건)이 포함되어 있어, 일본 대기업들이 양자내성암호 구현 기술을 확보하기 위해 많은 투자를 하고 있음을 확인할 수 있다. 그리고 네덜란드의 필립스(17건), 한국의 삼성(16건), 미국의 마스터카드(14건), IBM(12건), 인텔(9건)도 구현특허 다출원인에 포함되어 있다.

〔표 5〕 양자내성암호 구현특허 다출원인

순위	출원인	국적	출원건
1	SONY		64
2	PANASONIC		21
3	FUJITSU		18
4	PHILIPS		17
5	삼성		16
6	KDDI		15
7	K. Sakumoto		14
8	MASTERCARD		14
9	IBM		12
10	INTEL		9

Ⅳ. 결 론

본 고에서는 양자내성암호 국적별 및 세부기술별 특허출원 동향을 살펴봤으며, 더불어 구현특허 출원 동향도 함께 분석했다. 양자내성암호에서 큰 이벤트인 NIST의 표준화가 관련 특허출원에 많은 영향력을 미치고 있으며, 다양한 국적의 출원인들이 관련 기술을 확보하기 위해 적극적 투자하고 있음을 확인했다. 특히, 발행국별 양자내성암호 구현특허의 출원량도 지속적으로 증가하고 있어, 앞으로 양자내성암호 시장 선점을 위한 각국의 기술 경쟁이 치열해질 것으로 예상된다.

참 고 문 헌

[1] 과학기술정보통신부, 한국지능정보사회진흥원(NIA), 미래양자융합포럼, 양자정보기술백서, 2020.

[2] F. Arute, K. Arya, R. Babbush, et al., “Quantum

supremacy using a programmable superconducting processor", *Nature*, 574(7779), pp. 505-510, Oct 2019.

[3] IBM, *The IBM Quantum Development Roadmap*, https://www.ibm.com/quantum/roadmap, 2022.

[4] 특허청 보도자료, *양자정보기술의 시대가 오고 있다*, 2021.

[5] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring." *Proceedings 35th annual symposium on foundations of computer science*. IEEE, 1994.

[6] 김현준, 엄시우, 송민호, 서화정, "양자컴퓨팅 환경에 안전한 암호로의 전환 동향", *정보보호학회논문지*, 33(2), April 2023.

[7] NIST, "Selected Algorithms 2022", 2022, https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms-2022

[8] 특허청 보도자료, *양자컴퓨터 시대, 보안 시장 선점을 위한 경쟁 뜨겁다*, 2023.

[9] 김동천, 김영범, 서석충, "NIST PQC 공모전 동향 분석 및 표준화 대상 & Round 4 알고리즘 소개", *정보보호학회논문지*, 33(2), April 2023.

〈저자소개〉

강 민 성 (Min-Sung Kang)

2016년 8월 : 고려대학교 정보보호대학원 박사

2016년 9월~2019년 8월 : 한국과학기술연구원 양자정보연구단 박사후연구원

2019년 8월~현재 : 특허청 인공지능 빅데이터심사과 심사관

<관심분야> 양자알고리즘, 양자통신, 양자내성암호