KOSDAQ | 기술하드웨어와장비

아이씨티케이 (456010)

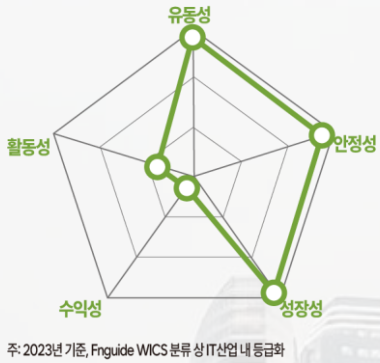
PUF 기반 보안칩과 양자내성암호(PQC) 기술 선도

체크포인트

- 아이씨티케이는 2017년 설립된 보안칩 설계 전문 기업으로, MIT에서 발표된 다수의 논문에서 개념적으로 제시되었던 복제방지기능(PUF, Physically Unclonable Function) 기반 보안칩 상용화에 성공. PUF는 물리적 시스템의 특성을 이용해 복제 불가능한 식별값을 생성. 사람의 지문과 같은 생체 정보처럼 고유한 값을 생성. 아이씨티케이는 반도체 제조 공정에서 발생하는 물리적 편차를 활용한 PUF 기술을 전문으로 함
- 자체 개발한 PUF 기술에 대한 국제 특허를 포함하여 150개 이상의 특허를 보유하고 있으며, PUF IP, PUF 보안칩, PUF 기반 보안 모듈/장비, 보안 플랫폼을 포함한 보안 S/W 솔루션/펌웨어까지 보안 관련 전 영역의 기술을 확보하여 사업을 영위. 현재는 보안칩, 보안 모듈/장비 등의 매출이 대부분이지만, 장기적으로 PUF IP 사업 위주 포트폴리오 구축 위해 노력 중
- 2024년 5월 코스닥 시장에 상장한 신생 기업으로, IoT 보안 시장에서의 성장 가능성이 주목받고 있음. 기존 암호 체계가 양자컴퓨터의 등장으로 위협받는 상황에서, PUF 기술은 양자내성암호(PQC)와 함께 사용되어 보안을 한층 강화할 수 있으며, 생성형 AI 시대의 데이터 보안에도 활용될 것으로 기대

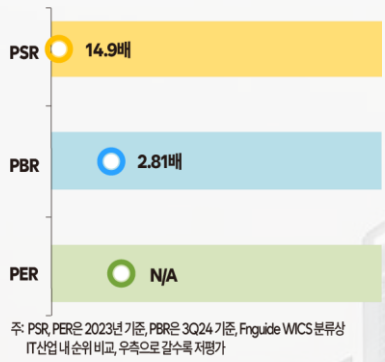
주가 및 주요이벤트

재무지표



주: 2023년 기준, Fnguide WICS 분류 상 IT산업 내 등급화

밸류에이션 지표



주: PSR, PER은 2023년 기준, PBR은 3Q24 기준, Fnguide WICS 분류상 IT산업 내 순위 비교, 우측으로 갈수록 저평가

아이씨티케이 (456010)

KOSDAQ
기술하드웨어와장비

Analyst 김경민, CFA clairekmkim@kirs.or.kr
RA 권지승 rnjswltmd32@kirs.or.kr

보안칩 설계 전문 기업으로 VIA PUF 기술 기반 보안칩 상용화에 성공

아이씨티케이는 2017년 10월 설립 이후 PUF(Physically Unclonable Function) 기술을 기반으로 한 보안칩 개발에 주력해왔으며, 독자적인 VIA PUF 기술을 통해 기존 PUF 기술의 한계였던 온도/습도 등 환경 변화에 대한 취약점을 극복하며 상용화에 성공. VIA PUF는 반도체 내부의 수동소자인 VIA홀의 물리적 특성을 활용해 고유값을 생성하는 방식으로, 환경 변화에도 안정적인 성능을 보장함. 현재 이 분야의 특허 150여개를 보유하고 있으며, PUF IP부터 보안칩, 보안 모듈/장비, 보안 플랫폼, 보안 S/W 솔루션까지 보안 관련 전 영역의 기술을 확보

G3 보안칩 양산 및 국제 인증 획득으로 기술력 입증, 글로벌 시장 확대

2018년 5월 주력제품인 무선공유기용 G3(Giant-3) 보안칩 양산을 시작으로 꾸준한 기술력을 인정받아 2020년 12월 PUF 보안 기술의 ISO 국제표준 등재(ISO/IEC 20897-1), 2022년 1월 GSA IoT 보안분과 RoT(Root of Trust: 보안의 기본이 되는 신뢰 기반) 선도업체 선정, 2022년 7월 G3 제품의 KCMVP H/W Level2 인증 획득 등 주요 성과를 달성. 2023년 3월에는 미국 San Jose 소재의 상장기업 램버스(Rambus)와 MOU를 체결하고 공동 영업을 진행하는 등 글로벌 시장 진출도 확대 중

코스닥 상장과 함께 IoT·양자컴퓨터·AI 시대의 보안 솔루션 제공 가능성 기대

2024년 5월 코스닥 시장에 상장한 아이씨티케이는 IoT 보안 시장에서의 높은 성장 잠재력을 인정받고 있음. 특히 당사의 PUF 기술은 양자컴퓨터 시대를 대비한 차세대 보안 기술로 평가받고 있으며, 최근 부각되고 있는 생성형 AI의 데이터 보안 이슈 해결에도 핵심 역할을 할 것으로 기대

Forecast earnings & Valuation

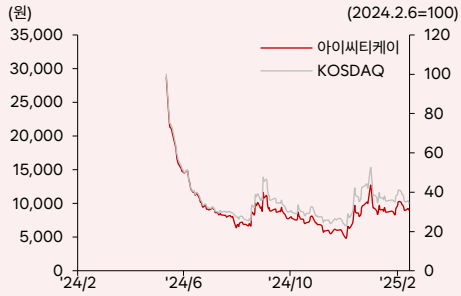
	2021	2022	2023	2024F	2025F
매출액(억원)	20	26	62	72	119
YoY(%)	136.0	28.3	141.1	15.6	66.7
영업이익(억원)	-31	-33	-24	-56	-9
OP 마진(%)	-155.3	-129.9	-38.2	-78.1	-7.4
지배주주순이익(억원)	-53	-108	-90	-97	-47
EPS(원)	-652	-1,233	-902	-781	-352
YoY(%)	적지	적지	적지	적지	적지
PER(배)	N/A	N/A	N/A	N/A	N/A
PSR(배)	0.0	0.0	0.0	17.1	10.3
EV/EBITDA(배)	N/A	N/A	N/A	N/A	N/A
PBR(배)	N/A	N/A	0.0	3.3	3.6
ROE(%)	25.7	41.4	83.2	-40.3	-12.8
배당수익률(%)	N/A	N/A	N/A	0.0	0.0

자료: 한국IR협의회 기업리서치센터

Company Data

현재주가 (2/21)		9,230원
52주 최고가		28,700원
52주 최저가		4,810원
KOSDAQ (2/21)		774.65p
자본금		56억원
시가총액		1,225억원
액면가		500원
발행주식수		13백만주
일평균 거래량 (60일)		250만주
일평균 거래액 (60일)		240억원
외국인지분율		0.23%
주요주주	이정원 외 19 인	29.66%
	유티씨인베스트먼트 외 5 인	8.30%

Price & Relative Performance



Stock Data

주가수익률(%)	1개월	6개월	12개월
절대주가	4.5	36.1	
상대주가	-2.0	37.1	

참고

1) 표지 재무지표에서 안정성 지표는 '부채비율', 성장성 지표는 '매출액 증가율', 수익성 지표는 '영업이익률', 활동성지표는 '순운전자본회전율,' 유동성지표는 '유동비율'임. 2) 표지 밸류에이션 지표 차트는 해당 산업군내 동사의 상대적 밸류에이션 수준을 표시. 우측으로 갈수록 밸류에이션 매력도 높음.

기업 개요

1 국내에서는 중소기업으로서 보기 드물게 보안칩 설계 및 후공정 라인을 보유

PUF(Physically Unclonable Function) 기반 보안칩 상용화에 성공

2017년 10월 설립된 아이씨티케이는 PUF(Physically Unclonable Function) 기술 기반 보안칩 상용화에 성공한 보안칩 설계 전문기업이다. 전 세계적으로 PUF 기반 보안칩을 양산할 수 있는 기업이 많지 않은 가운데, 국내에서는 중소기업으로서 보기 드물게 보안칩 설계 능력 및 후공정 라인을 보유하고 있다. 특히 한국 기술로 독자 개발한 'VIA(Vertical Interconnect Access) PUF' 기술은 세계적으로 소수의 기업만이 보유한 핵심 기술이다. PUF 기술은 반도체의 고유한 물리적 특성을 이용해 보안키를 생성하는데, 기존에는 주변 환경의 온도나 습도가 변화하면 이 물리적 특성도 함께 변화하여 동일한 보안키를 안정적으로 생성하기 어려웠다. 아이씨티케이의 'VIA PUF' 기술은 이러한 환경 변화에도 안정적으로 동일한 보안키를 생성할 수 있어 시장에서 기술력을 인정받았다.

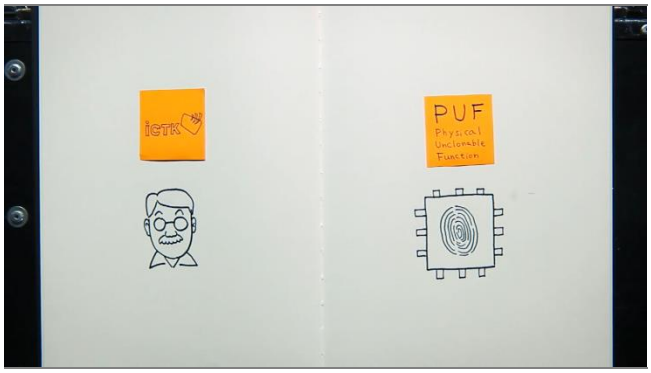
한국 시장에 무선공유기용 보안칩을 공급하며 해외 수출 확대 추진

아이씨티케이는 보안칩 설계 후 삼성전자 파운드리, SK키파운드리, 대만 UMC 등에서 웨이퍼를 양산하고, 서울 강남 본사 지하에 구축한 클린룸에서 후공정을 진행하는 독특한 사업구조를 갖추고 있다. 한국전력, LG유플러스 등에 스마트 미터기, 무선공유기용 보안칩을 공급하고 있으며, 실리콘밸리 소재의 빅테크 기업과도 IoT 분야에서 계약을 맺으며 글로벌 시장 진출을 확대하고 있다.

설계자산(IP) 분야에서 새로운 성장 동력을 모색 중

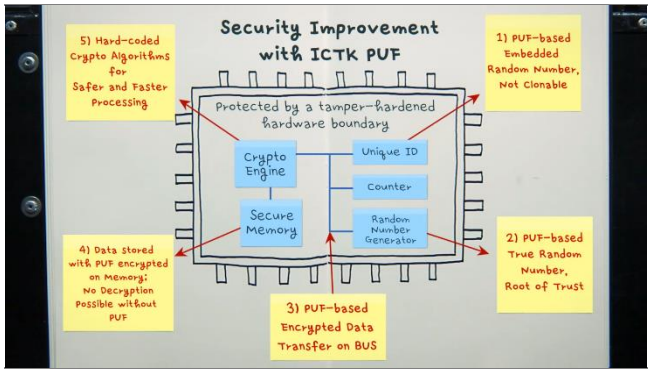
2024년 5월 코스닥 시장에 성공적으로 상장한 아이씨티케이는 설계자산(IP) 분야에서 새로운 성장 동력을 모색 중이며, 자사의 PUF 기술을 머신러닝 칩이나 기기 제어를 담당하는 다양한 시스템반도체에 IP 형태로 탑재하는 전략을 추진하고 있다. 나아가 AI 시대의 데이터 무결성과 인증이 중요해지는 환경에서, 모든 접근을 잠재적 위험으로 간주하고 지속적으로 검증하는 '제로 트러스트'(방화벽 내에서도 모든 접근을 의심하고 검증하자는 방식이며 'Never trust, always verify') 보안을 선도하는 기업으로 도약을 준비하고 있다.

PUF는 물리적 디지털 지문으로 보안칩의 복제를 원천적으로 방지



주: 사람마다 고유한 지문이 있듯이, 반도체(칩)도 제조 과정에서 발생하는 물리적 특성으로 인해 각각 고유한 '디지털 지문'을 가지게 되며, 이러한 PUF 기술은 보안칩의 복제를 원천적으로 방지
자료: 아이씨티케이, 한국IR협의회 기업리서치센터

PUF를 통한 보안 강화 시스템 구조도



주: ICTK의 PUF 기술이 적용된 보안 시스템의 구조에서는 다음과 같은 4가지 핵심 보안 요소 포함
1) PUF 기반 임베디드 난수: 복제 불가능한 고유한 값 생성
2) PUF 기반 실제 난수 생성: 신뢰점(Root of Trust)으로 작동
3) PUF 기반 데이터 전송: 버스 상의 암호화된 데이터 전송
4) PUF 암호화 메모리 저장: PUF 없이는 복호화가 불가능한 보안 저장 방식
5) 하드코드 암호 알고리즘: 하드웨어 내부에 구현되어 안전하고 빠름
자료: 아이씨티케이, 한국IR협의회 기업리서치센터

2 PUF 기술은 이러한 기존 보안 방식의 한계를 근본적으로 해결

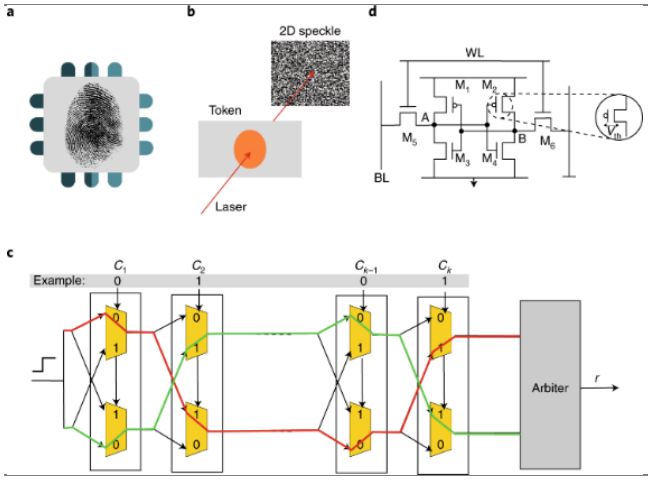
PUF란 지문이나 홍채처럼 각 반도체 칩마다 가지고 있는 고유한 '디지털 지문'

아이씨티케이라는 회사는 코스닥 시장에 상장할 당시부터 PUF(Physically Unclonable Function) 기술로 주목받았는데, PUF란 무엇일까? 이는 우리 몸의 지문이나 홍채처럼 각 반도체(칩)마다 가지고 있는 고유한 '디지털 지문'을 의미한다. 이 기술이 주목받는 이유는 보안의 새로운 패러다임을 제시했기 때문이다. 사물인터넷(IoT) 시대가 도래하면서 수많은 기기들이 네트워크로 연결되어 있고, 이들 각각의 보안이 확보되지 않으면 전체 시스템이 위험에 빠질 수 있다. 기존의 보안 방식은 주로 소프트웨어적으로 암호키를 저장하고 관리하는 방식이었다. 이는 마치 금고에 비밀번호를 저장해두는 것과 같은데, 문제는 이 비밀번호가 유출되거나 해킹될 수 있다는 점이다.

PUF는 하드웨어 자체의 물리적 특성을 활용

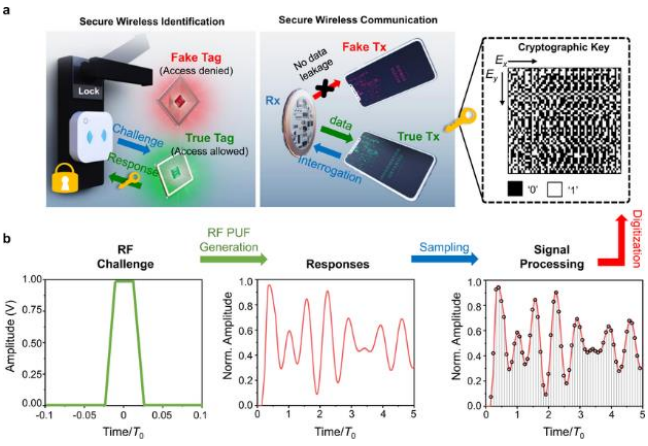
PUF 기술은 이러한 기존 보안 방식의 한계를 근본적으로 해결한다. 기존 방식이 소프트웨어적으로 보안키를 저장하고 관리했다면, PUF는 물리적 시스템 자체의 고유한 특성을 활용하기 때문이다. 이는 마치 사람의 지문이 형성되는 것과 비슷하다. 태어날 때부터 저절로 생기는 지문처럼, PUF를 적용한 시스템은 제작 과정에서 자연스럽게 고유한 '물리적 지문'을 갖게 된다. 예를 들어 투명한 물질에 레이저를 비출 때 생기는 고유한 빛의 패턴이나, 특수 자석을 뿌려 만든 막의 불규칙한 자기장 패턴, 회로 위에 입힌 특수 물질의 불규칙한 두께와 구조 등 다양한 물리적 특성을 이용할 수 있다. 특히 반도체 분야에서는 칩 제조 과정에서 발생하는 미세한 물리적 차이를 활용하는데, 아무리 정교한 공정을 사용하더라도 발생하는 이러한 차이를 이용해 각 시스템만의 고유한 식별 코드를 만들어낸다. 이는 마치 사람의 지문이 형성되는 것과 비슷하다. 태어날 때부터 저절로 생기는 지문처럼, PUF를 적용한 시스템은 제작 과정에서 자연스럽게 고유한 '물리적 지문'을 갖게 되는 것이다.

