특허청	보 도 자 료		다시 도약하는 대한민국 함께 잘사는 국민의 나라
보도 일시	2023. 1. 8.(일) 낮12시	배포 일시	2023. 1. 6.(금) 14:30
담당 부서	융복합기술심사국 인공지능빅데이터심사과	책임자	과 장 박재일 (042-481-5782)
		담당자	사무관 임민섭 (042-481-8216) 주무관 강민성 (042-481-5140)

양자컴퓨터 시대, 보안 시장 선점을 위한 경쟁 뜨겁다

- 새롭게 열리는 '포스트-양자 암호' 시장 경쟁 치열 -

□ **양자컴퓨터가 현대의 정보통신 분야 암호체계를 무력화**시킬 수 있다는 우려가 커지면서, **사이버 보안의 새로운 시장을 선점하기 위한 각국의 경쟁이 치열**해지고 있다.

○ 각국은 **양자컴퓨터의 공격에도 안전한 암호체계** 개발을 서두르고 있는데, 현재로선 **'양자 암호*'와 '포스트-양자 암호**'**가 유력한 대안으로 보인다.

* 현대의 암호체계와 같은 디지털 정보를 이용하지 않고, 양자컴퓨터에서 사용되는 물리적 양자상태를 이용하는 암호 방식

** 양자컴퓨터로도 풀 수 없도록 수학 문제의 복잡도를 대폭 높인 형태의 암호 알고리즘

○ **포스트-양자 암호** 기술의 경제적 가치는 '**26년에 27조원***에 이를 것으로 예상되며, 이는 **전체 보안 시장 규모(247조원)의 11%**를 차지하는 규모이다.

* STATISTA(2021)의 전 세계 사이버보안 시장 규모, 미국 국립표준기술연구소(NIST)의 자료 등을 종합하여 예측함

□ 특허청(청장 이인실)에 따르면, **포스트-양자 암호** 관련 **특허출원은 '11년 이후 연평균 17.3%씩 증가**해 **10년 만에 4.2배 증가**('11년 52건 → '20년 219건)한 것으로 나타났다. [붙임 1]

○ 국가별로는 **미국이 31.6%**로 가장 많았으며, 일본(16.2%), 중국(13.2%)이 그 뒤를 이었고, **우리나라는 10.2%로 4위**를 차지했다.

- 일본의 출원량은 다소 감소하는 경향을 보인 반면, **중국(연평균 43.6%)과 한국(연평균 40.3%)의 출원 증가폭은 상대적으로 높았다.**

□ 포스트-양자 암호는 어떠한 수학 문제에 기반하고 있는지에 따라 대략 5종류(격자, 해시, 다변수, 코드, 타원곡선)로 구분되는데, **격자 기반의 암호 방식이 32.0%로 가장 많이 출원**되었다. [붙임 2]

○ **우리나라의 격자 기반 기술분야 출원량('11~'20)**은 69건으로 미국(90건)과 일본(76건)에 밀렸지만, **최근 5년간의 출원은 2위**(59건)로 1위인 미국(62건)과 근소한 차이를 보였다.

□ 전체 출원을 **출원인 유형별**로 살펴보면, 전 세계적으로는 **포스트-양자 암호 기술 개발**은 **기업**이 **주도**(80%)하고 있는 반면, **우리나라**는 **대학(38.8%)과 연구소(10.1%)**의 비율이 높은데, 이는 연구개발이 주로 정부 주도로 이루어진다는 의미이다. [붙임 3]

○ **주요 출원인**으로는 네덜란드의 1위**필립스(73건)가 가장 많은 출원**을 했으며, 그 뒤를 2위소니(72건), 3위인텔(63건), 4위IBM(43건), 5위후지쯔(35건) 등이 차지했다.

