Safe with us

INVESTOR RELATIONS 2024

ICTK
SAFE WITH US

Disclaimer

본 자료는 기관투자자들을 대상으로 실시되는 PRESENTATION에서 정보 제공을 목적으로 주식회사 아이씨티케이(이하 '회사')에 의해 작성되었으며 이의 반출, 복사 또는 타인에 대한 재배포는 금지됨을 알려드립니다. 본 PRESENTATION에의 참석은 위와 같은 제한 사항의 준수에 대한 동의로 간주될 것이며, 제한 사항에 대한 위반은 관련 '자본시장과 금융투자업에 관한 법률'에 대한 위반에 해당될 수 있음을 유념해주시기 바랍니다.

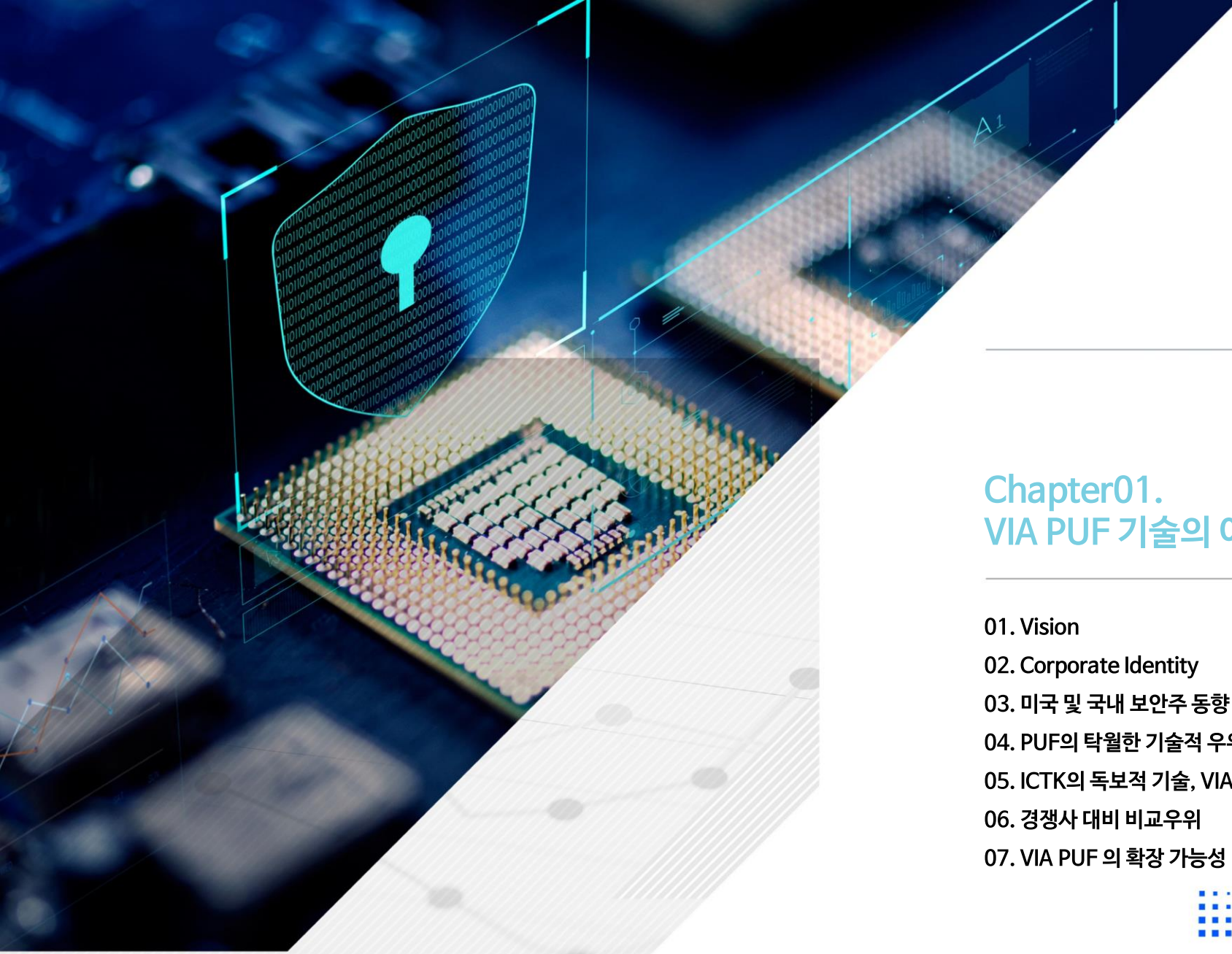
본 자료에 포함된 '예측정보'는 개별 확인 절차를 거치지 않은 정보들입니다. 이는 과거가 아닌 미래의 사건과 관계된 사항으로 회사의 향후 예상되는 경영현황 및 재무실적을 의미하고, 표현상으로는 '예상', '전망', '계획', '기대', '(E)' 등과 같은 단어를 포함합니다. 위 '예측정보'는 향후 경영환경의 변화 등에 따라 영향을 받으며, 본질적으로 불확실성을 내포하고 있는 바, 이러한 불확실성으로 인하여 실제 미래실적은 '예측정보'에 기재되거나 암시된 내용과 중대한 차이가 발생할 수 있습니다. 또한, 향후 전망은 PRESENTATION 실시일 현재를 기준으로 작성된 것이며 현재 시장상황과 회사의 경영방향 등을 고려한 것으로 미래 시장환경의 변화와 전략수정 등에 따라 변경될 수 있으며, 별도의 고지 없이 변경 될 수 있음을 양지하시기 바랍니다.