PUF가 장치를 식별하고 보안 키를 생성하는 데 사용할 수 있는 다양한 방법



주: PUF가 장치를 식별하고 보안 키를 생성하는 데 사용할 수 있는 다양한 방법 4가지는 다음과 같음
(a) 칩에 있는 지문: 각 장치는 제조 과정에서 발생하는 미세한 변동으로 인해 고유한 "지문"을 갖게 됨
(b) 레이저 기반 PUF: 레이저를 사용하여 토큰에 2D 스페클 패턴을 투사하는 PUF의 한 유형. 스페클 패턴은 레이저 빛이 거친 표면에서 산란될 때 생성되는 무작위 간섭 패턴을 의미
(c) 아비터(Arbiter) PUF: 2개의 동일한 경로 사이의 지연 차이를 기반으로 하며, 일련의 스위칭 단계에서 각 단계는 제어 비트(C1, C2, ..., Ck)에 따라 두 경로 중 하나로 신호를 보내고, 최종 결과는 아비터에 의해 결정되어 0 또는 1의 출력을 생성. 지연 차이는 제조 변동에 민감하므로 PUF가 고유한 값을 가지게 됨
(d) SRAM 메모리 셀 기반 PUF: 메모리 셀의 두 트랜지스터(M1-M6)는 제조 변동으로 인해 약간 다른 임계 전압(Vth)을 가질 수 있는데, 이러한 차이를 메모리 셀이 전원을 켤 때 0 또는 1로 무작위로 설정되도록 하며, 이러한 시작 값은 장치의 고유한 식별자로 사용될 수 있음
자료: Nature Electronics, 한국IR협의회 기업리서치센터

RF(Radio Frequency) PUF를 사용하여 보안 무선 통신 및 식별 구현



주: 1) 좌측 상단 그림(Secure Wireless Identification): RF PUF를 사용하여 장치를 인증하는 방법. 'True Tag'는 'Challenge'에 대한 올바른 'Response'를 보내 잠금을 해제하여 접근이 허용되는 반면, 'Fake Tag'는 접근이 거부, 2) 중앙 상단 그림(Secure Wireless Communication): RF PUF를 사용하여 통신을 암호화하는 방법. 'True Tx'는 데이터를 안전하게 전송할 수 있지만 'Fake Tx'는 데이터를 유출, 3) 우측 상단 그림(Cryptographic Key): RF PUF에서 생성된 응답은 암호화 키로 변환될 수 있음
자료: Nature Communications, ResearchGate, 한국IR협의회 기업리서치센터

PUF는 다수의 장점 때문에 차세대 보안 기술로 주목받고 있음

PUF 기술이 기존의 보안 기술과 차별화되는 특별한 이유는 크게 세 가지로 설명할 수 있다. 이를 일상생활의 예시와 함께 자세히 살펴보자.

첫째, 물리적으로 복제가 불가능하다는 점이다. 흔히 디지털 정보는 완벽한 복사가 가능하다고 생각한다. 예를 들어 문서 파일이나 사진을 복사하면 원본과 똑같은 복사본을 만들 수 있다. 하지만 PUF는 다르다. 똑같은 공정으로 반도체를 제조하더라도 각 칩마다 서로 다른 PUF 값이 자연스럽게 생성된다. 이는 마치 일란성 쌍둥이도 서로 다른 지문을 갖는 것과 같은 원리다. 같은 DNA를 가진 쌍둥이라도 태아 시기의 미세한 환경 차이로 인해 다른 지문이 만들어지는 것처럼, 같은 공정으로 만든 반도체라도 제조 과정의 미세한 차이로 인해 서로 다른 고유한 특성을 갖게 되는 것이다.

둘째, 외부에서 PUF 값을 읽어내는 것이 불가능하다. 이는 마치 잠금 장치가 있는 금고에서 비밀번호를 알아내려고 할 때, 금고를 물리적으로 분해하면 오히려 내부 장치가 망가져서 비밀번호를 영원히 알 수 없게 되는 것과 비슷하다. PUF 값은 칩 내부의 고유한 물리적 특성에서 비롯되는데, 이 칩을 물리적으로 분해하거나 전기적으로 분석하려고 하면 그 과정에서 원래의 물리적 특성이 변형되거나 손상되어 버린다. 따라서 아무리 정교한 분석 장비를 사용하더라도 PUF 값을 알아내거나 복제하는 것이 극도로 어렵다.

셋째, 추가 제조 비용이 거의 들지 않는다는 경제성이다. 이는 마치 사람의 지문을 만들기 위해 특별한 장치나 비용이 필요하지 않은 것과 같다. 기존의 보안 시스템은 마치 집에 별도의 도난 경보기를 설치하는 것처럼 추가적인 보안 장치가 필요했다. 하지만 PUF 기술을 적용한 보안칩은 반도체 제조 과정에서 자연스럽게 발생하는 물리적 특성을 활용한다. 따라서 특별한 장비나 추가 공정이 필요하지 않아 경제적이다. 예를 들어, 집을 지을 때 벽돌을 쌓는 과정에서 자연스럽게 생기는 벽돌의 미세한 특징을 보안 요소로 활용하는 것과 비슷하다고 할 수 있다.

이러한 세 가지 특징 '복제 불가능성, 외부 해석 불가능성, 경제성' 은 PUF가 차세대 보안 기술로 주목받는 핵심적인 이유이다. 특히 사물인터넷(IoT) 시대가 도래하면서 저비용으로 높은 수준의 보안을 제공할 수 있는 PUF 기술의 중요성은 더욱 커지고 있다.

PUF 기술이 기존의 보안 기술과 차별화되는 특별한 이유

품목	장점
복제 불가능	- 물리적으로 복제가 불가능 - 똑같은 공정으로 반도체를 제조하더라도 각 칩마다 서로 다른 PUF 값이 자연스럽게 생성
읽기 불가능	- 외부에서 PUF 값을 읽어내는 것이 불가능 - 아무리 정교한 분석 장비를 사용하더라도 PUF 값을 알아내거나 복제하는 것이 극도로 어려움
경제성	- 추가 제조 비용이 거의 들지 않는다는 경제성 - PUF 기술을 적용한 보안칩은 반도체 제조 과정에서 자연스럽게 발생하는 물리적 특성을 활용

자료: 아이씨티케이, 한국IR협의회 기업리서치센터

VIA PUF는 환경 변화에 관계없이 항상 동일한 고유값을 생성

아이씨티케이가 개발한 'VIA(Vertical Interconnect Access) PUF' 기술은 이러한 PUF의 장점을 유지하면서도 한 걸음 더 나아갔다. 기존의 반도체 기반 PUF 기술들(SRAM PUF, Ring Oscillator PUF, Arbiter PUF 등)은 온도나 습도 변화에 민감하다는 문제가 있었다. 이는 마치 손가락이 너무 건조하거나 젖었을 때 지문이 제대로 인식되지 않는 것과 비슷한데, 보안 시스템에서는 치명적인 약점이 될 수 있다. 아이씨티케이는 반도체 내부의 배선 연결부(VIA)에서 발생하

는 미세한 차이를 활용함으로써 이 문제를 해결했다. VIA PUF는 환경 변화에 관계없이 항상 동일한 고유값을 생성할 수 있어, 안정적인 보안 시스템 구축이 가능하다.

PUF 기술의 응용 분야는 매우 광범위한 편

아이씨티케이의 이러한 기술적 혁신은 반도체 분야에서 PUF 기술의 다양한 상용화를 앞당기는 계기가 되었다. 특히 환경 변화에 안정적인 PUF의 구현은 다양한 실제 환경에서 PUF 기술을 활용할 수 있는 길을 열었다고 할 수 있다. 이러한 PUF 기술의 응용 분야는 매우 광범위하다. 가장 기본적으로는 IoT 기기의 보안에 활용될 수 있다. 예를 들어 스마트홈의 각종 기기들, 산업용 센서들, 자율주행차의 부품들이 모두 고유한 디지털 지문을 가지게 되면, 해킹이나 위조로부터 훨씬 안전해진다. 또한 디지털 금융 거래나 개인 인증 시스템에도 활용될 수 있다. 더 나아가 최근 화두가 되고 있는 AI 시대에는 데이터의 진위 여부를 판별하는 데도 중요한 역할을 할 것으로 기대한다.

PUF는 단순한 기술 혁신을 넘어 보안의 새로운 패러다임을 제시

특히 양자컴퓨터 시대가 다가오면서 PUF의 중요성은 더욱 커지고 있다. 양자컴퓨터는 현재의 수학적 암호 체계를 무력화할 수 있는 엄청난 연산 능력을 가지고 있지만, 물리적 특성을 기반으로 하는 PUF는 양자컴퓨터의 연산 능력에 대해 상대적으로 강한 내성을 가질 것으로 기대한다. 이러한 이유로 PUF는 포스트 양자 시대의 주요 보안 기술 중 하나로 주목받고 있다. 이처럼 PUF는 단순한 기술 혁신을 넘어 보안의 새로운 패러다임을 제시하고 있다. 복잡한 암호 알고리즘과 보안 모듈에 의존하던 기존의 보안 체계에서, 하드웨어의 고유한 물리적 특성을 활용하는 근본적인 보안 체계로의 전환을 가능케 하는 것이다. 아이씨티케이는 이러한 혁신적인 변화를 이끌어가는 기업 중 하나로서, 안정적인 PUF 기술을 확보했다는 점에서 성장 가능성에 대한 기대가 높아지고 있다.

아이씨티케이 제품 또는 기술 관련 용어 설명

용어	설명
PUF (Physically Unclonable Function)	물리적 복제방지기술을 말하며, 동일한 제조 공정에서 생산되는 반도체의 미세구조 차이를 이용해 물리적으로 복제가 불가능한 보안키를 생성하는 기술이다. 일종의 지문과 같은 고유 정보를 담고 있으며, 고유한 보안키 값은 외부로 유출될 수 없는 특성을 지니고 있다.
VIA (Vertical Interconnect Access)	반도체(칩) 내부에서 서로 다른 층의 금속 배선을 수직으로 연결하는 통로를 의미한다. 마치 아파트의 엘리베이터 통로처럼 반도체의 각 층을 수직으로 이어주는 연결부로, 회로의 전기적 신호가 이동하는 경로가 된다. 반도체 제조 공정에서 이 VIA의 미세한 구조적 차이가 발생하는데, 아이씨티케이는 이러한 자연스러운 물리적 편차를 활용하여 고유한 보안키를 생성하는 VIA PUF 기술을 개발했다.
VIA PUF	반도체 내부의 배선 연결부(VIA)에서 발생하는 미세한 차이를 활용한 PUF 기술로, 온도나 습도 변화에 관계없이 항상 동일한 고유값을 생성할 수 있는 특징을 가진다.
MCU(Microcontroller Unit)	기기 제어를 담당하는 반도체(칩)으로, 마이크로프로세서와 입출력 장치 등을 하나의 칩에 집적한 일종의 초소형 컴퓨터이다.
CPU(Central Processing Unit	연산처리의 핵심을 담당하는 중앙처리장치로, 컴퓨터의 두뇌 역할을 하는 핵심 반도체이다.
SRAM (Static Random -Access Memory)	정적 임의 접근 메모리로, 전원이 공급되는 동안 데이터를 저장할 수 있는 메모리 반도체의 한 종류이다. DRAM과 달리 데이터를 주기적으로 재충전할 필요가 없어 속도가 빠르고 안정적이지만, 집적도가 낮고 가격이 비싸서 주로 CPU 캐시나 고성능이 필요한 곳에 제한적으로 사용된다. 마치 고급 레스토랑(SRAM)과 대중식당(DRAM)의 차이처럼, SRAM은 속도와 안정성이 뛰어나지만 공간 대비 비용이 높은 반면, DRAM은 속도는 조금 느리지만 많은 양의 데이터를 저장할 수 있다.
SRAM PUF	메모리 칩이 태어날 때부터 자신만의 고유한 '초기 서명'을 갖는 원리를 활용한 기술이다. 컴퓨터의 메모리(SRAM)가 처음 전원이 들어올 때 저절로 만들어지는 0과 1의 패턴이 칩마다 다르다는 특성을 이용하는데, 이는 마치 사람의 지문처럼 각자 다른 패턴을 보여준다. 그러나 손가락이 너무 건조하거나 물기가 있을 때 지문이 잘 인식되지 않는 것처럼, 환경의 온도나 습도가 변하면 이 패턴이 달라질 수 있다는 것이 한계다.
Ring Oscillator PUF	여러 개의 진동자(발진기)가 각각 다른 속도로 움직이는 것을 이용한 기술이다. 이는 마치 똑같이 제작한 여러 개의 메트로놈을 동시에 작동시켰을 때, 미세한 제작 차이로 인해 각각 조금씩 다른 속도로 움직이는 것과 같다. 이 속도 차이를 비교해서 고유한 값을 만들어내는 방식인데, 마치 전자시계가 극단적인 온도에서 시간이 빨라지거나 느려지는 것처럼 환경 변화에 민감하다는 것이 문제다.
아비터(Arbiter) PUF	Arbiter PUF는 마치 육상 경기에서 두 선수가 똑같은 트랙을 달리는 것과 같은 원리로 작동한다. 트랙이 완벽하게 같은 길이로 설계되었더라도 실제로는 미세한 차이가 있을 수 있듯이, 신호를 두 개의 경로로 동시에 보내고 어느 쪽이 먼저 도착하는지를 판단해서 고유값을 만드는 방식이다. 여기서 'Arbiter'라는 이름은 라틴어에서 유래한 것으로 '심판관'을 의미하는데, 마치 육상 경기에서 심판이 결승선에서 승자를 판정하듯이 두 신호 중 어느 것이 먼저 도착했는지를 판정하는 역할을 하기 때문이다. 하지만 비가 오거나 날씨가 너무 더우면 선수들의 달리기 기록이 달라지는 것처럼, 온도나 습도 변화에 따라 신호의 도착 시간이 달라질 수 있다는 것이 단점이다.
IoT (Internet of Things)	사물들이 네트워크로 연결되어 정보를 공유하고 상호작용하는 기술을 의미하며, 각종 센서와 통신 기능이 내장된 기기들이 인터넷을 통해 데이터를 주고받는 지능형 네트워크 환경을 말한다. 스마트홈의 가전제품들, 산업용 센서들, 웨어러블 기기들이 서로 연결되어 정보를 교환하고 자동화된 서비스를 제공하는 것이 대표적인 예시이다.
ECC(Error Correction Code)	능동소자 기반의 PUF 기술에서 온도, 습도, Aging으로 인하여 Key 값이 변화하는 경우 이를 정정할 수 있는 오류정정 코드이다.
ECC (Elliptic Curve Cryptography)	인터넷에서 정보를 안전하게 주고받기 위한 암호화 방식의 하나로, 타원이라는 특별한 도형의 수학적 성질을 이용한다. 마치 두 사람이 서로 다른 열쇠를 가지고 있어서 한 사람은 잠그기만 할 수 있고 다른 사람은 열기만 할 수 있는 것처럼, 암호화와 복호화에 서로 다른 키를 사용하는 방식이다. 은행 거래나 보안이 필요한 통신에서 사용되고 있다.
난수(Random Number)	예측할 수 없고, 특정 패턴이 없는 숫자를 의미한다. 난수는 보안, AI, 시뮬레이션, 게임 등 다양한 시스템의 공정성과 안전성을 보장한다.
양자(Quantum)	동전을 공중에 던져 빙빙 돌고 있는 상태와 같다. 이 상태에서는 앞면인지 뒷면인지 정해지지 않은 채로 두 가지 가능성을 모두 가지고 있는데, 이것이 바로 양자의 기본 특성이다.
양자컴퓨팅 (Quantum Computing)	마치 수많은 동전을 동시에 공중에 던져 모두 빙빙 돌게 한 후, 특정한 패턴의 결과를 찾아내는 것과 같다. 기존 컴퓨터가 한 번에 하나의 계산만 할 수 있는 것과 달리, 양자컴퓨터는 여러 가능성을 동시에 계산할 수 있다.
중첩 (Superposition)	마치 회전하는 동전이 앞면과 뒷면의 상태를 동시에 가지고 있는 것과 같다. 관찰하기 전까지는 동전이 앞면일 확률과 뒷면일 확률이 공존하는 상태로, 이는 양자가 여러 상태를 동시에 가질 수 있다는 특성을 보여준다.
얽힘 (Entanglement)	마치 한 쌍의 장갑과 같다. 오른손 장갑을 발견하면 자동으로 다른 하나는 왼손 장갑임을 알 수 있듯이, 두 양자가 서로 연결되어 하나의 상태가 결정되면 다른 하나의 상태도 즉시 결정되는 현상이다.
간섭 (Interference)	마치 잔잔한 호수에 돌을 두 개 던졌을 때 발생하는 물결의 상호작용과 같다. 두 돌이 만드는 파동이 만날 때, 파도의 높이가 더 커지거나(보강 간섭) 서로 상쇄되어 없어지는(상쇄 간섭) 현상이 발생한다. 양자 세계에서도 이와 비슷한 현상이 일어나는데, 이는 파도풀에서 볼 수 있는 파도와도 같다. 파도풀의 여러 파도 발생기가 만드는 파도들이 서로 만나 더 큰 파도를 만들거나 잔잔해지는 것처럼, 양자 상태들도 서로 만나면서 특정 상태는 강화되고 다른 상태는 약화된다. 앞서 소개한 중첩이나 얽힘과 마찬가지로 간섭은 양자컴퓨팅의 핵심 특성이자 강점이다. 양자컴퓨터는 이러한 간섭 현상을 이용해 복잡한 계산 문제를 해결할 수 있다.
중첩소멸 (Decoherence)	양자 중첩소멸(decoherence)은 양자가 주변 환경과 상호작용하면서 중첩 상태가 깨지고 특정한 상태로 고정되는 현상으로, 이는 양자컴퓨터 구현의 가장 큰 기술적 과제다. 이는 마치 중식당의 짬짜면 주문 과정과 비슷하다. 짬뽕과 짜장면의 속성을 동시에 가진 '짬짜면'이라는 메뉴가 주문을 받아 조리되기 전까지는 두 가지 가능성이 공존하는 상태지만, 실제 조리가 시작되는 순간 반드시 짬뽕이든, 짜장면이든, 한쪽을 먼저 만들어야 하는 것처럼, 양자도 관찰하거나 측정하는 순간 중첩된 상태가 깨지고 하나의 특정한 상태로 고정되는 현상이다. 앞서 소개한 중첩이나 얽힘, 간섭은 양자컴퓨팅의 강점이지만, 중첩소멸은 극복해야 할 과제이다. 중첩소멸이 발생하면 양자컴퓨팅의 가장 큰 장점인 '중첩' 상태가 사라지기 때문이다.