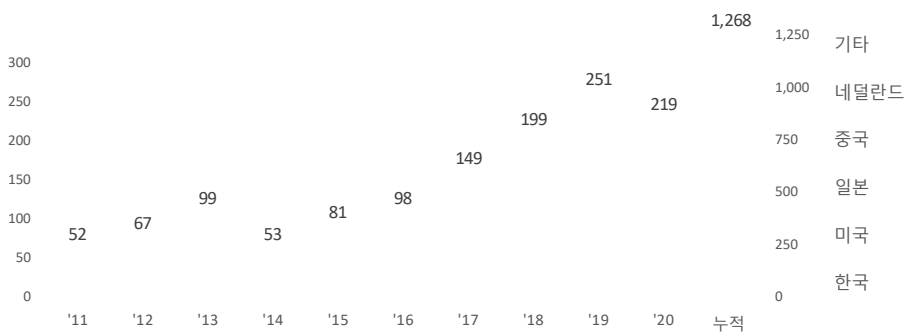
○ **국내 출원인**으로서는 **9위크립토랩(25건), 16위삼성(18건), 20위서울대(12건), 23위조선대(11건)** 순으로 많은 출원을 했다.

- **격자 기반 기술분야**에서는 **4위크립토랩(25건), 6위삼성(14건), 11위서울대(7건), 고려대(7건) 순**으로 나타나, 우리 기업·대학의 약진이 더욱 눈에 띈다.

□ 특허청 박재일 인공지능빅데이터심사과장은 "**암호 기술은 뛰어난 생각으로 세계적 대기업과 경쟁할 수 있는 분야**로 우리 기업과 연구자들이 선전하고 있어 고무적이다"라며, "양자 컴퓨팅이라는 파괴적 기술의 등장으로 **차세대 암호 기술 시장이 열리고 있는 지금**, 핵심 기술을 확보해 **사이버 안보 위협에 대비하고 시장을 선점하기 위한 범국가적 노력이 필요**한 시점이다"라고 말했다.

붙임 1 포스트-양자 암호(PQC) 국적별 특허출원 동향

< 출원인 국적별 특허출원 동향 >



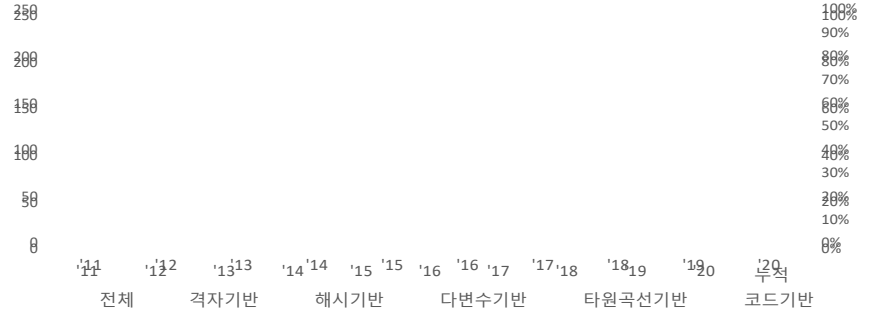
연도	'11	'12	'13	'14	'15	'16	'17	'18	'19	'20*	합계	비율	연평균 증가율
미국	7	3	19	15	21	41	51	70	82	92	401	31.6%	33.1%
일본	35	44	24	10	21	9	28	16	9	9	205	16.2%	-14.0%
중국	1	6	8	11	7	14	17	17	60	26	167	13.2%	43.6%
한국	**2**	**3**	**5**	**1**	**5**	**9**	**13**	**24**	**25**	**42**	**129**	**10.2%**	**40.3%**
네덜란드	0	1	24	8	9	7	5	25	10	5	94	7.4%	22.3%**
기타	7	10	19	8	18	18	35	47	65	45	272	21.5%	23.0%
전체	**52**	**67**	**99**	**53**	**81**	**98**	**149**	**199**	**251**	**219**	**1,268**		**17.3%**