본 자료의 활용으로 인해 발생하는 손실에 대하여 회사 및 회사의 임원들은 그 어떠한 책임도 부담하지 않음을 알려드립니다(과실 및 기타의 경우 포함). 본 문서는 주식의 모집 또는 매출, 매매 및 청약을 위한 권유를 구성하지 아니하며 문서의 그 어느 부분도 관련 계약 및 약정 또는 투자 결정을 위한 기초 또는 근거가 될 수 없음을 알려드립니다.

ICTK
SAFE WITH US

Safe with us

Contents



Chapter01.
VIA PUF 기술의 이해

01. Vision
02. Corporate Identity
03. 미국 및 국내 보안주 동향
04. PUF의 탁월한 기술적 우위
05. ICTK의 독보적 기술, VIA PUF
06. 경쟁사 대비 비교우위
07. VIA PUF 의 확장 가능성

ICTK
SAFE WITH US

01 Vision


수많은 IoT 기기들이 하나로 연결되는 초연결 시대
이들의 Life cycle을 관리하기 위한 신뢰점(Root of Trust)가 필수
ICTK
“Safe with us”
ICTK는 VIA PUF 기술을 바탕으로 IoT 기기에 생체 아이디를 부여하여
가장 신뢰성 높은 네트워크 환경을 구축하는데 앞장섭니다.

02 Corporate Identity

ICTK

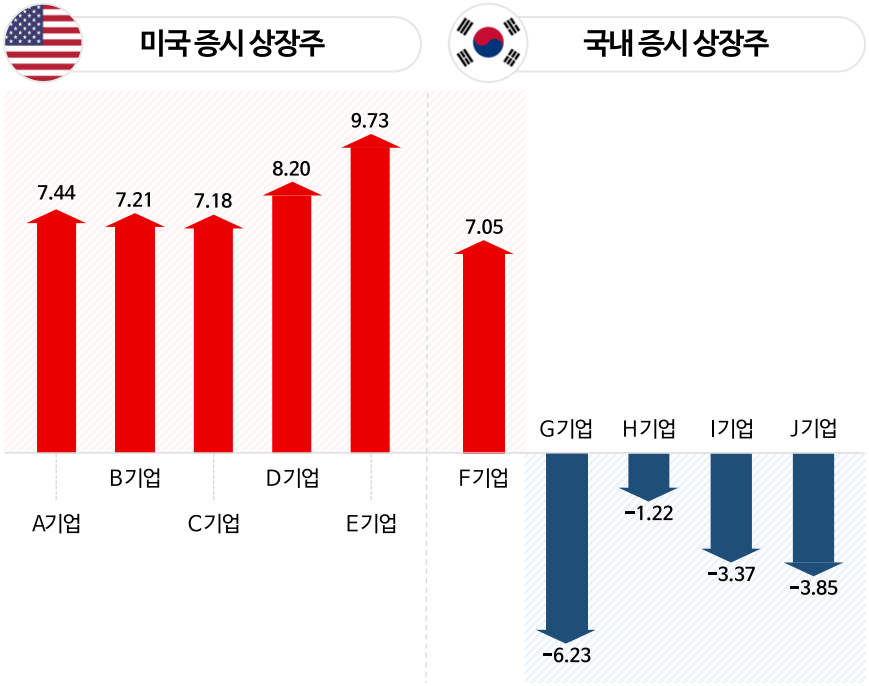
AI, 양자컴퓨터 시대 도래로 해킹의 원천 방지를 위한 Root of Trust 필요