자료: 아이씨티케이, 한국IR협의회 기업리서치센터

3 주요 제품 및 매출 비중

제품은 크게 IP(지적재산권), 보안칩(SoC), 보안모듈/디바이스로 구분되며 솔루션 등 개발용역 매출도 발생

아이씨티케이의 제품은 크게 IP(지적재산권), 보안칩(SoC), 보안모듈/디바이스로 구분할 수 있다. 각각의 제품군은 서로 다른 시장 수요와 기술적 특성을 가지고 있으며, 아이씨티케이의 성장 전략에서 중요한 축을 담당하고 있다.

IP(지적재산권, Intellectual Property)는 아이씨티케이의 핵심 기술력을 보여주는 제품군이다. VIA PUF(Physically Unclonable Function) IP는 반도체 생산 공정의 VIA홀 크기 조절로 발생하는 편차를 이용해 고유 ID를 생성하는 기술이며, RoT(Root of Trust, 신뢰 기반) IP는 모든 보안 기능의 시작점이 되는 신뢰할 수 있는 핵심 기술이다. 동사는 ECC(Elliptic Curve Cryptosystem: 공개키 형식의 암호방식으로 타원곡선이라고 불리는 수식에 의해서 정의되는 특수한 가산법을 기반으로 하여 암호화·복호화를 하는 암호화 방식)와 양자내성암호(PQC, Post Quantum Cryptography) 등의 비대칭키(Asymmetric Key) 알고리즘, 그리고 고급암호화표준(AES, Advanced Encryption Standard)과 한국형 블록 암호화 알고리즘(SEED) 등의 대칭키(Symmetric Key) 알고리즘을 보유하고 있다. 여기에 미국 국립표준기술연구소(NIST, National Institute of Standards and Technology)의 엄격한 규격을 만족하는 진난수 생성기(TRNG, True Random Number Generator: 물리적 현상을 기반으로 하며, 완벽한 무작위성을 가진 숫자를 만들어내는 생성기) 기술까지 갖추고 있다. IP 사업에서는 아직 본격적으로 유의미한 매출이 발생하지 않고 있으나, 이러한 다양한 핵심 기술의 보유는 아이씨티케이의 기술력을 시장에서 인정받는 중요한 기반이 되고 있으며 동사는 IP 사업화를 적극적으로 추진하고 있다.

보안칩(SoC)은 현재 아이씨티케이의 주요 매출원이다. 2024년 3분기 기준 전체 매출의 39.9%(17억 원)를 차지하고 있는 이 제품군은 PUF로 생성된 고유 ID를 활용한 하드웨어 기반 보안 솔루션과, IoT 기기의 보안과 통신 기능을 동시에 제공하는 eSIM/USIM 통합 칩셋으로 구성되어 있다. 특히 이 제품군은 IoT 시대의 핵심 보안 솔루션으로 자리잡고 있다.

보안모듈/디바이스는 다양한 형태의 보안 솔루션을 제공한다. Wi-Fi와 BLE 통신 기능이 통합된 qTrustFi와 qTrustCombo, 서버용 PCI 슬롯 보안 모듈인 qTrustPCI, USB 인터페이스 형태의 qTrust USB, 통신 모뎀 형태의 LTE/5G Module, 그리고 WireGuard 프로토콜 기반의 qTrustNet VPN 등 다양한 제품을 보유하고 있다. 이 제품군은 2024년 3분기 기준 전체 매출의 4.1%(1.8억 원)를 차지하고 있다. 한편, 솔루션 등 개발용역 매출은 2024년 3분기 기준 전체 매출의 55.9%(24억 원)를 차지하고 있다. 이는 아이씨티케이가 단순한 제품 공급을 넘어 고객 맞춤형 보안 솔루션을 제공하는 종합 보안 기업으로 성장하고 있음을 보여준다.

매출 유형 (단위: 백만 원)

품목	2024년 1~3분기	2023년	2022년
보안칩	1,714	2,761	750
보안모듈/디바이스	176	869	226
솔루션 등 개발용역	2,400	2,557	1,591
합산	**4,290**	**6,187**	**2,567**

자료: 아이씨티케이, 한국IR협의회 기업리서치센터

매출 비중 (단위: %)

품목	2024년 1~3분기	2023년	2022년
보안칩	39.9	44.7	29.2
보안모듈/디바이스	4.1	14.0	8.8
솔루션 등 개발용역	55.9	41.3	62.0
합산	100	100	100

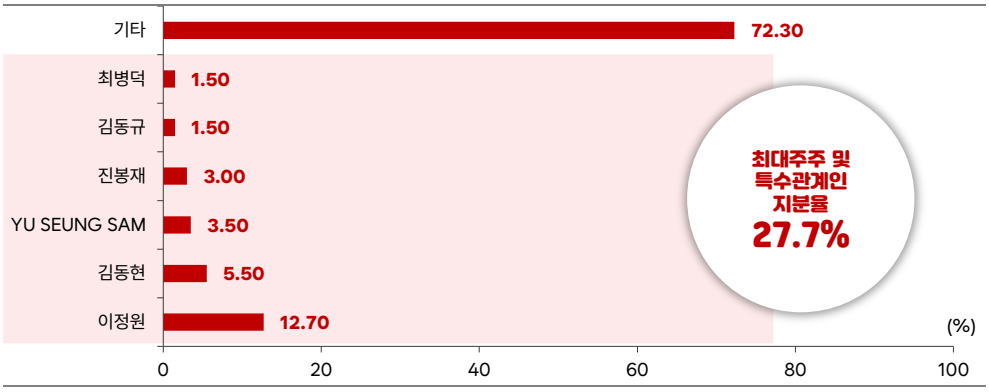
자료: 아이씨티케이, 한국IR협의회 기업리서치센터

주주 구성과 대표이사 이력

최대주주는 이정원 대표이사

아이씨티케이의 최대주주는 이정원 대표이사이다. 2024년 9월 말 기준 보통주 1,675,428주(지분율 12.7%)를 보유하고 있다. 미등기임원인 김동현 부사장이 729,360주(5.5%), 등기임원인 유승삼 부회장이 460,267주(3.5%), 관계사 등기임원인 진봉재가 396,120주(3.0%)를 보유하고 있으며, 김동규 기술고문과 최병덕 기술고문이 각각 195,384주(1.5%)를 보유하고 있다. 최대주주 및 특수관계인의 전체 지분율은 27.7%에 달한다. 이정원 대표이사는 다양한 기술 기업에서의 경험을 바탕으로 2018년 5월부터 아이씨티케이를 이끌고 있다. 티니아텍 개발팀(2004-2006년), 싱가포르 바이오센서 기업 Brain Bio Lab에서 제품기획 이사(2006-2009년), 호서대학교 겸임교수 및 호서벤처투자 투자전략 이사(2007-2009년), 주식회사 자원의 해외사업 이사(2011-2013년) 등을 역임했다. 특히 스마트카드 인증 사업을 전개하던 뷰로베리타스아이씨티케이의 COO&GM으로 재직(2013-2024년)하며 보안 산업에 대한 이해를 넓혔다. 이러한 경험은 보안칩 설계 전문기업인 아이씨티케이를 이끄는 데 밑바탕이 되고 있다.

아이씨티케이 최대주주 및 특수관계인의 주식소유 현황



자료: 아이씨티케이, 한국IR협의회 기업리서치센터

산업 현황

1 사물인터넷 기기 증가로 인해 보안의 중요성이 더욱 커지며 PUF, PQC 기술 부각

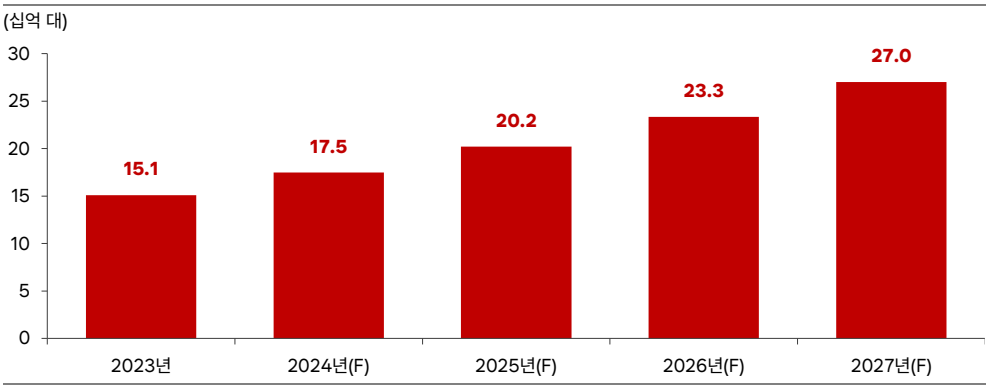
아이씨티케이가 속한 산업 현황에서 반드시 알고 넘어가야 하는 것은 PUF, PQC

아이씨티케이가 속한 산업 현황을 이해하기 위해서 알아 두어야 할 키워드는 PUF(Physically Unclonable Function, 물리적 복제방지 함수)와 PQC(Post Quantum Cryptography, 양자내성암호)이다. PUF와 PQC 같은 보안 기술이 주목받는 것은 사물인터넷 기기의 확산과 더불어 연결된 기기에 대한 보안 위협이 증가하고 있기 때문이다.

사물인터넷(IoT, Internet of Things)은 각종 사물에 센서와 통신 기능을 내장하여 인터넷에 연결하는 기술을 의미하는데, 스마트홈의 가전제품부터 산업 현장의 센서, 자율주행차의 부품까지 일상 곳곳에서 찾아볼 수 있다. 시장조사기관 IoT Analytics에 따르면 이러한 IoT 기기의 수가 2023년 이미 150억 대를 넘어섰으며 2027년에는 270억 대에 이를 것으로 전망된다. 문제는 이렇게 많은 기기들이 서로 연결되면서 보안 위험도 함께 증가한다는 점이다.

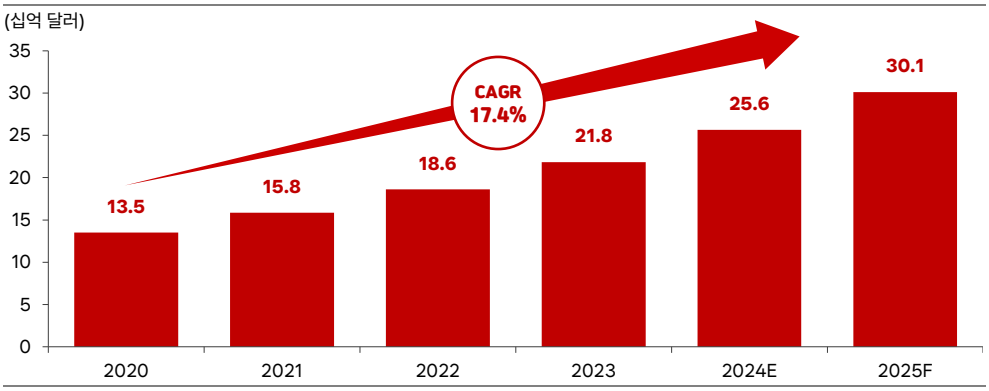
예를 들어 스마트홈의 기기 하나가 해킹되면 같은 네트워크에 연결된 다른 제품들도 위험해질 수 있으며, 산업 현장의 센서가 뚫리면 전체 생산 시스템이 마비될 수도 있다. 따라서 각 기기의 안전한 인증과 데이터 보호가 매우 중요해졌다. 여기에 양자컴퓨터 시대가 다가오면서 기존 암호 체계의 무력화 가능성이 제기되고 있다. 이러한 배경에서 하드웨어 기반의 PUF 기술과 양자컴퓨터 시대를 대비하는 PQC가 차세대 보안 기술로 주목받고 있다.

사물인터넷 기기 증가



자료: IoT Analytics, 한국IR협의회 기업리서치센터

사물인터넷 기기용 보안 시장 규모



자료: Statista, 한국IR협의회 기업리서치센터

수학이 아닌 물리적 현상을 활용한 새로운 보안 접근법이 PUF로 발전

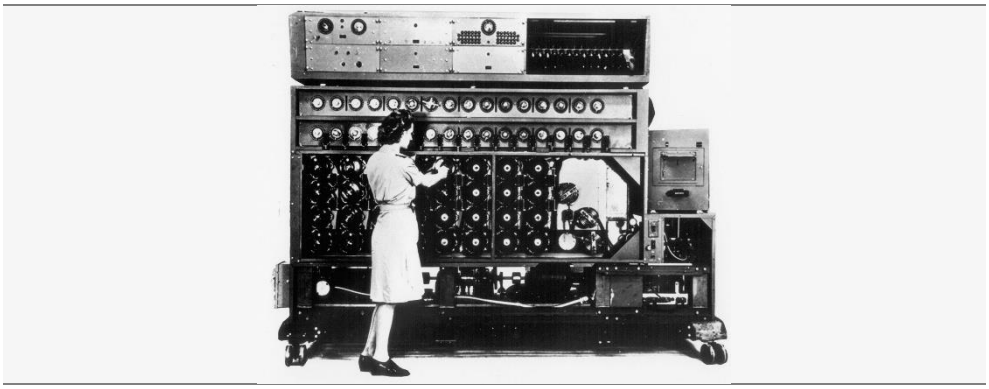
PUF 기술의 초기 개념은 2001년 MIT의 Pappu Ravikanth가 박사학위 논문 "Physical One-Way Functions"에서 제시했다. 기존의 디지털 보안은 '일방향 함수'라는 복잡한 수학적 계산을 기반으로 했다. 일방향 함수란 한 방향으로는 계산이 쉽지만 반대 방향으로는 계산이 매우 어려운 수학적 함수를 의미하는데, 이는 마치 자물쇠의 비밀번호처럼, 정답을 알면 쉽게 열 수 있지만 그 반대 방향으로 푸는 것은 매우 어려운 것이다. 제2차 세계대전 당시 독일군이 사용했던 이니그마 암호 기계가 일방향 함수 방식의 대표적인 예시다.

이니그마는 평문을 암호문으로 바꾸는 과정은 간단했지만, 암호문을 다시 평문으로 해독하는 것은 기계의 초기 설정값을 모르면 거의 불가능했다. 하지만 이러한 수학적 암호화 방식은 이론적인 가정에 기반하거나 약점이 발견되는 경우가 있었다. 실제로 이니그마도 앨런 튜링을 비롯한 영국의 블레츨리 파크 암호해독팀에 의해 결국 해독되었는데, 이 역사적 사실은 2014년 개봉한 영화 '이미테이션 게임'을 통해 대중에게 널리 알려졌다.

영화 '이미테이션 게임'에서 앨런 튜링 팀이 이니그마를 해독할 수 있었던 결정적인 단서는 독일군이 매일 아침 날씨 보고를 할 때 사용하는 정형화된 메시지였다. 날씨 보고는 항상 "Wetter"(날씨)라는 단어로 시작했고, 매일 같은 시간에 전송되었다. 이 패턴을 이용해 앨런 튜링 팀은 암호 해독 기계 'Bombe'를 개발했다. 또한 독일군이 메시지 끝에 항상 "Heil Hitler"를 포함시켰다는 점도 해독에 도움이 되었다. 이러한 반복되는 패턴들이 있었기에, 특정 시간대의 암호문에서 예상되는 평문의 위치를 추정할 수 있었고, 이를 통해 이니그마의 초기 설정값을 역추적할 수 있었다.

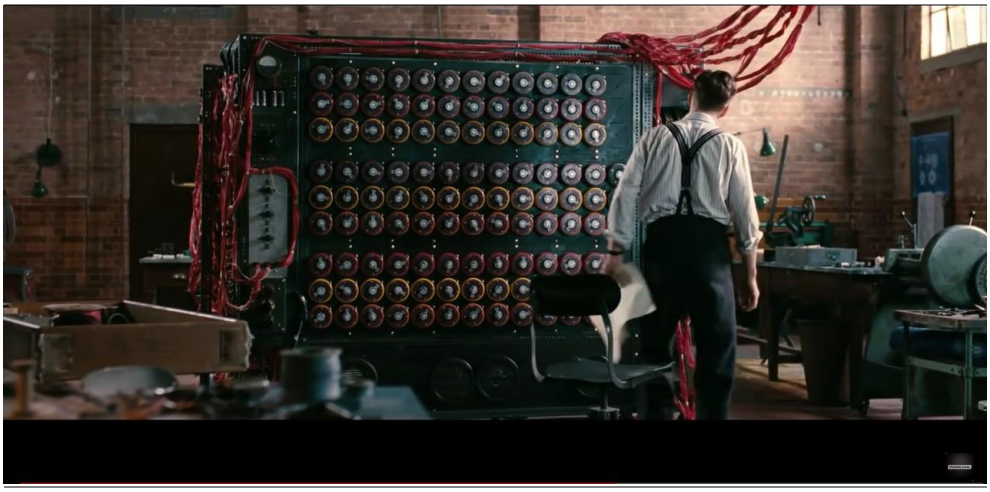
이는 아무리 강력한 암호 체계라도 사용자의 패턴화된 행동이 보안의 취약점이 될 수 있다는 것을 보여주는 좋은 예시였다. 이것이 바로 수학적 암호화 방식의 한계였고, 이러한 한계를 극복하기 위해 Pappu Ravikanth가 제안한 물리적 보안 방식이 주목받게 된 이유이기도 했다.

앨런 튜링 팀은 암호 해독 기계 'Bombe'를 개발



자료: https://www.britannica.com/topic/Bombe, 한국IR협의회 기업리서치센터

영화 이미테이션 게임에 등장한 암호 해독 기계



자료: 영화 이미테이션 게임 예고편, AI타임스, 한국IR협의회 기업리서치센터

반도체 분야에서의 PUF 보안기술은 SRAM부터 적용되기 시작

Pappu Ravikanth는 수학적 일방향 함수가 아닌 물리적 현상을 활용한 보안 접근법을 제시했다. 그는 투명한 에폭시 내 미세 입자들이 만드는 고유한 산란 패턴에 주목했으며, 이 패턴은 복제가 불가능하고 손상 시 복원되지 않는다는 점에서 보안성을 지닌다. Pappu Ravikanth의 연구는 물리적 특성을 활용한 보안 기술의 기반을 마련하며, PUF(Physically Unclonable Function) 기술의 시초로 평가받는다.