* '20년은 미공개 출원 제외

** 네덜란드의 연평균 증가율은 최근 9년간('12~'20)으로 산정

붙임 2 포스트-양자 암호(PQC) 기술분야별 특허출원 동향

< 세부 기술분야별 특허출원 동향 >



연도	'11	'12	'13	'14	'15	'16	'17	'18	'19	'20*	합계	비율
격자기반	14	14	35	16	36	26	53	81	61	70	406	**32.0%**
해시기반	1	0	3	6	13	38	50	51	105	92	359	28.3%
다변수기반	30	36	56	21	19	12	14	13	24	13	238	18.8%
타원곡선기반	0	1	0	1	7	10	17	46	54	59	195	15.4%
코드기반	9	16	5	10	17	14	24	28	23	14	160	12.6%
전체(중복제거)	**52**	**67**	**99**	**53**	**81**	**98**	**149**	**199**	**251**	**219**	**1,268**	

* '20년은 미공개 출원 제외

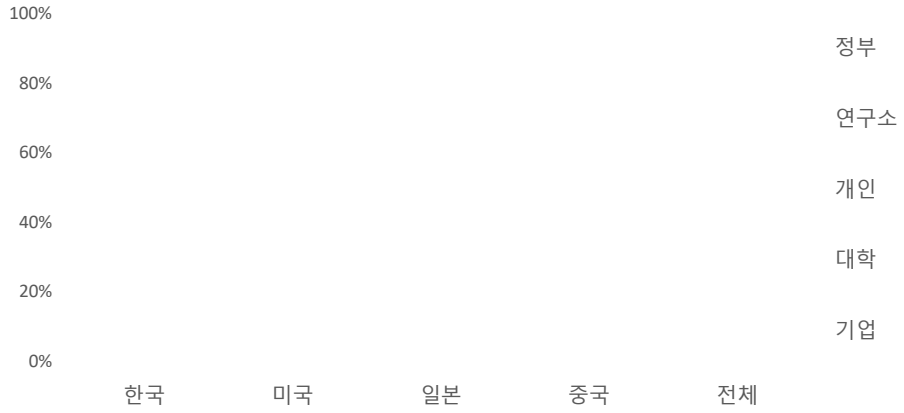
<격자기반 포스트-양자 암호, 국적별 특허출원 동향>

연도	'11	'12	'13	'14	'15	'16	'17	'18	'19	'20*	합계 ('11~'20)	합계 ('16~'20)
미국	6	2	9	6	5	13	5	15	14	15	90	62
일본	4	3	4	6	18	3	19	11	3	5	76	41
한국	**2**	**2**	**5**	**1**	**0**	**2**	**3**	**9**	**15**	**30**	**69**	**59**
네덜란드	0	1	12	0	8	0	4	21	9	3	58	37
중국	0	2	1	1	1	4	8	7	11	7	42	37
기타	2	4	4	2	4	4	14	18	9	10	71	55
전체	**14**	**14**	**35**	**16**	**36**	**26**	**53**	**81**	**61**	**70**	**406**	**291**

* '20년은 미공개 출원 제외

붙임 3 포스트-양자 암호(PQC) 출원인 유형 및 다출원인

< 출원인 국적별 출원인 유형 >



< 포스트 양자 암호 전체 다출원인 >

순위	출원인	국적	출원건
1	PHILIPS	NL	73
2	SONY	JP	72
3	INTEL	US	63
4	IBM	US	43
5	FUJITSU	JP	35
6	ISARA	CA	33
7	MITSUBISHI	JP	31
8	NTT	JP	26
9	CRYPTO LAB	KR	25
9	RUBAN QUANTUM TECH.	CN	25
16	삼성	KR	18
20	서울대	KR	12
23	조선대	KR	11

< 격자 기반 기술분야 다출원인 >

순위	출원인	국적	출원건
1	PHILIPS	NL	54
2	FUJITSU	JP	28
3	IBM	US	27
4	CRYPTO LAB	KR	25
5	MITSUBISHI	JP	18
6	삼성	KR	14
7	NTT	JP	10
7	TORONTO UNIV	CA	10
7	INTEL	US	10
10	MICROSOFT	US	8
11	서울대	KR	7
11	고려대	KR	7