“ ICTK 는 VIA PUF라는 H/W 기반 Inborn Key로 해결 ”

03 미국 및 국내 보안주 동향

미국 증시에 상장되어 있는 보안 관련 주식과 상반된 흐름을 보여주는 국내 보안 관련 주식

주요 사이버보안주 주가 등락률

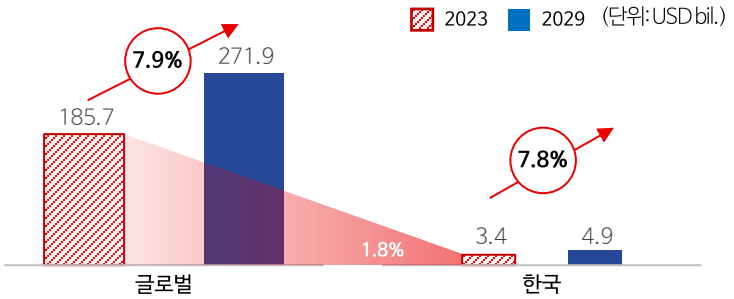


※ 9.30~10.25 기준, 단위:%

※ 9.30~10.28 기준, 단위:%

Cyber Security market

국내 보안 시장은 글로벌 대비 1.8%에 불과



출처: Statista

2024. 2분기 매출액 비중

국내 주요 보안 상장회사의 해외 수출 비중은 평균 3.4% 에 불과

(단위: 백만원)

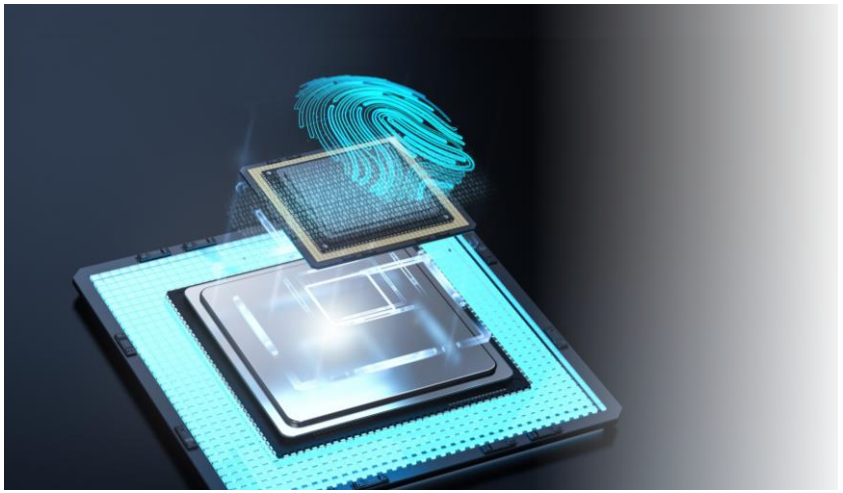
	F기업	G기업	H기업	J기업
내수	105,893	17,316	18,357	44,658
수출	3,545	2,123	518	318
합계	109,438	19,439	18,875	44,976

출처: 사업보고서

ICTK의 VIA PUF는 글로벌에서 인정 받는 국내 유일의 보안 IP

04 PUF의 탁월한 기술적 우위

기존 S/W 기반 Key Injection 방식으로는 해킹 방지 불가



S/W 기반 Key Injection 방식		H/W 기반 Inborn Key(PUF)
외부 ID 주입 후 메모리 저장 방식	방식	복제 불가한 Chip 고유 ID 생성
Key 관리 부실 및 Key 주입 과정 중 유출 위험	Key 유출	Key 값 탈취 문제 원천 방지
보안에 취약	해킹 방지	Zero-trust 기반의 강력한 접근 통제