2002년, MIT의 Blaise Gassend와 연구진(Silvio Micali, Ronald L. Rivest, Srini Devadas 등)은 Pappu Ravikanth가 주장했던 개념을 반도체 공정에 적용해 'Silicon Physical Random Functions(PRF)'을 발표했다. 이들은 반도체 제조 시 발생하는 미세 공정 변이를 활용해 입력 신호(Challenge)에 대해 고유하고 재현 가능한 출력을 반환하는 기술을 구현했다. PRF는 동일한 칩이라도 공정 차이로 인해 각기 다른 응답 패턴을 제공하며, 복제가 불가능하다.

Pappu Ravikanth의 광학 기반 접근법은 미세 입자의 산란 패턴을, Gassend의 PRF는 반도체 공정 변이에 따른 전기적 특성을 활용한다. 두 방식은 구현 원리가 다르지만, 각각 광학적 무작위성과 반도체 공정의 불규칙성을 기반으로 PUF 기술 발전의 양대 출발점으로 평가된다.

이후 PUF 기술은 다양한 분야로 확장되었다. 최초의 PUF는 광학 현상을 이용했지만, 2004년 MIT 연구진이 반도체(칩)의 물리적 특성을 활용한 'Silicon PUF'를 개발하면서 본격적으로 전자 산업에 도입되기 시작했다. 특히 SRAM(Static Random-Access Memory, 정적 임의접근 메모리)의 초기 상태가 칩마다 다르게 나타나는 현상을 활용한 'SRAM PUF'는 실용성을 인정받아 널리 사용되었다.

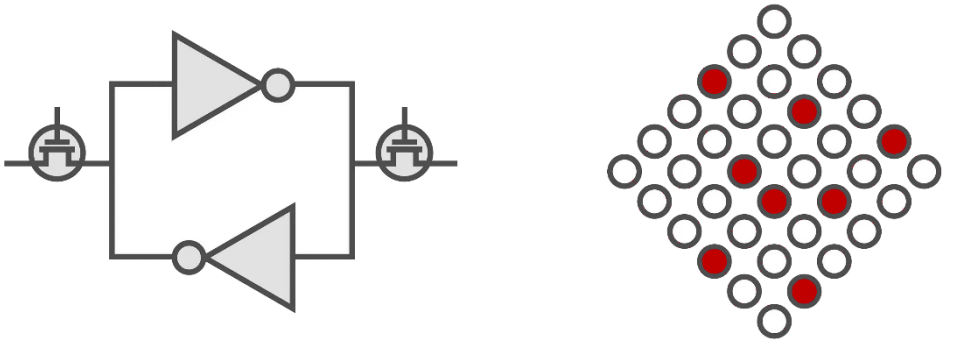
SRAM은 컴퓨터나 스마트폰 등 대부분의 전자기기에서 사용되는 필수적인 메모리 부품이다. CPU가 빠르게 처리해야 하는 데이터를 임시로 저장하는 역할을 하는데, 전원이 공급되는 동안에만 데이터를 유지하는 특성이 있다. 메모리 반도체 중에서 일반적으로 잘 알려진 DRAM(Dynamic Random-Access Memory, 동적 임의접근 메모리)도 SRAM같은 휘발성 메모리지만, SRAM은 DRAM과 달리 주기적인 재충전이 필요 없어 더 빠르고 안정적이다. 다만 SRAM은 집적도가 낮고 제조 비용이 높아 주로 CPU 내부의 캐시 메모리와 같이 고성능이 요구되는 용도로 제한적으로 사용된다.

SRAM에서는 초기값들의 배열이 각 칩마다 고유하면서도 매우 안정적으로 재현된다는 특징 보유

SRAM은 그 자체로 하나의 반도체 소자이지만, 다른 반도체(칩)의 일부 영역에 함께 집적되어 제조되는 것이 일반적이다. 예를 들어 CPU나 GPU 같은 복잡한 반도체(칩)의 경우, 내부에 SRAM 영역을 포함하고 있어 빠른 데이터 접근이 가능하다. 이러한 SRAM의 특성은 PUF 구현에 매우 적합했다. 우선 이미 대부분의 반도체(칩)에 포함되어 있어 추가적인 회로나 공정이 필요하지 않았다는 점에서 비용 효율적이었다. 또한 전원이 켜질 때 메모리 셀이 초기화되는 과정에서 각 메모리 비트가 0 또는 1의 값을 무작위로 가지게 되는데, 이 초기값들의 배열이 각 칩마다 고유하면서도 매우 안정적으로 재현된다는 특징이 있었다.

예를 들어 1메가바이트(MB) SRAM의 경우 800만 개의 비트가 있는데, 이 비트들이 보여주는 0과 1의 패턴이 마치 각자의 '지문'처럼 고유한 것이다. 같은 SRAM 칩은 전원을 껐다 켜도 거의 동일한 초기값 패턴을 보여주지만, 다른 SRAM 칩은 서로 다른 패턴을 보여준다. 더불어 SRAM은 이미 수십 년간 사용되어온 검증된 기술이었기 때문에, 신뢰성과 안정성 면에서도 큰 장점이 있었다. 이러한 이유들로 인해 SRAM PUF는 PUF 기술의 실용화를 이끈 선구자적인 역할을 할 수 있었다.

SRAM PUF

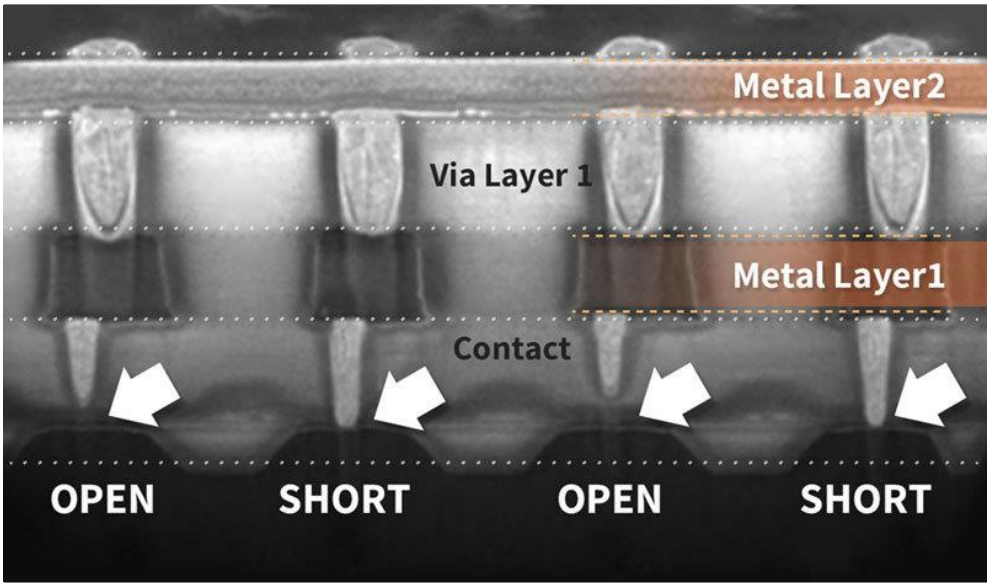


자료: https://www.embedded.com/, 한국IR협의회 기업리서치센터

PUF 기술은 다양한 형태로 발전하며 VIA PUF 등장

SRAM PUF의 성공 이후, PUF 기술은 다양한 형태로 발전했다. 초기에는 DRAM의 데이터 유지 특성을 이용한 DRAM PUF, 플래시 메모리의 문턱전압 차이를 활용한 Flash Memory PUF 등 메모리 기반의 PUF들이 연구되었다. 하지만 이러한 메모리 기반 PUF들은 SRAM PUF와 마찬가지로 온도나 습도 변화에 민감하다는 한계가 있었다. 이러한 한계를 극복하기 위해 2010년에는 반도체 배선 연결부의 특성을 활용한 VIA PUF가 등장했다. 반도체(칩)은 여러 층의 금속 배선들로 구성되어 있는데, 이 배선들은 'VIA'라고 불리는 수직 연결부를 통해 서로 연결된다. 쉽게 말해 VIA는 반도체(칩) 내부의 '수직 통로' 역할을 하는 구조물이다. 제조 공정에서 이 VIA의 크기와 저항값이 미세하게 달라지는 현상이 발생하는데, VIA PUF는 이러한 차이를 활용하여 고유한 식별값을 생성한다. 특히 VIA PUF는 온도나 습도 변화에 상대적으로 안정적이라는 장점이 있어, 다양한 환경에서 사용되는 IoT 기기의 보안에 적합했다.

VIA PUF의 단면 구조도



주: 상기 그림은 VIA PUF의 단면 전자현미경 이미지. Metal Layer1과 Metal Layer2 사이를 연결하는 Via Layer 1에서 제조 공정상의 미세한 물리적 차이로 인해 OPEN(연결 안 됨)과 SHORT(연결됨) 패턴이 자연스럽게 형성. 이러한 고유한 패턴은 각 칩마다 다르게 나타나며, 환경 변화에도 안정적으로 유지
자료: 동아일보, 한국IR협의회 기업리서치센터

링 발진기의 주파수 차이를 이용한 Ring Oscillator PUF 기술 등장

2011년, 반도체(칩)에서 동작하는 Ring Oscillator PUF가 개발되었다. 발진기(Oscillator)는 전자회로에서 일정한 주파수의 신호(파형)를 생성하는 장치이다. 그중에서도 링 발진기(Ring Oscillator, RO)는 여러 개의 인버터(신호를 반전시키는 논리 회로)를 둥근 고리(Ring) 형태로 연결한 단순한 구조를 가지고 있다.

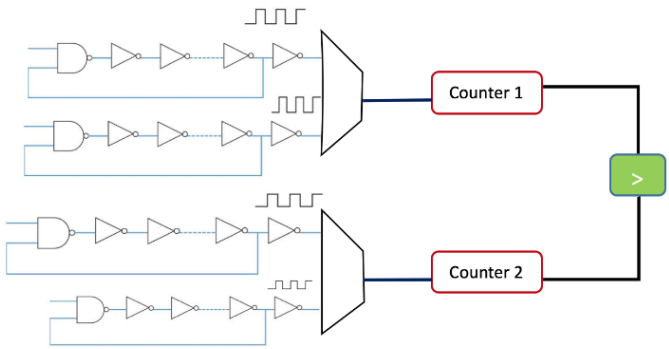
반도체(칩)에서 똑같은 설계로 여러 개의 RO를 만들어도, 반도체 제조 과정에서 발생하는 미세한 차이 때문에 각 RO의 진동 주파수(속도)가 서로 다르게 나타난다. Ring Oscillator PUF는 이러한 주파수 차이를 이용해 반도체(칩)마다 고유한 식별값(0과 1의 조합)을 생성한다. 구체적인 동작 방식은 다음과 같다.

1. 여러 개의 RO 중에서 두 개를 선택(MUX, 멀티플렉서, 스위치 역할)한다.
2. 각 RO의 진동 횟수(주파수)를 Counter가 측정한다.
3. 두 RO의 진동 수를 비교해 어느 것이 더 빠른지를 기준으로 0 또는 1을 결정한다.

4. 이렇게 만들어진 고유한 0과 1의 조합이 반도체(칩)의 디지털 지문(PUF 값) 역할을 한다.

이 기술은 구현이 단순하면서도 신뢰성이 높고, 기존 반도체 공정에서 쉽게 만들 수 있어 대량 생산에도 적합한 보안 기술로 주목받았다. 특히 칩마다 고유한 응답을 생성할 수 있어, 복제가 어렵고 보안성이 뛰어난 특징을 가진다.

Ring Oscillator PUF



주: Ring Oscillator PUF는 이러한 주파수 차이를 이용해 반도체(칩)마다 고유한 식별값(0과 1의 조합)을 생성한다. 구체적인 동작 방식은 다음과 같다.
1) 여러 개의 RO 중에서 두 개를 선택(MUX, Multiplexer, 스위치 역할)한다.
2) 각 RO는 일정 시간 동안 자기만의 고유한 주파수(진동 수)를 발생시키며, Counter(카운터 1, 카운터 2)가 이를 숫자로 세어 기록
3) 두 RO(Counter 1, Counter 2)의 진동 수를 비교해 어느 것이 더 빠른지 기준으로 0 또는 1을 결정한다. Counter 1이 크면 '1', Counter 2가 크면 '0'으로 결정한다.
4) 이렇게 만들어진 고유한 0과 1의 조합이 반도체(칩)의 디지털 지문(PUF 값) 역할을 한다.
자료: https://ece-eee.final-year-projects.in/, 한국IR협의회 기업리서치센터

회로 위에 특수 코팅을 입히는 Coating PUF도 존재

또 다른 접근으로는 회로 위에 특수 코팅을 입히는 Coating PUF가 있다. 이는 표면에 불규칙한 유전체(전기를 잘 통하지 않는 절연체(Insulator)의 일종으로, 전기장을 가했을 때 내부에 전하가 약간 이동하며(분극, Polarization) 전기 에너지를 저장할 수 있음) 물질을 코팅하고, 이로 인해 발생하는 전기적 특성의 차이를 활용하는 방식이다. 유전체 물질이 불규칙하게 도포되면서 각 칩마다 고유한 전기적 특성이 만들어지는데, 이는 마치 사람의 지문처럼 복제가 불가능하다. 더욱이 유전체 코팅 자체가 물리적 보호막 역할을 하기 때문에 외부의 물리적 공격으로부터 회로를 보호할 수 있어 보안성이 더욱 강화되는 장점이 있었다. 특히 이 방식은 표면을 물리적으로 분석하려는 시도를 막을 수 있어, 높은 수준의 보안이 요구되는 분야에서 선호되었다.

하나의 제품에 여러 종류의 PUF를 함께 적용하는 하이브리드 방식도 연구

이처럼 다양한 형태의 PUF가 개발되면서, 각각의 장단점을 고려한 선택적 적용이 가능해졌다. 예를 들어 저전력이 중요한 사물인터넷 기기에는 전력 소모가 적은 SRAM PUF를, 높은 보안성이 요구되는 군사용 장비에는 물리적 보호 기능이 있는 Coating PUF를, 대량 생산되는 소비자 전자제품에는 제조가 용이한 Ring Oscillator PUF를 적용하는 식이다. 이러한 다양한 구현 방식의 등장은 PUF 기술이 단순한 개념 증명을 넘어 실제 산업 현장의 다양한 요구사항을 충족시킬 수 있는 성숙한 기술로 발전했음을 보여준다. 특히 각 방식의 장단점이 서로를 보완할 수 있다는 점에서, 하나의 제품에 여러 종류의 PUF를 함께 적용하는 하이브리드 방식도 연구되고 있다. 예를 들어, Ring Oscillator PUF의 신속한 생성과 Coating PUF의 물리적 보호를 결합함으로써, 다양한 공격에 대한 저항력을 높일 수 있다. 이러한 하이브리드 PUF 접근법은 보안 기술의 진화를 이끌며, 각 산업의 특성과 요구에 맞춘 맞춤형 솔루션을 제공할 수 있다. 앞으로의 연구는 이러한 조합의 효율성을 극대화하는 방향으로 진행될 것이다.

중소기업 중에서 상용화된 PUF 기술을 보유한 기업은 아이씨티케이, Intrinsic ID, eMemory

반도체 산업에 국한하면, PUF 기술 적용 기업은 종합 반도체 회사와 전문 보안 기술 기업으로 나뉜다. 예를 들어 인텔 등 주요 종합 반도체 회사는 반도체 보안성을 강화하기 위해 자사 반도체 제품에 PUF 기술을 적용하고 있다. 인텔은 자사 프로세서와 칩셋에 True Random Number Generator 기반 PUF 기술을 적용해 하드웨어 보안성을 향상시켰다. 쉽게 말해, 인텔은 반도체 내부에서 자연스럽게 발생하는 미세한 전기적 차이를 '디지털 지문'처럼 활용해 제품마다 고유한 암호키를 만든다. 이를 통해, 하드웨어 복제는 어려워지고, 위조 시도를 탐지하기는 쉬워진다. 또한, 인텔의 PUF는 SGX(Software Guard Extensions)라는 보안 기능과 결합된다. SGX는 '디지털 금고'처럼 중요한 데이터를 외부 공격으로부터 보호하는 역할을 하며, 이 덕분에 서버, 클라우드, IoT 기기 등 다양한 플랫폼에서 더욱 안전한 보안 환경을 제공한다. 인텔과 같은 종합 반도체 회사를 제외하면, 반도체 중소기업 혹은 중견기업 중에서 상용화된 PUF 기술을 보유한 기업은 아이씨티케이, Intrinsic ID(네덜란드, 2024년 3월에 미국 기업 Synopsys가 인수), eMemory(대만) 세 곳이라고 할 수 있다.

이들 기업이 PUF 기술을 구현할 때, 개별 소자의 특성(**능동소자** 여부, **수동소자** 여부)에 따라 PUF 기술을 구분하는 것이 중요하다. **능동소자**와 **수동소자**의 차이는 전류의 제어 여부에 있다. **능동소자**는 전류를 증폭하거나 신호를 변조하는 역할을 하며, 트랜지스터와 다이오드 등이 대표적이다. 반면, **수동소자**는 신호를 저장하거나 흐름을 조절하지만 증폭하지는 않으며, 저항, 캐패시터, 인덕터 등이 이에 해당한다. 쉽게 말해, **능동소자**는 전류로 '일'을 하고, **수동소자**는 그 전류의 흐름을 '돕는' 역할을 한다. PUF 기술에서는 이러한 소자 특성을 기반으로 각기 다른 보안성과 신뢰성을 구현한다. 앞서 언급한 인텔의 PUF 방식은 **능동소자**인 트랜지스터를 사용해 무작위 전기적 변화를 감지하고, 이를 기반으로 유일한 보안 키를 생성한다.

▶ **아이씨티케이** VIA PUF(**수동소자** 기반): 아이씨티케이의 VIA PUF는 반도체(칩)의 비아(VIA), 즉 반도체 층간을 연결하는 금속 경로에서 발생하는 미세한 공정 편차를 활용해 보안 키를 생성한다. VIA는 전류 증폭 기능이 없기 때문에 수동소자 기반의 PUF에 해당하며, 제조 공정의 편차 자체가 보안성을 제공한다.

▶ **Intrinsic ID**의 SRAM PUF(**능동소자** 기반): Intrinsic ID는 네덜란드 에인트호번에 본사를 둔 보안 전문 기업으로, 주력 제품인 SRAM PUF는 반도체 메모리 셀의 전력 특성을 활용해 고유한 보안 키를 생성한다. 이 기술은 저전력, 빠른 초기화 등의 장점으로 IoT 및 보안 인증 솔루션에 널리 사용된다.

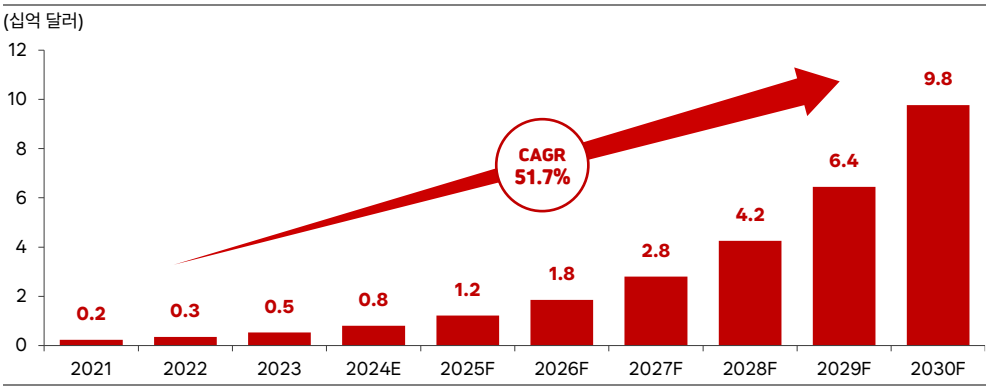
▶ **eMemory**의 NeoPUF(**능동소자** 기반): 대만에 본사를 둔 반도체 비휘발성 메모리(IP) 전문 기업인 eMemory는 NeoPUF 기술을 제공한다. NeoPUF는 반도체 공정 중 트랜지스터 내부의 임계전압 변동(Threshold Voltage Variation)을 활용해 고유한 키를 생성한다. 트랜지스터는 전류를 제어하는 능동소자이며, NeoPUF는 비휘발성 메모리 기술과 결합해 높은 내구성과 보안성을 갖춘 솔루션을 제공한다.

2 PUF와 더불어 보안 산업에서 중요한 키워드는 PQC(Post-Quantum Cryptography)

PQC는 양자컴퓨터의 발전에 대비해 기존 암호 방식의 취약점을 보완하기 위한 새로운 암호화 기술

PUF와 더불어 아이씨티케이가 속한 보안 산업을 이해하기 위해서 알아두어야 하는 또 다른 키워드는 PQC(Post-Quantum Cryptography)이다. 최근 미국에서 퀀텀(양자) 컴퓨팅 관련주가 크게 주목을 받으면서 한국에서 퀀텀 컴퓨팅에 대한 관심이 커지고 있고 이와 관련된 PQC(Post-Quantum Cryptography, 양자내성암호) 기술이 부각되고 있다. PQC는 양자컴퓨터의 발전에 대비해 기존 암호 방식의 취약점을 보완하기 위한 새로운 암호화 기술로, 보안성을 높이는 데 중요한 역할을 할 것으로 기대된다. PQC는 양자컴퓨터의 공격에 대비하여 기존의 비대칭 암호 방식보다 더 강력한 보안을 제공한다. 이 기술은 다양한 알고리즘을 통해 데이터 보호를 강화하고, 미래의 보안 요구에 부응할 수 있는 기반을 마련한다. 시장조사기관 Statista에 따르면 PQC를 비롯한 양자 관련 보안 시장 규모는 연평균 51.7% 성장할 것으로 기대된다.

양자 관련 보안 시장 규모



자료: Statista, 한국IR협의회 기업리서치센터

양자컴퓨팅은 '큐비트(Qubit)'라는 양자 비트를 사용

PQC(Post-Quantum Cryptography, 양자내성암호)의 개념을 쉽게 이해하려면, 먼저 양자컴퓨터와 양자컴퓨팅의 원리를 알아두는 것이 중요하다.

기존 컴퓨터는 '비트(bit)'라는 단위를 사용해 0 또는 1 중 하나의 상태로 데이터를 처리하며, 이진법을 기반으로 순차적으로 계산을 수행한다. 반면, 양자컴퓨터는 '큐비트(Qubit)'라는 양자 비트를 사용하며, 기존 컴퓨터와 전혀 다른 방식으로 연산한다.

큐비트는 '중첩(Superposition)'이라는 양자 특성 덕분에 0과 1을 동시에 가질 수 있어, 여러 경우의 수를 한 번에 계산할 수 있다. 예를 들어, 기존 컴퓨터가 한 번에 한 경로만 탐색한다면, 양자컴퓨터는 여러 경로를 동시에 탐색할 수 있다.

또한, '얽힘(Entanglement)'이라는 현상 덕분에 여러 큐비트가 서로 강하게 연결된다. 이 연결 덕분에 한 큐비트의 상태가 바뀌면, 다른 큐비트도 즉시 함께 반응한다. 이를 통해 여러 큐비트가 서로 협력하며 동시에 많은 계산을 효율적으로 수행할 수 있게 된다.

이러한 양자컴퓨팅의 중첩과 얽힘 덕분에 복잡한 수학 문제나 암호 해독을 기존 컴퓨터보다 훨씬 빠르게 해결할 수 있다. 이 때문에 기존의 공개키 암호(RSA, ECC 등)는 양자컴퓨터에 의해 쉽게 뚫릴 위험이 생긴다. 이를 방지하기 위해 등장한 것이 PQC(Post-Quantum Cryptography, 양자내성암호)이며, 양자컴퓨터로도 쉽게 풀 수 없는 수학적 문제를 기반으로 안전성을 확보한다.

양자컴퓨터의 개념은 1980년대 초반에 구체화

양자컴퓨터의 개념은 언제부터 구체화되었을까? 그리고 양자컴퓨터가 활성화되면 기존의 전통적인 반도체를 이용한 컴퓨터는 쓸모 없어질까? 양자컴퓨터의 개념은 1980년대 초반, 물리학자 리처드 파인만(Richard Feynman)과 데이비드 도이치(David Deutsch)에 의해 구체화되었다. 파인만은 기존 컴퓨터로는 양자역학 시스템을 효율적으로 시뮬레이션할 수 없음을 지적했다. 여기서 양자역학 시스템이란 원자, 전자, 광자처럼 아주 작은 입자들이 중첩(Superposition)과 얽힘(Entanglement) 같은 특성을 가지며, 고전 물리학과는 다르게 동작하는 세계를 말한다. 이런 세계에 대한 관찰과 분석은 단순한 학문적 호기심을 넘어서, 새로운 물질과 에너지원 개발, 초고속 컴퓨팅, 신약 개발, 그리고 더 안전한 보안 기술 등 삶을 혁신할 수 있는 다양한 기술의 기반이 된다. 파인만은 이러한 양자역학적인 현상을 그대로 모방해 계산할 수 있는 컴퓨터, 즉 양자컴퓨터의 필요성을 강조했다.

쇼어 알고리즘 등장 이후 양자컴퓨터는 현존하는 RSA 암호 체계를 무너뜨릴 수 있는 강력한 위협으로 여겨지게 됨

이후, 양자컴퓨터가 기존 컴퓨터보다 우월할 수 있다는 점을 보여주는 중요한 알고리즘들이 등장했다. 대표적인 것이 쇼어 알고리즘(Shor's Algorithm)과 그로버 알고리즘(Grover's Algorithm)이다.

쇼어 알고리즘(Shor's Algorithm)은 큰 수를 소인수분해하는 데 매우 빠른 성능을 보여준다. 여기서 소인수분해(Prime Factorization)란 큰 수를 작은 소수(1과 자기 자신만으로 나누어지는 수)들의 곱으로 나누는 것을 말한다. 예를 들어, 15는 3과 5라는 소수의 곱으로 표현된다. 소인수분해는 단순해 보이지만, 숫자가 수백 자리로 커지면 그 해를 찾는 것은 엄청나게 어렵고 시간이 오래 걸린다.

소인수분해가 중요한 이유는 현재 인터넷 보안의 핵심인 RSA 암호(Rivest–Shamir–Adleman encryption)가 이 원리를 기반으로 하기 때문이다. RSA 암호는 두 개의 매우 큰 소수(1과 자기 자신만으로 나누어지는 수)의 곱으로 만든 '공개 키'를 사용해 데이터를 암호화한다. 데이터를 해독하려면 이 두 소수를 알아야 하지만, 기존 컴퓨터로는 이 소인수분해가 거의 불가능에 가까워 보안이 유지된다.

하지만 쇼어 알고리즘은 양자컴퓨터의 병렬 연산 능력과 양자 푸리에 변환(Quantum Fourier Transform, QFT)을 사용해 소인수분해를 매우 빠르게 해결한다. 양자 푸리에 변환(QFT)은 양자 중첩(Superposition) 상태에 있는 데이터를 주파수(패턴) 형태로 변환해 주는 일종의 '양자 신호 분석 기술'이다. 기존의 푸리에 변환(Fourier Transform)은 음성이나 영상 신호에서 패턴을 찾는 데 사용되지만, 양자 푸리에 변환은 그 과정을 양자컴퓨터의 중첩 특성을 이용해 훨씬 빠르게 처리한다.

결과적으로, 기존 컴퓨터가 수백 년이 걸릴 소인수분해 문제를 쇼어 알고리즘을 사용한 양자컴퓨터는 몇 초 만에 해결할 수 있다. 이 때문에 양자컴퓨터는 현존하는 RSA 암호 체계를 무너뜨릴 수 있는 강력한 위협으로 여겨진다. 이런 위협에 대비해 새로운 암호 기술인 PQC(Post-Quantum Cryptography, 양자내성암호)가 주목받고 있는 것이다.

그로버 알고리즘은 양자 중첩과 양자 간섭을 이용해 기존 컴퓨터보다 훨씬 빠르게 원하는 데이터를 찾을 수 있는 강력한 도구

쇼어 알고리즘(Shor's Algorithm)은 큰 수를 소인수분해하는 데 매우 빠른 성능을 보여주는 반면, 그로버 알고리즘(Grover's Algorithm)은 데이터베이스에서 원하는 정보를 매우 빠르게 찾을 수 있는 양자컴퓨터의 대표적인 알고리즘이다.

기존 컴퓨터에서는 원하는 데이터를 찾기 위해 하나씩 순서대로 확인해야 한다. 예를 들어, 100만 개의 연락처에서 특정 이름을 찾으려면, 평균적으로 절반인 50만 번 정도 검색해야 한다. 기존 컴퓨터에서는 원하는 데이터를 찾기 위해 하나씩 순서대로 확인하는 선형 탐색(Linear Search) 방식을 사용하기 때문이다. 선형 탐색은 처음부터 끝까지 데이터를 하나씩 비교하며 원하는 값을 찾는 방식이다. 100만 개의 연락처 중에서 특정 이름을 무작위로 찾는 경우, 원하는 데이터는 평균적으로 중간쯤(50만 번째)에 위치할 가능성이 가장 높다.

그로버 알고리즘은 이런 탐색을 훨씬 빠르게, 약 1,000번 정도의 연산만으로 끝낼 수 있다. 이렇게 빠른 검색이 가능한 이유는 양자 중첩(Superposition)과 양자 간섭(Interference)이라는 양자역학의 특별한 원리를 사용하기 때문이다.

그렇다면, 양자 중첩(Superposition)이란 무엇일까? 전술했던 바와 같이 양자 중첩은 양자 비트(큐비트, Qubit)가 0과 1을 동시에 가질 수 있는 상태를 말한다. 기존 컴퓨터의 비트는 한 번에 0이나 1 중 하나의 값만 가질 수 있지만, 큐비트는 여러 상태를 동시에 계산할 수 있다. 예를 들어, 기존 컴퓨터가 4개의 데이터 중 원하는 데이터를 찾으려면 한 번에 하나씩 확인해야 하지만, 양자컴퓨터는 4개를 동시에 탐색할 수 있다. 데이터가 많아질수록 이 차이는 더욱 커진다.

양자 중첩과 달리 양자 간섭(Interference)이란 파동이 서로 겹쳐지면서 특정 신호를 강하게 하고 다른 신호는 약하게 만드는 현상이다. 양자컴퓨터는 이 간섭을 이용해 정답일 확률을 높이고, 오답일 확률은 낮추는 방향으로 연산을 반복한다. 예를 들어, 여러 갈림길 중 정답으로 이어지는 길을 갈수록 두 개의 파동이 만나서 점점 더 강해지고, 정답이 아닌 길은 파동이 상쇄되어 점점 사라지는 것과 같다.

왜 이렇게 하면 원하는 데이터를 빨리 찾을 수 있을까? 기존 컴퓨터는 데이터를 하나씩 일일이 확인하는 데 비해, 그로버 알고리즘은 양자 중첩으로 모든 데이터를 동시에 탐색하며, 양자 간섭으로 정답만 남도록 확률을 강화한다. 이렇게 중첩과 간섭을 여러 번 반복하면, 정답에 해당하는 데이터는 점점 더 강하게 표시되고, 결국 컴퓨터는 짧은 시간에 정답을 찾아낼 수 있게 된다.

예를 들어, 100만 개의 비밀번호 중 정답을 찾는 상황을 생각해 보자. 기존 컴퓨터는 하나씩 시도해야 하지만, 그로버 알고리즘은 처음부터 100만 개의 비밀번호를 동시에 시도하고, 중첩과 간섭을 반복해 정답일 확률만 점점 높여 빠르게 찾아낸다.

그로버 알고리즘은 단순한 검색 문제뿐 아니라, 금융 사기 탐지, 신약 후보 물질 탐색, 최적 경로 탐색, 인공지능 모델 학습 등 데이터가 방대할수록 더욱 강력한 성능을 발휘한다. 요약하자면, 양자 중첩은 동시에 여러 가능성을 탐색하게 해주고, 양자 간섭은 그중에서 정답만 남게 해주는 기술이다. 그로버 알고리즘은 이 두 가지 특성을 잘 활용해 기존 컴퓨터보다 훨씬 빠르게 원하는 데이터를 찾을 수 있는 강력한 도구인 것이다.

양자컴퓨터는 특정한 문제 해결에 압도적 성능 발휘

쇼어 알고리즘(Shor's Algorithm)과 그로버 알고리즘(Grover's Algorithm)을 기반으로 양자컴퓨터가 기존의 반도체 기반 컴퓨터를 완전히 대체할 것이라는 생각은 오해일 수 있다. 양자컴퓨터는 특정한 문제, 특히 소인수분해 풀이, 최적화, 기계 학습 등의 분야에서 기존 컴퓨터보다 압도적인 성능을 발휘하지만, 모든 계산 작업에 적합한 것은 아니다. 반도체 기반의 전통적인 컴퓨터는 일반적인 데이터 처리, 운영체제 관리, 사무 작업 등 일상적인 업무에서는 여전히 효율적이고 경제적이다.

양자컴퓨터와 기존 컴퓨터가 공존할 가능성이 큰 상황

미래에는 양자컴퓨터와 기존 컴퓨터가 각자의 강점을 살리며 공존할 가능성이 크다. 예를 들어, 양자컴퓨터는 복잡한 연산과 시뮬레이션을, 기존 컴퓨터는 제어와 입출력 및 사용자 인터페이스를 담당하는 하이브리드 컴퓨팅 환경이 주류가 될 수 있다. 따라서 양자컴퓨터의 발전은 전통적인 반도체 기술을 무력화하는 것이 아니라, 오히려 새로운 반도체 및 하드웨어 아키텍처 혁신을 촉진하는 계기가 될 수 있다.

최근 미국 증시에서는 양자컴퓨팅 기업들이 주목받는 중

이러한 전망을 반영하듯 최근 미국 증시에서는 양자컴퓨팅 기업들이 주목받고 있다. 대표적으로 2013년 설립된 리게티(RGTI)는 초전도체 기반 양자 프로세서를 개발하고 클라우드 기반 양자컴퓨팅 서비스(QCaaS)를 제공하는 기업이고, 1999년 설립된 디웨이브퀀텀(QBTS)은 양자컴퓨터를 초기에 상용화한 기업으로, 양자어닐링 방식의 '어드밴티지' 시스템을 개발했다. 어닐링은 마치 금속을 담금질할 때 천천히 식히면서 단단한 상태를 찾아가는 것을 의미하는데, 양자어닐링은 수많은 변수 중에서 최적의 해답을 찾아가는 방식이다. 이는 자연계의 기본 원리를 활용한 것으로, 높은 온도에서는 입자들이 자유롭게 움직이다가 온도가 낮아지면서 점차 안정적인 상태로 정착하는 현상을 컴퓨팅에 적용한 것이다. 특히 전통적인 어닐링과 달리 양자 터널링 현상을 이용해 에너지 장벽을 넘어 최적해를 찾을 수 있다는 것이 특징이다. 예를 들어 수천 대의 택배 트럭이 수만 개의 배송지를 가장 효율적으로 방문하는 최적 경로를 찾거나, 수많은 투자 종목 중에서 위험은 최소화하고 수익은 최대화하는 포트폴리오를 구성하는 등 기존 컴퓨터로는 계산하기 어려운 최적화 문제를 해결하는 데 특히 강점을 보인다. 현재 디웨이브퀀텀은 양자 컴퓨팅 시스템, 소프트웨어, 서비스 개발 및 제공 분야의 선두주자로 자리매김하고 있다. 한편, 2018년 설립된 퀀텀컴퓨팅(QUBT)은 저전력으로 상온에서도 작동 가능한 디랙(Dirac) 시스템을 개발하여 인공지능, 사이버보안, 원격감지 등의 분야에 솔루션을 제공하고 있으며, 2015년 설립된 아이온큐(IONQ)는 이온트랩 기술을 활용한 양자컴퓨터를 개발하여 AWS, 마이크로소프트 Azure, 구글 클라우드 등 주요 클라우드 플랫폼을 통해 서비스를 제공하고 있다.

미국에서 양자컴퓨팅 관련주가 급등했을 때 가상화폐 관련주가 하락

최근에 미국 증시에서 양자컴퓨터 관련주의 흐름과 시장의 반응을 보면 양자컴퓨터의 특징을 직관적으로 이해할 수 있다. 미국에서 양자컴퓨팅 관련주가 급등했을 때 가상화폐 관련주가 하락했다. 양자컴퓨터가 암호의 해답을 기존 컴퓨터보다 훨씬 빠르게 찾아낼 수 있기 때문이다.

가상화폐, 특히 비트코인과 같은 암호화폐는 블록체인(Blockchain) 기술을 기반으로 하며, 거래의 안전성을 SHA-256 같은 복잡한 암호화 알고리즘으로 보장한다. SHA-256(Secure Hash Algorithm 256-bit)은 데이터를 고정된 길이인 256비트(bit)의 암호화된 코드(해시, Hash)로 변환하는 수학적 알고리즘이다. "Hello"라는 단어를 SHA-256으로 변환하면 완전히 다른 긴 숫자·문자 조합이 생성된다. "hello"처럼 철자 하나만 대문자로 바꿔도 해시(암호화된 코드) 값은 완전히 달라진다. 이는 SHA-256 알고리즘이 입력의 아주 작은 변화에도 전혀 다른 출력값을 생성하는 '혼돈성(Avalanche Effect)' 특성을 갖기 때문이다.

예시 1) Hello: **185f8db32271fe25f561a6fc938b2e264306ec304eda518007d1764826381969**
예시 2) hello: **2cf24dba5fb0a30e26e83b2ac5b9e29e1b161e5c1fa7425e73043362938b9824**

SHA-256 알고리즘은 매우 어려운 수학적 문제를 풀어야만 거래가 승인되는 구조이며, 이를 푸는 과정을 '채굴(mining)'이라고 한다. 기존 컴퓨터는 이 암호를 해독하려면 어마어마한 연산 시간이 필요하지만, 그 덕분에 블록체인 시스템은 매우 안전하게 유지된다. 그러나 양자컴퓨터, 특히 그로버 알고리즘(Grover's Algorithm)과 쇼어 알고리즘(Shor's Algorithm)이 등장하면 상황이 달라진다.

그로버 알고리즘은 암호 해시(Hash)를 역추적해 비밀번호나 해시 값을 빠르게 찾는 데 특화되어 있다. 기존 컴퓨터보다 연산 속도를 제곱근 수준으로 단축하기 때문에, 암호화폐 지갑의 해시를 풀거나 비밀번호를 찾는 시간이 기존 대비 극적으로 줄어든다.

한편, 쇼어 알고리즘은 RSA, ECC(Elliptic Curve Cryptography) 등 공개키 암호(public-key encryption)를 빠르게 해독할 수 있다. 많은 블록체인 거래는 공개키 기반 암호화 방식을 사용하기 때문에, 쇼어 알고리즘으로는 지갑의 개인키를 역산해 자금을 탈취할 위험이 커진다.

이 때문에, 양자컴퓨터가 상용화되면 현재 암호화폐의 보안 시스템이 무력화될 것이라는 불안감이 커지면서, 양자컴퓨팅 관련주가 급등할 때 가상화폐 관련주는 급락하는 현상이 나타난 것이다. 양자컴퓨팅은 데이터 탐색, 암호 해독, 최적화, 신약 개발 등에서 혁신적인 기술이지만, 동시에 기존 보안 체계를 위협하는 '양날의 검'이다. 그래서 양자컴퓨팅 관련주가 급등할 때, 가상화폐 관련주가 하락하는 것은 기술 혁신이 가져올 새로운 기회와 위협이 동시에 반영된 시장의 자연스러운 반응인 것이다.

3 양자컴퓨터의 위협에 대비해, PQC(양자내성암호) 기술이 개발되는 중

NTRU'와 CRYSTALS 알고리즘이 PQC 기술 후보군으로 부각

이와 같은 양자컴퓨터의 위협에 대비해, PQC(Post-Quantum Cryptography, 양자내성암호) 기술이 개발되고 있다. PQC는 전술했던 바와 같이 양자컴퓨터로도 풀기 어렵게 설계된 새로운 암호화 기술로, 블록체인에도 양자 저항성을 갖춘 암호 알고리즘을 도입하려는 움직임이 활발히 진행 중이다. 예를 들어 아이씨티케이(ICTK)는 Post-Quantum 시대에 대비해 NIST(미국 표준기술연구소)의 PQC 프로젝트 3라운드에 올라 있던 알고리즘 'NTRU'와 'CRYSTALS'에 대한 기술력을 확보했다.

NTRU 알고리즘은 격자(Lattice)라는 수학적 구조를 기반 암호, Lattice-based Cryptography를 의미하며 양자컴퓨터의 쇼어 알고리즘으로도 풀기 어렵다는 점에서 안전성이 매우 높다. 연산 속도가 빠르고 key 값의 크기가 작아 IoT 기기나 반도체 보안 모듈에 적합하다. 한편, CRYSTALS 알고리즘은 'Kyber'(키 교환)와 'Dilithium'(전자서명)이라는 두 가지 알고리즘을 포함하는 격자 기반 암호 기술이다. Kyber는 양자컴퓨터 공격에도 안전한 키 교환(Key Exchange) 프로토콜이다. Dilithium은 위·변조가 불가능한 전자서명(Digital Signature) 기술이다. 앞서 소개했던 NTRU 알고리즘보다 구현이 쉽고 안정적이며, NIST(미국 표준기술연구소) PQC(Post-Quantum Cryptography, 양자내성암호) 프로젝트에서도 최종 라운드 후보군으로 평가받고 있다. 빠른 속도, 짧은 key 값 크기, 고성능 하드웨어 구현 용이성 덕분

에 금융 보안, 블록체인, 디지털 인증 등에 적합하다.

다양한 글로벌 기업과 기관들이 PQC 기술 확보 및 표준화에 주력

PQC에 대한 연구와 개발은 단순히 암호 기술을 넘어, 블록체인, 금융, 클라우드, IoT, 자율주행차 등 산업 전반에 걸쳐 필수적인 보안 기술로 자리 잡고 있다. 양자컴퓨터가 실용화될 경우, 기존의 보안 프로토콜은 무력화될 위험이 높기 때문에, 다양한 글로벌 기업과 기관들이 PQC 기술 확보 및 표준화에 주력하고 있다. 미국 표준기술연구소(NIST)는 2024년 8월에 3라운드 Post-Quantum Cryptography(PQC) 알고리즘 표준을 공식 발표하며, 양자컴퓨터 시대의 보안 표준을 규정했다. 이번 발표에는 CRYSTALS-Kyber(키 교환) 및 CRYSTALS-Dilithium(전자서명)이 표준으로 선정되었으며, FALCON 및 SPHINCS+는 전자서명 보완 알고리즘으로 추가 검토 중이다. 이는 향후 금융, 블록체인, IoT, 클라우드 산업 전반에 필수적인 보안 체계로 자리 잡을 전망이다.

글로벌 빅테크 기업들은 양자컴퓨터 시대에 대비해 적극적으로 PQC 기술을 도입

구글(Google), IBM, 퀄컴(Qualcomm), AWS 등 글로벌 빅테크 기업들은 양자컴퓨터 시대에 대비해 적극적으로 PQC 기술을 도입하고 있다. 구글은 크롬 브라우저 및 클라우드 서비스에 Kyber(키 교환) 기반 PQC 프로토콜을 적용해 데이터 보호를 강화했으며, IBM은 Quantum Safe 솔루션을 통해 Dilithium(위·변조가 불가능) 기반 전자서명을 자사 보안 제품군에 통합했다. 퀄컴은 NTRU(격자(Lattice))라는 수학적 구조를 기반 암호, Lattice-based Cryptography를 의미) 및 Kyber(키 교환) 기반 보안 모듈을 Snapdragon SoC에 탑재할 계획이며, AWS는 Kyber 기반 키 관리 서비스(KMS)를 통해 클라우드 데이터 보호 수준을 높였다. **사실, 이러한 빅테크 기업들의 PQC 관련 움직임은 보안 기술의 미래를 바꾸는 중요한 변화지만, 우리가 실생활에서 즉각적으로 체감하기는 어렵다.** 그러나 이들 기업의 노력은 금융, 통신, IoT 등 보이지 않는 곳에서 데이터를 보호하며, 미래의 보안 위협에 대비하고 있다.

PQC 기술을 주력 솔루션으로 삼고 있는 상장기업도 존재

이와 같이 빅테크 기업 외에 PQC 기술을 주력 솔루션으로 삼고 있는 상장기업도 있다. Arqit Quantum Inc.는 2017년 영국에서 설립되어 양자컴퓨터 시대의 보안 위협에 대응하는 암호화 솔루션을 개발하고 있다. 특히 이 회사는 QuantumCloud라는 플랫폼(현재는 Arqit SKA Platform™으로 변경)을 통해 양자컴퓨터로도 해독이 불가능한 암호화 키를 생성하는 서비스를 제공하며, 정부기관, 통신사, 금융기관 등을 주요 고객으로 확보하고 있다. 초기에는 위성 기술을 활용했으나 현재는 기존 인터넷과 통신 인프라를 활용하는 지상 기반 배포 방식으로 전환하여 비용을 크게 절감했다. 현재는 미국 국가안보국(NSA, National Security Agency)의 엄격한 보안 표준을 충족하는 암호화 솔루션을 다양한 기술 플랫폼에 제공하고 있다.

PQC와 PUF는 보안성을 극대화하기 위해 함께 사용되는 상호 보완적 기술

전술했던 바와 같이, PQC(Post-Quantum Cryptography)는 양자컴퓨터 공격에도 안전한 암호화 알고리즘으로, 데이터 전송과 저장 시 보안을 책임진다. 이는 기존 RSA나 ECC 같은 전통적인 암호 체계의 취약점을 보완하며, 데이터 암호화와 인증에 필수적인 보호막 역할을 한다.

PUF(Physical Unclonable Function)는 물리적 특성을 기반으로 복제할 수 없는 고유 식별자를 생성해 보안성을 높이는 기술이다. 반도체 외에도 광학, 폴리머 등 다양한 분야에 적용되며, 하드웨어 고유성을 활용해 보안 키를 생성한다. 특히 반도체 분야에서는 칩의 미세한 공정 차이를 '디지털 지문'처럼 활용해 복제 불가능한 고유 키를 생성하며, 하드웨어 기반 키 관리 및 기기 인증에 사용된다. 이러한 특성 덕분에 별도의 키 저장소 없이 하드웨어 자체에서 키를 생성해 해킹 위험을 최소화한다.

이처럼 PQC는 데이터 보호를 위한 '잠금장치'이며, PUF는 '복제 불가능한 열쇠'이다. PQC는 암호화 및 인증을 담당하고, PUF는 안전한 키를 생성한다. 즉, PQC와 PUF는 대체제가 아닌, 보안성을 극대화하기 위해 함께 사용되는 상호 보완적 기술(Complementary Technology)이라고 할 수 있다.

PUF와 PQC가 동시에 적용된 사례는 SK텔레콤과 케이씨에스(KCS)가 공동 개발한 'Q-HSM' 양자암호칩

PUF와 PQC가 동시에 적용된 사례는 2024년부터 이미 등장했다. 그 대표적인 예가 SK텔레콤과 케이씨에스(KCS)가 공동 개발한 'Q-HSM' 양자암호칩이다. 언론 보도에 따르면, 'Q-HSM' 양자암호칩은 엑스퀀텀(X Quantum)이라는 대한민국 양자 기술 얼라이언스를 통해 선보였으며, PQC(양자내성암호)와 PUF(물리적 복제 방지) 기술이 동시에 적용된 양자암호칩이다.

언론 보도에 따르면, Q-HSM은 하드웨어 기반의 QRNG(Quantum Random Number Generator: 양자의 불확실성을 이용한 난수 생성)와 PUF(물리적 복제 방지), 그리고 소프트웨어 기반의 PQC(양자내성암호) 기술을 통합했다. QRNG는 양자의 불확정성을 활용해 예측 불가능한 순수 난수(random number)를 생성하여 암호 키의 안전성을 확보한다. PUF(Physical Unclonable Function)는 전술했던 바와 같이, 반도체 소자의 미세한 물리적 특성을 활용해 고유한 디지털 지문을 생성함으로써 하드웨어 복제를 방지한다. 여기에 PQC(Post-Quantum Cryptography)는 양자컴퓨터의 공격에도 안전한 암호 알고리즘을 적용해 보안을 더욱 강화했다.

Q-HSM은 양자 기술을 기반으로 하드웨어와 소프트웨어 보안을 모두 확보했다는 점에서 보안 업계에 큰 전환점이 되었다. 또한, 이 제품은 드론, CCTV, IoT 단말기, 홈네트워크 등 다양한 저전력 디바이스에 적용될 예정이다. 특히 양자내성암호(PQC)와 유선 QKD(Quantum Key Distribution)를 결합한 하이브리드 보안 솔루션도 향후 선보일 계획이다.

투자포인트

1 독자적인 VIA PUF 기술 확보

기존 PUF 기술의 한계였던 온도/습도 등 환경 변화에 대한 취약점을 극복

아이씨티케이의 첫 번째 투자포인트는 독자적인 VIA PUF 기술을 통한 차별화된 기술 경쟁력이다. 2017년 설립된 아이씨티케이는 반도체 내부의 VIA홀을 활용한 독자적인 PUF 기술을 통해 기존 PUF 기술의 한계였던 온도/습도 등 환경 변화에 대한 취약점을 극복하며 상용화에 성공했다. PUF는 2001년 MIT에서 보안 인증 기술로 개발된 개념으로, 이후 국방, 반도체, IoT 등 다양한 분야의 보안 솔루션에 적용되었다. MIT에서 제안한 Arbiter PUF는 신호 도착 시간 차이를 기반으로 고유값을 생성하나, 온도와 습도 변화에 민감해 신뢰성이 낮았다. 한편, 2007년 Intrinsic-ID에서 상용화된 SRAM PUF는 전원이 켜질 때 메모리 셀의 초기 상태(0 또는 1) 패턴을 보안 키로 활용하지만, 온도와 습도 변화에 민감한 단점을 지녔다.

SRAM PUF 방식과 달리 ID가 바뀌지 않는다는 장점 보유

반면, 아이씨티케이의 VIA PUF 기술은 반도체 내부의 Via Hole(구리 및 텅스텐을 채우는 수직 통로)의 물리적 특성을 이용해 고유한 값을 만드는 방식이다. 각 칩에는 약 3,000~5,000개의 Via Hole이 형성되며, 각 Via Hole은 0 또는 1의 값을 생성해 고유한 디지털 지문(ID)을 만든다. 이로 인해 하나의 칩은 최대 2^{3000}개에서 2^{5000}개에 이르는 어마어마한 수의 고유 ID를 생성할 수 있다. 또한, 구리와 텅스텐은 1,000도 이상의 고온에서만 변형되기 때문에, VIA PUF는 온도나 습도 변화에도 안정적으로 동일한 ID를 유지한다. 이는 SRAM PUF와 달리 외부 환경에 민감하지 않아 보안성이 뛰어나다. 더불어, VIA PUF는 반도체 내부의 미세한 물리적 특성을 기반으로 한 수동소자 방식이기 때문에, 복제가 불가능하며 **침투 공격**과 **비침투 공격** 모두에 강한 내성을 지닌다.

▶ **침투 공격**(Invasive Attack): 실제로 반도체(칩)을 물리적으로 열거나 절단해 내부 회로를 분석해 보안 키를 알아내려는 공격이다. 예를 들어, 현미경이나 특수 장비를 사용해 칩을 해부하는 방식이다.

▶ **비침투 공격**(Non-Invasive Attack): 칩을 물리적으로 손상하지 않고 외부 신호를 분석해 보안 정보를 알아내려는 공격이다. 예를 들어, 칩이 작동할 때 발생하는 전력 소모, 전자기파, 발열 패턴 등을 측정해 내부 암호 정보를 추측하는 방식이다.

VIA PUF는 이러한 공격 방식 모두에 안전하다. 물리적 특성을 기반으로 고유 ID를 생성하기 때문에, 칩을 해부하거나 신호를 분석하더라도 동일한 보안 키를 재현하거나 복제하는 것이 사실상 불가능하다. 이러한 독자적인 기술력을 기반으로, 아이씨티케이 임직원들은 VIA PUF와 관련된 연구 성과를 다수의 논문을 통해 발표하며 기술적 전문성과 신뢰성을 인정받고 있다.

아이씨티케이 임직원 논문 발표

저자	논문 제목
Kim, T. W., Choi, B. D., & Kim, D. K. (2014)	Zero-bit error rate ID generation circuit using via formation probability in 0.18 μm CMOS process (0.18 μm CMOS 공정에서 비아(연결 구멍) 형성 확률을 이용한 무(無) 비트 오류 식별자(ID) 생성 회로 설계)
Jeon, D., Baek, J. H., Kim, D. K., & Choi, B. D. (2015)	Towards Zero Bit-Error-Rate Physical Unclonable Function: Mismatch-Based vs. Physical-Based Approaches in Standard CMOS Technology (제로 비트 오류율을 목표로 한 PUF(물리적 복제 방지 기능): 표준 CMOS 기술에서 불일치 기반과 물리적 기반 접근법 비교)
Jeon, D., & Choi, B. D. (2016)	Circuit design of physical unclonable function for security applications in standard CMOS technology (보안 응용을 위한 표준 CMOS 기술 기반 PUF(물리적 복제 방지 기능) 회로 설계)
Jeon, D., Baek, J. H., Kim, Y. D., Lee, J., Kim, D. K., & Choi, B. D. (2019)	A Physical Unclonable Function With Bit Error Rate < 2.3×10^{-8} Based on Contact Formation Probability Without Error Correction Code (에러 정정 코드 없이 접촉 형성 확률을 기반으로 비트 오류율 2.3×10^{-8} 미만을 달성한 PUF(물리적 복제 방지 기능))
Jeon, D., Lee, D., Kim, D. K., & Choi, B. D. (2022)	Contact PUF: Highly Stable Physical Unclonable Functions Based on Contact Failure Probability in 180 nm, 130 nm, and 28 nm CMOS Processes(접촉 PUF(Contact PUF): 180 nm, 130 nm, 28 nm CMOS 공정에서 접촉 실패 확률을 기반으로 한 고안정성 PUF)
Jeon, D., Lee, D., Kim, D. K., & Choi, B. D. (2023)	A 325F^2 Physical Unclonable Function Based on Contact Failure Probability With Bit Error Rate < 0.43 ppm After Preselection With 0.0177% Discard Ratio(선별 과정(0.0177% 불량 제외) 후 비트 오류율 0.43ppm 미만을 달성한 접촉 실패 확률 기반 325F^2 PUF(물리적 복제 방지 기능))

자료: 아이씨티케이, 한국IR협의회 기업리서치센터

2 글로벌 파트너십 확대를 통한 해외 시장 진출의 본격화

글로벌 빅테크 기업과 노트북 제조사 등으로 고객사 확대

아이씨티케이의 두 번째 투자포인트는 글로벌 파트너십 확대를 통한 해외 시장 진출의 본격화다. LG유플러스와의 협력을 통해 PQC PUF 칩 개발 및 양자보안 VPN 서비스를 상용화했으며, 현재는 글로벌 빅테크 기업과 노트북 제조사 등으로 고객사를 확대하고 있다. 2024년 매출의 50% 이상이 글로벌 기업들로부터 발생할 것으로 전망하며, GSA(Global Semiconductor Alliance)의 IoT Security Working Group 내 Root of Trust 요구조건 구축 담당업체로 선정되는 등 글로벌 시장에서 기술력을 인정받고 있다. 특히 독일의 SIEMENS, 영국의 Arm Holdings 등과 Root of Trust 표준화를 진행하고 있으며, 독일의 BOSCH, 네덜란드의 NXP 등 글로벌 기업과 공동 저자로 기술백서를 준비하는 등 글로벌 파트너십도 지속 확대하고 있다.

글로벌 시장별로는 미국에서 PC 보안 분야 점유율을 확대하고 국방, 항공으로 시장을 확대하고 있으며, 중국에서는 현지 유통업체를 통한 마케팅 확대와 함께 스마트카드, 스마트도어락, 전기오토바이 제조사 등에 칩 공급을 진행 또는 논의 중이다. 일본에서는 미국 레퍼런스를 기반으로 영업을 확대하고 있으며, 유럽에서는 글로벌 통신사와 신기술 도입에 대한 협력 관계를 구축하고 있다. 대만 및 아시아 지역에서는 팹리스 기업 IP 공급과 현지 네트워크 장비 제조사 등과의 협업을 추진하고 있다.

3 IP부터 솔루션까지 보안 전 영역 One-Stop 제공

보안 솔루션까지 전 영역의 제품 포트폴리오를 구축

아이씨티케이의 세 번째 투자포인트는 사업 영역의 다각화와 높은 수익성이다. 자체 지식재산권을 바탕으로 반도체(칩), 모듈/디바이스, 솔루션/프로젝트까지 One-Stop 솔루션을 제공할 수 있다. VIA PUF IP, RoT(신뢰점) IP, Cryptographic Algorithm(암호 알고리즘) IP, TRNG(True Random Number Generator, 진난수 생성기) IP 등 다양한 자체 IP를 보유하고 있으며, Giant1/3/5, MTR 등의 보안칩과 USIM/eSIM(통신 인증용), qTrust PCI(금융 보안), qTrust Net(네트워크 보안), LTE/5G Module, qTrust USB 등의 보안 모듈/디바이스, 그리고 ISF_FOTA(무선 소프트웨어 업데이트), ISF_KMS(키 관리 시스템), ISF_AUTH(인증 서비스), PQC(양자내성암호) 등의 보안 솔루션까지 전 영역의 제품 포트폴리오를 구축했다.

금융결제, 정품인증, 네트워크 해킹방지, 국방 및 공공기관 등 다양한 분야에 적용

아이씨티케이의 기술은 금융결제, 정품인증, 네트워크 해킹 방지, 국방 및 공공기관 등 다양한 분야에 적용된다. 예를 들어, 복제 불가능한 IC 카드, 전자신분증(eID), 금융기관용 암호키 보안모듈에 사용되며, 한국전력의 스마트 전력계량기(AMI) 공급, 무선공유기/통신 모뎀 보안, CCTV 및 로봇청소기 등 스마트 디바이스 보안, 개인용 PC 보안, PQC 인증 및 터널 서버 보안까지 폭넓은 응용이 가능하다. 특히, IP 사업부는 80% 이상의 높은 마진율, 칩 사업부는 30~40%의 안정적인 수익성을 보이며, 중장기적으로 우수한 수익성을 기대할 수 있다. 더 나아가, 딥페이크 방지 기술, 미세공정(Sub 10nm) 대응, 2.5D 패키징과 같은 첨단 기술 분야로 확장할 수 있는 가능성도 보유하고 있다.

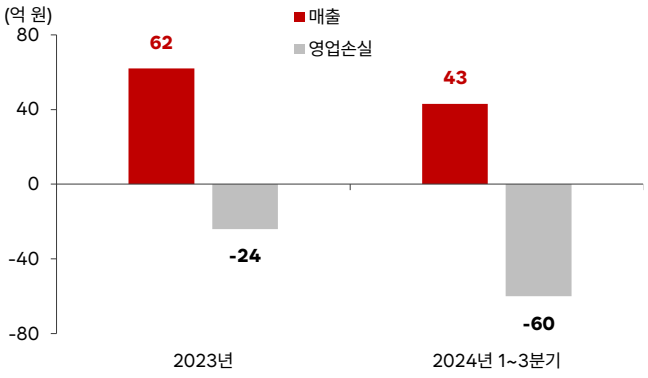
실적 추이 및 전망

1 2024년 실적 전망

매출 72억 원,
영업손실 56억 원으로 전망

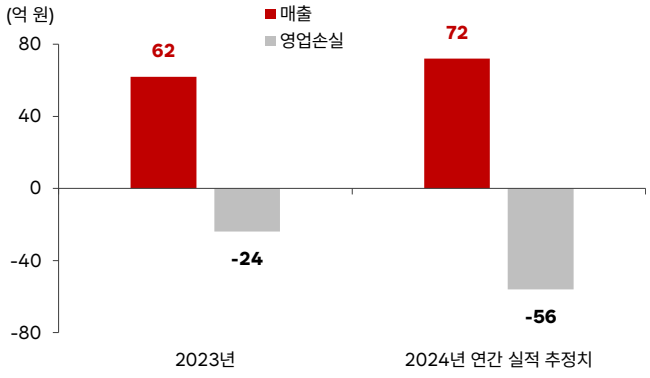
2024년 1분기부터 3분기까지 아이씨티케이는 43억 원의 매출, 60억 원의 영업손실을 기록했다. 4분기 실적 추정치를 포함하지 않은 상태에서 이를 2023년 실적(매출 62억 원, 영업손실 24억 원)과 단순비교해보면 매출은 증가했으나, 영업손실은 확대되었음을 알 수 있다. 2024년 4분기에 상대적으로 호실적(소폭의 흑자 전환)을 달성한다고 가정하더라도, 1~3분기에 발표된 실적을 바탕으로 2024년 연간 실적을 추정하면 매출 72억 원, 영업손실 56억 원으로 전망된다. 유틸리티/통신/팹리스 분야에서 복제 불가능한 특성을 지닌 보안칩의 응용처가 늘어나고, 동사가 이미 공급 중이던 보안칩의 점유율이 상승한 효과에 힘입어 매출은 증가할 것으로 예상한다. 그러나 IPO 당시 49명이던 임직원이 59명으로 증가하며 인건비 부담이 커져 영업손실이 늘어난 것으로 추정한다. 현재 신규 응용처 확대 단계에 있어 실적의 변동성이 클 수 있으나, 중장기적으로는 보안칩 시장 확대와 함께 수익성 개선을 기대한다. 다만 현 시점에서는 시장 개척 초기 단계로 인한 매출 규모의 제한적 특성을 고려할 때, 분기별 손익 변동성이 크게 나타날 수 있어 단기 실적 추정에는 보수적인 접근이 필요해 보인다.

2024년 1~3분기 실적과 2023년 실적 비교



자료: 아이씨티케이, 한국IR협의회 기업리서치센터

2024년 연간 기준 실적 추정치와 2023년 실적 비교



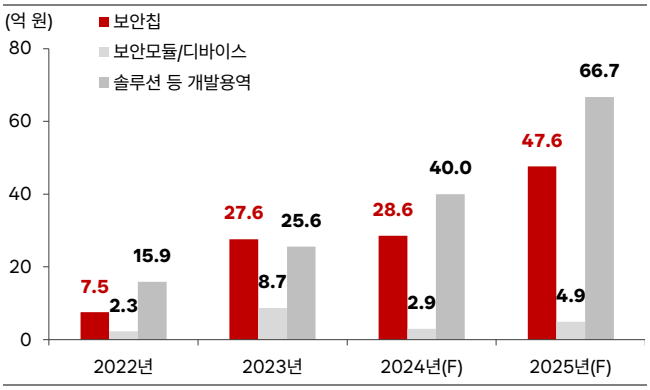
자료: 아이씨티케이, 한국IR협의회 기업리서치센터

2 2025년 실적 전망

매출과 영업손실은 각각 119억 원, 9억 원으로 전망

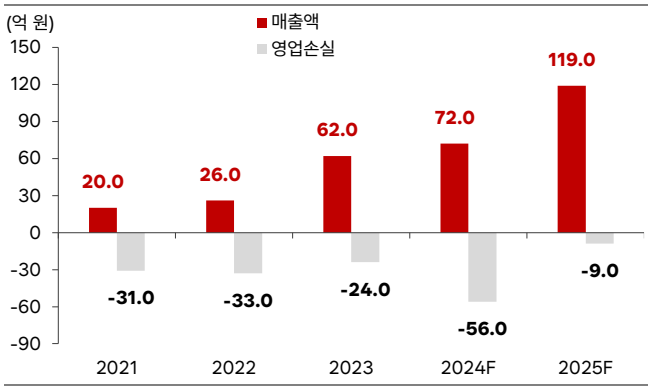
2025년 매출과 영업손실은 각각 119억 원, 9억 원으로 전망한다. 2025년 하반기부터 글로벌 빅테크 기업으로의 제품 공급 및 매출 시현이 본격화될 것으로 예상하며, 통신 분야에서 무선공유기용 보안칩과 CCTV용 보안칩 공급이 확대될 전망이다. 또한 IP 사업화 노력이 가시적 성과로 이어질 것으로 기대되는 점을 종합적으로 고려할 때, 매출이 100억 원을 상회할 가능성이 높다고 판단한다. 흑자 전환 여부에서는 보수적으로 예상한다. 59명으로 증가한 인력 구조와 IP 매출 발생 시점의 불확실성을 감안하여, 2025년에는 9억 원 수준의 영업손실이 발생할 것으로 추정한다.

부문별 매출액 추이



주: 2025년에 IP 매출이 발생하지 않은 것으로 가정
자료: 아이씨티케이, 한국IR협의회 기업리서치센터

연간 매출 및 영업이익 추이



주: 2025년에 IP 매출이 발생하지 않은 것으로 가정
자료: 아이씨티케이, 한국IR협의회 기업리서치센터

Valuation

동종 업계 peer 그룹과의 상대적 밸류에이션 비교 분석이 유의미한 상황

2025년 흑자전환이 어려울 것으로 예상, 수익성 지표인 P/E 밸류에이션 산출 불가

아이씨티케이는 2024년 5월 17일 코스닥시장 신규 상장 당일 공모가 대비 43.5% 상승한 28,700원으로 거래를 마감하며 높은 시장 관심도를 증명했다. 그러나 주가는 지속적인 하락세를 보이며 현재 10,000원 미만대에서 거래되며 공모가를 크게 하회하고 있다. 아이씨티케이의 향후 실적을 전망해보면, 2025년에는 매출 성장과 함께 의미 있는 적자 폭 축소를 기대한다. 특히 신규 사업 확장과 기존 사업부문의 실적 개선이 동반될 것으로 전망한다. 다만 고마진 IP 사업의 실적 기여 시기를 예측하기 어렵고, 이에 따라 2025년까지 흑자 전환이 어려울 것으로 예상해 수익성 지표인 P/E 밸류에이션 산출이 불가능한 상황이다. 이에 현 시점에서 주가의 절대적 밸류에이션 적정성을 판단하기에는 제약이 있으며, 동종 업계 peer 그룹과의 상대적 밸류에이션 비교 분석이 더욱 유의미할 것으로 판단한다.

동종 업종 밸류에이션

(단위: 주가는 현지통화, 시가총액과 매출과 영업이익은 십억 원, P/E는 배)

지수 및 기업명	관련성	종가	시가총액	매출액			영업이익			P/E		
				2023	2024F	2025F	2023	2024F	2025F	2023	2024F	2025F
아이씨티케이	**PUF, PQC**	**9,230**	**123**	**6**	**7**	**12**	**-2**	**-6**	**-1**	**N/A**	**N/A**	**N/A**
유비벨록스(한국)	PUF	6,670	98	544	N/A	N/A	49	N/A	N/A	6.5	N/A	N/A
LG유플러스(한국)	PUF	10,640	4,646	14,373	14,694	14,882	998	909	975	7.2	8.7	7.7
Synopsys(미국)	PUF IP	475	105,680	6,934	8,832	9,770	1,660	3,438	3,820	59.2	36.2	31.8
Cadence Design Systems (미국)	반도체 IP	258	101,986	5,305	6,670	7,490	1,623	2,833	3,270	71.4	43.7	38.4
Arm Holdings(영국)	반도체 IP	145	219,741	4,237	5,746	7,133	145	2,631	3,435	426.7	90.0	70.7
Rambus(미국)	반도체 IP	63	9,623	598	810	991	199	371	455	22.7	31.6	25.3
Adeia(미국)	반도체 IP	17	2,666	504	534	588	177	325	337	19.6	14.1	12.7
케이씨에스(한국)	PUF, PQC	12,170	146	48	N/A	N/A	3	N/A	N/A	30.0	N/A	N/A
NVE Corporation(미국)	PQC	74	514	39	N/A	N/A	24	N/A	N/A	25.5	N/A	N/A
Infineon Technologies(독일)	EAL5+	39	76,047	22,869	22,689	22,885	5,536	4,125	3,771	13.2	20.9	24.6
Nuvoton Technology(대만)	EAL5+	97	1,796	1,489	1,437	1,647	71	19	106	24.7	77.8	17.8
NXP Semiconductors (네덜란드)	EAL5+	237	86,344	17,220	18,148	17,359	4,749	6,173	5,664	21.5	18.2	20.1
Thales(프랑스)	EAL5+	182	56,748	25,945	30,443	32,644	1,861	3,532	4,045	27.4	21.3	19.3
평균(Arm Holdings 포함)										**58.1**	**36.2**	**26.8**
평균(Arm Holdings 제외)										**29.3**	**30.3**	**22.0**

주: 1) 동종 업종 선정 기준: PUF 또는 PQC와의 관련성을 참고로 했으며 그 밖에 기반 기술을 기반으로 반도체 IP 사업을 영위하는 곳(Cadence Design Systems, Arm Holdings, Rambus, Adeia) 및 암호화 알고리즘의 내구성, 키 재생산성, 공격 복원력을 의미하는 EAL5+ 등급의 인증을 보유한 반도체 기업 또는 보안 서비스 기업(Infineon Technologies, Nuvoton Technology, NXP Semiconductors, Thales) 포함, 2) 한국 기업 중에 유비벨록스와 LG유플러스: 아이씨티케이와 비즈니스 모델이 다르지만, 유비벨록스는 스마트카드와 PUF 칩을 포함한 전자 장치 및 이의 동작 방법 특허를 아이씨티케이와 공동 출원했고, LG유플러스는 동 기술을 기반으로 PUF-eSIM을 개발 완료, 3) 한국 기업 중에 케이씨에스: 언론 보도에 따르면 SK텔레콤과 협업하여 PUF, PQC 기술이 적용된 제품을 2024년에 발표했으므로 동종 업종에 포함

자료: FnGuide, ChatGPT, Claude AI, Perplexity, 한국IR협의회 기업리서치센터

PUF 및 PQC 기술 관련 기업군으로 유비벨록스, LG유플러스, 케이씨에스 등이 대표적

아이씨티케이의 peer 그룹은 크게 세 가지 범주로 구분할 수 있다. 첫째, PUF 및 PQC 기술 관련 기업군으로 유비벨록스, LG유플러스, 케이씨에스 등이 대표적이다. 특히 유비벨록스는 아이씨티케이와 스마트카드 및 PUF 칩 관련 특허를 공동 출원한 이력이 있으며, LG유플러스는 해당 기술을 활용한 PUF-eSIM 개발을 완료했다. 케이씨에스의 경우 언론보도에 따르면 SK텔레콤과의 협업을 통해 2024년 PUF, PQC 기술이 적용된 신제품을 발표하며 시장 진출을 본격화했다.

이들 기업군의 밸류에이션을 살펴보면, LG유플러스의 경우 다수의 통신 섹터 애널리스트들이 커버리지를 제공하고 있으나, 전통적인 이동통신사의 특성으로 인해 P/E 밸류에이션이 10배 미만으로 형성되어 있다. 유비벨록스와 케이씨에스의 경우 비교 가능한 P/E 밸류에이션이 부재한 상황이다.

한편, 동 기업군에 포함된 미국의 NVE Corporation은 PQC 기술을 접목한 자기 터널 접합(Magnetic Tunnel Junction) 기반의 PUF를 국방용으로 개발하며 기술적 유사성을 보이고 있다. 그러나 미국 시장에서 스몰캡으로 분류되어 애널리스트 커버리지 및 컨센서스 확보가 제한적이므로, 밸류에이션 비교 목적의 활용에는 한계가 있다.

반도체 IP 사업을 영위하는 글로벌 기업군 존재

둘째, 반도체 IP 사업을 영위하는 글로벌 기업군으로 Synopsys, Cadence Design Systems, Arm Holdings, Rambus, Adeia 등이 있다. 이들은 아이씨티케이와 유사하게 기반 기술을 활용한 IP 비즈니스 모델을 구축하고 있어 사업구조 측면에서 비교 가능성이 높다. 특히 Synopsys는 아이씨티케이의 주요 경쟁사인 Intrinsic-ID를 인수하며 PUF 기술 시장 내 입지를 강화했다는 점에서 주목할 만하다.

EAL5+ 등급의 보안 인증을 보유한 글로벌 반도체 및 보안 서비스 기업군 존재

셋째, EAL5+ 등급의 보안 인증을 보유한 글로벌 반도체 및 보안 서비스 기업군으로 Infineon Technologies, Nuvoton Technology, NXP Semiconductors, Thales 등이 있다. EAL5+ 인증은 PUF 및 PQC 기술이 적용된 보안 시스템에서 특히 중요한 의미를 지닌다. 해당 인증은 양자 컴퓨터 시대의 암호 해독 위협에 대응하기 위한 고도화된 보안 요구사항을 충족함을 의미하며, 특히 키 생성 및 저장 메커니즘의 안정성을 보장한다. 이러한 맥락에서 EAL5+ 인증 보유 기업들은 암호화 알고리즘의 내구성, 키 재생산성, 공격 복원력 등에서 최고 수준의 기술력을 인정받은 기업들로 평가받고 있다.

상기 3가지 기업군 중에서 가장 P/E 밸류에이션이 높은 영역은 반도체 IP 기업군

상기 3가지 기업군 중에서 가장 P/E 밸류에이션이 높은 영역은 반도체 IP 기업군이다. 특히 글로벌 반도체 IP 시장 1위 기업인 Arm Holdings의 P/E 밸류에이션은 압도적인 프리미엄을 형성하고 있다. 이는 Arm Holdings가 보유한 독보적인 시장 지위와 모바일 CPU 아키텍처 시장에서의 사실상의 표준(De facto standard) 지위에 기인한다. 또한 AI 반도체, 자율주행, IoT 등 차세대 성장 산업에서 Arm Holdings의 IP가 핵심적인 역할을 할 것으로 전망되는 점, 그리고 IP 비즈니스 모델 특성상 한계비용이 낮아 수익성이 매우 높은 점 등이 고평가 요인으로 작용하고 있다.

아이씨티케이는 IP 비즈니스로의 전환을 핵심 전략으로 추진

이와 같은 이유로 아이씨티케이는 높은 수익성과 확장성을 지닌 IP 비즈니스로의 전환을 핵심 전략으로 추진하고 있다. 2024년 기준 IP 매출 비중은 미미한 수준이나, PUF 관련 IP 포트폴리오 확대와 글로벌 고객사 확보를 위해 전사적 역량을 집중하고 있다. 특히 양자 컴퓨팅 시대를 대비한 차세대 보안 수요 증가에 따라 아이씨티케이의 핵심 기술이 IP 형태로 폭넓게 채택될 것으로 기대되는 만큼, 향후 IP 매출 비중이 점진적으로 확대될 것으로 전망한다.

IP 사업 비중이 확대될 경우 반도체 IP 기업군의 높은 밸류에이션을 반영한 리레이팅 가능성이 존재

2025년 이후 아이씨티케이가 매출 성장세를 이어가며 의미 있는 수준의 당기순이익을 시현한다면, P/E 밸류에이션 산출이 가능해질 것으로 예상한다. 이 경우 아이씨티케이의 적정 밸류에이션은 상기 3개 기업군의 평균 P/E 수준에서 형성될 것으로 전망한다. 특히 주목할 점은 IP 사업 비중이 확대될 경우 반도체 IP 기업군의 높은 밸류에이션을 반영한 리레이팅 가능성이 존재한다는 것이다. 실제로 아이씨티케이는 기술 사업화에 대한 강력한 의지를 보이고 있으며, 한국의 중소기업임에도 불구하고 PUF 관련 분야 및 각종 인증 기관으로부터 기술 표준화에 기여하는 기업으로서의 위상을 인정받고 있다. 이는 향후 IP 비즈니스 모델로의 성공적인 전환 가능성을 시사하는 긍정적 신호로 해석된다. 장기적 관점에서 아이씨티케이의 성장 잠재력과 기업가치 제고 가능성을 조심스럽게 기대해 볼 수 있는 대목이다.

리스크 요인

1 PUF 기술은 아직 시장 대중화 단계에 접어들지 않은 신기술

아이씨티케이의 1번째 리스크는 PUF(Physical Unclonable Function) 기술의 시장 대중화 속도이다. 아이씨티케이는 반도체 보안 기술의 핵심인 H/W 기반 VIA PUF 보안칩을 통해 기존 S/W 기반 보안 기술이 지닌 보안 취약성과 환경 민감성을 극복하며, 차별화된 기술 경쟁력을 확보했다. VIA PUF는 반도체 제조 과정에서 발생하는 미세한 물리적 특성을 고유한 보안 키로 활용해 복제가 불가능한 고유 ID를 생성하는 기술이다. 해당 기술은 이미 양산화에 성공했으며, 일부 종합 반도체 기업에서도 VIA PUF 기술에 관심을 보이며 차세대 보안 기술로서의 가능성을 인정받고 있다. 그러나, PUF 기술은 여전히 시장 대중화 단계에는 이르지 못한 신기술인 만큼, 기존 S/W 기반의 암호화 및 인증 기술이 당분간 주류 기술로 남을 가능성이 있다. 이러한 상황은 시장 점유율 확대에 시간이 소요될 수 있음을 시사하며, 전통적인 보안 솔루션에 익숙한 고객사의 기술 전환 속도가 예상보다 느릴 경우 아이씨티케이의 매출 성장세에 일정한 영향을 줄 수 있다.

2 주요 경쟁사 및 신규 진입자에 의한 시장 위협

아이씨티케이의 2번째 리스크는 주요 경쟁사 및 신규 진입자에 의한 시장 위협이다. 현재 반도체 업종에서 PUF(Physical Unclonable Function) 기술을 상용화한 중소기업은 아이씨티케이, Intrinsic ID(미국 Synopsys에 인수), eMemory(대만 상장 기업), NVE Corporation(미국 상장 기업: 나노 스케일의 전자 소자인 자기 터널 접합(Magnetic Tunnel Junction)의 물리적 특성을 이용한 PUF를 국방용으로 개발) 등 소수에 불과하다. 경쟁사들은 SRAM PUF, NeoPUF, 자기 터널 접합 기반 PUF 등 전류나 자기장을 통해 상태를 변경할 수 있는 능동적인 특성을 보유한 능동소자 기반 PUF 기술을 보유하고 있으나, 아이씨티케이는 외부 환경 변화에 내성적인 수동소자 기반 VIA PUF 기술로 차별성을 확보했다. 그러나 2024년 3월 20일, 글로벌 IP 및 반도체 설계 자동화(EDA) 대기업인 시놉시스(Synopsys)가 Intrinsic ID를 인수하며 경쟁 구도가 급변했다. 시놉시스는 인수를 계기로 네덜란드에 PUF 기술 우수 센터를 설립해 대규모 투자와 연구개발을 강화할 계획을 발표했다. 이러한 경쟁사의 기술력 향상 및 시장 확대는 아이씨티케이의 시장 점유율과 지배력에 위협이 될 수 있다. 또한, 향후 대기업이나 신규 기술을 기반으로 한 스타트업이 시장에 진입할 경우, 기술 혁신과 가격 경쟁을 통해 아이씨티케이의 시장 지위를 약화시킬 위험이 있다. 따라서, 업계 동향과 경쟁사 전략을 면밀히 모니터링하며, 차별화된 기술력과 신사업 발굴을 통해 경쟁 우위를 지속적으로 확보하는 전략이 요구된다.

3 전방시장 성장 둔화 및 산업환경 변화 가능성

아이씨티케이의 3번째 리스크는 전방시장 성장 둔화 및 산업환경 변화 가능성이다. 아이씨티케이는 IoT 및 5G 전방시장의 수요에 크게 의존하며, VIA PUF 기반 보안칩 제품군을 통해 해당 시장의 보안 수요를 선점해왔다. 그러나 5G 인프라 확장 지연, IoT 시장의 투자 위축, 글로벌 경기 침체 등으로 전방시장의 성장세가 기대에 미치지 못할 경우, 아이씨티케이의 제품 수요 감소와 매출 타격이 불가피할 수 있다. 특히, 반도체 및 통신 산업의 특성상 주요 고객사들의 신규 설비투자가 지연되면 공급망 전체에 파급 효과를 미치며, 이는 아이씨티케이의 수익성 저하로 이어질 수 있다. 또

한, 산업 구조 변화 및 기술 트렌드 전환은 추가적인 위험 요인이다. 예컨대, 시장이 대체 보안 기술이나 통합 보안 솔루션으로 빠르게 전환할 경우, VIA PUF의 시장 지위가 약화될 가능성이 있다. 동시에, 전방시장 내 경쟁 환경이 재편되거나 신규 대기업이 진입해 가격 경쟁이 심화되면, 아이씨티케이의 수익성 확보에 부담이 될 수 있다. 이처럼 외부 산업 환경과 기술 변화는 회사의 경영 성과에 장기적인 불확실성을 초래할 수 있다.

포괄손익계산서

(억원)	2021	2022	2023	2024F	2025F
매출액	20	26	62	72	119
증가율(%)	136.0	28.3	141.1	15.6	66.7
매출원가	9	15	28	29	41
매출원가율(%)	45.0	57.7	45.2	40.3	34.5
매출총이익	11	10	34	42	78
매출이익률(%)	55.0	40.0	54.4	59.0	65.6
판매관리비	42	44	57	98	87
판관비율(%)	210.0	169.2	91.9	136.1	73.1
EBITDA	-26	-30	-18	-41	-17
EBITDA 이익률(%)	-130.0	-115.5	-28.9	-56.7	-14.5
증가율(%)	적지	적지	적지	적지	적지
영업이익	-31	-33	-24	-56	-9
영업이익률(%)	-155.3	-129.9	-38.2	-78.1	-7.4
증가율(%)	적지	적지	적지	적지	적지
영업외손익	-21	-74	-67	-46	-41
금융수익	6	2	2	8	14
금융비용	22	77	69	53	53
기타영업외손익	-5	0	-1	-1	-1
종속/관계기업관련손익	0	0	1	1	1
세전계속사업이익	-53	-108	-90	-101	-49
증가율(%)	적지	적지	적지	적지	적지
법인세비용	0	0	0	-3	-2
계속사업이익	-53	-108	-90	-97	-47
중단사업이익	0	0	0	0	0
당기순이익	-53	-108	-90	-97	-47
당기순이익률(%)	-262.7	-419.7	-146.0	-136.1	-39.2
증가율(%)	적지	적지	적지	적지	적지
지배주주지분 순이익	-53	-108	-90	-97	-47

재무상태표

(억원)	2021	2022	2023	2024F	2025F
유동자산	54	80	80	412	376
현금성자산	13	27	15	337	251
단기투자자산	25	13	27	31	52
매출채권	2	3	10	11	19
재고자산	8	18	14	17	28
기타유동자산	5	18	14	16	26
비유동자산	19	19	24	10	22
유형자산	2	3	7	-6	4
무형자산	10	10	9	8	7
투자자산	4	4	4	4	7
기타비유동자산	3	2	4	4	4
자산총계	73	98	104	422	397
유동부채	279	407	8	14	24
단기차입금	0	0	0	0	0
매입채무	2	1	0	0	0
기타유동부채	277	406	8	14	24
비유동부채	3	2	2	19	31
사채	0	0	0	0	0
장기차입금	0	0	0	0	0
기타비유동부채	3	2	2	19	31
부채총계	283	410	10	33	55
지배주주지분	-210	-311	94	389	343
자본금	30	30	56	66	66
자본잉여금	24	24	486	863	863
자본조정 등	-139	-133	-124	-119	-119
기타포괄이익누계액	0	1	0	0	0
이익잉여금	-125	-233	-324	-421	-468
자본총계	-210	-311	94	389	343

현금흐름표

(억원)	2021	2022	2023	2024F	2025F
영업활동으로인한현금흐름	-31	-45	-12	-66	-64
당기순이익	-53	-108	-90	-97	-47
유형자산 상각비	3	2	4	14	-10
무형자산 상각비	2	1	1	1	1
외환손익	0	0	0	0	0
운전자본의감소(증가)	-6	-22	-2	17	-8
기타	23	82	75	-1	0
투자활동으로인한현금흐름	-13	11	-21	-5	-23
투자자산의 감소(증가)	0	0	0	0	-2
유형자산의 감소	0	0	0	0	0
유형자산의 증가(CAPEX)	-1	-1	-3	-1	0
기타	-12	12	-18	-4	-21
재무활동으로인한현금흐름	48	48	21	393	1
차입금의 증가(감소)	0	0	0	0	1
사채의증가(감소)	0	0	0	0	0
자본의 증가	0	0	23	387	0
배당금	0	0	0	0	0
기타	48	48	-2	6	0
기타현금흐름	1	-0	-0	0	0
현금의증가(감소)	5	14	-12	322	-86
기초현금	8	13	27	15	337
기말현금	13	27	15	337	251

주요투자지표

	2021	2022	2023	2024F	2025F
P/E(배)	N/A	N/A	N/A	N/A	N/A
P/B(배)	N/A	N/A	0.0	3.3	3.6
P/S(배)	0.0	0.0	0.0	17.1	10.3
EV/EBITDA(배)	N/A	N/A	N/A	N/A	N/A
배당수익률(%)	N/A	N/A	N/A	0.0	0.0
EPS(원)	-652	-1,233	-902	-781	-352
BPS(원)	-2,455	-3,474	847	2,932	2,580
SPS(원)	248	294	618	573	898
DPS(원)	0	0	0	0	0
수익성(%)					
ROE	25.7	41.4	83.2	-40.3	-12.8
ROA	-78.2	-125.8	-89.2	-37.0	-11.4
ROIC	-145.3	-101.1	-51.6	-134.7	-18.1
안정성(%)					
유동비율	19.2	19.6	1,008.7	2,905.2	1,590.3
부채비율	-134.8	-131.6	10.7	8.4	16.0
순차입금비율	-112.9	-115.7	-43.8	-94.3	-88.0
이자보상배율	-1.6	-1.3	-1.5	-975.5	-107.9
활동성(%)					
총자산회전율	0.3	0.3	0.6	0.3	0.3
매출채권회전율	12.0	8.8	9.5	6.9	8.0
재고자산회전율	3.1	2.0	3.8	4.6	5.3

최근 3개월간 한국거래소 시장경보제도 지정 여부

시장경보제도란?

한국거래소 시장감시위원회는 투기적이거나 불공정거래 개연성이 있는 종목 또는 주가가 비정상적으로 급등한 종목에 대해 투자자주의 환기 등을 통해 불공 정거래를 사전에 예방하기 위한 제도를 시행하고 있습니다.
시장경보제도는 「투자주의종목 투자경고종목 투자위험종목」의 단계를 거쳐 이루어지게 됩니다.

※관련근거: 시장감시규정 제5조의2, 제5조의3 및 시장감시규정 시행세칙 제3조~제3조의 7

종목명	투자주의종목	투자경고종목	투자위험종목
아이씨티케이	X	X	X

발간 History

발간일	제목
2025.02.25	아이씨티케이-PUF 기반 보안칩과 양자내성암호(PQC) 기술 선도

Compliance notice

본 보고서는 한국거래소, 한국예탁결제원과, 한국증권금융이 공동으로 출연한 한국IR협의회 산하 독립 (리서치) 조직인 기업리서치센터가 작성한 기업분석 보고서입니다. 본 자료는 시가총액 5천억원 미만 중소형 기업에 대한 무상 보고서로, 투자자들에게 국내 중소형 상장사에 대한 양질의 투자 정보 제공 및 건전한 투자문화 정착을 위해 작성되었습니다.

- 당사 리서치센터는 본 자료를 제3자에게 사전 제공한 사실이 없습니다.
- 본 자료를 작성한 애널리스트는 자료작성일 현재 해당 종목과 재산적 이해관계가 없습니다.
- 본 자료를 작성한 애널리스트와 그 배우자 등 관계자는 자료 작성일 현재 조사분석 대상법인의 금융투자상품 및 권리를 보유하고 있지 않습니다.
- 본 자료는 중소형 기업 소개를 위해 작성되었으며, 매수 및 매도 추천 의견은 포함하고 있지 않습니다.
- 본 자료에 게재된 내용은 애널리스트의 의견을 정확하게 반영하고 있으며, 외부의 부당한 압력이나 간섭 없이 신의 성실하게 작성되었음을 확인합니다.
- 본 자료는 투자자들의 투자판단에 참고가 되는 정보제공을 목적으로 배포되는 자료입니다. 본 자료에 수록된 내용은 자료제공일 현재 시점의 당사 리서치센터의 추정치로서 오차가 발생할 수 있으며 정확성이나 완벽성은 보장하지 않습니다.
- 본 조사자료는 투자 참고 자료로만 활용하시기 바라며, 어떠한 경우에도 투자자의 투자 결과에 대한 법적 책임 소재의 증빙자료로 사용될 수 없습니다.
- 본 조사자료의 지적재산권은 당사에 있으므로, 당사의 허락 없이 무단 복제 및 배포할 수 없습니다.
- 본 자료는 텔레그램에서 "한국IR협의회(https://t.me/kirsofficial)" 채널을 추가하시어 보고서 발간 소식을 안내받으실 수 있습니다.
- 한국IR협의회가 운영하는 유튜브 채널 'IRTV'에서 1) 애널리스트가 직접 취재한 기업탐방으로 CEO인터뷰 등이 있는 '小中한탐방'과 2) 기업보고서 심층해설방송인 '小中한 리포트 가치보기'를 보실 수 있습니다.