05 ICTK의 독보적 기술, VIA PUF

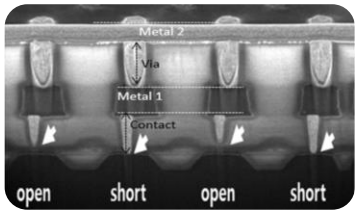
ICTK

반도체 제조 공정 상 나타나는 각 Chip 고유의 난수 값을 활용한 VIA PUF 기술

VIA PUF 구조

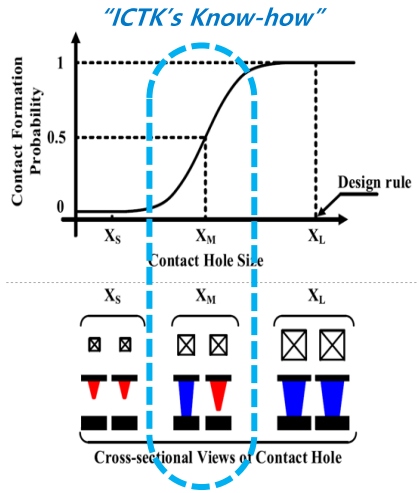
반도체의 메탈층간 연결해주는 VIA Hole을 활용하여 그 지름의 크기를 줄여 open과 short를 랜덤하게 발생하도록 컨디션하여 Physically Unclonable Function (PUF)를 형성

반도체 Standard 구조

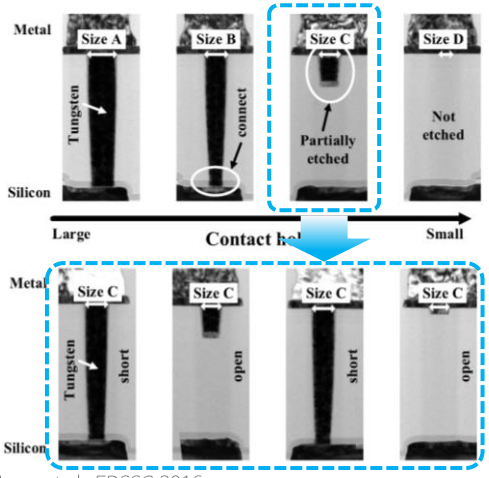


Metal Layer2	금속 배선층
VIA Layer 1 (VIA1)	Metal Layer를 수직으로 연결 신호 전달 배선 (구리 Cu, 텅스텐 W, 티타늄 Ti, 알류미늄 Al 등)
Metal Layer1	금속 배선층
Contact (VIA0)	첫번째 수직 배선층 단위소자의 전극에 직접 연결되어 있는 Layer
Substrate Layer	반도체 소자 구현

Contact 홀 크기에 따라 VIA hole 생성



VIA PUF의 형성



D. Jeon, et al, *EDSSC*, 2016

VIA PUF 장점

- 수학적 복제불가
- 물리적 복제불가
- 침투 • 비침투 공격방어

06 경쟁사 대비 비교우위

ICTK

글로벌 경쟁 기업을 압도하는 ICTK만의 VIA PUF 기술

Category	SRAM PUF (Intrinsic ID)	Neo PUF (eMemory)	VIA PUF
소자 종류	능동소자	능동소자	**수동소자**
항상성 (PVT: Process, Voltage, Temperature)	Sensitive	Less sensitive	**Robust** (형성된 VIA는 값이 변하지 않음)
무작위성 (NIST 인증 통과 여부)	통과	통과	**통과**
유일성 (Hamming distance, 이상적 값 50%)	47%	50%	**50%**
비트 에러율 (이상적 값 0%)	5.5%	0.0%	**0.0%**
오류 정정 코드 필요성	**필요함** (오류 정정 코드 적용)	**필요함** (오류 정정 방법 없음)	**필요 없음** (PVT Variation 없음)
추가 회로 필요성	**필요함** (Helper Data, Anti-aging, 오류 정정 코드)	**필요함** (High Voltage PGM, Charge Pump)	**필요 없음**
보안키 길이 신축성	중간 (블록 사이즈 한계)	중간 (블록 사이즈 한계)	**높음**
물리적 공격 대비 강건성 (침투 공격 방지)	중간 (IP Block 노출)	중간 (IP Block 노출)	**높음** (camouflaged 위장)

추가 회로가 필요하지 않아 높은 원가경쟁력 확보

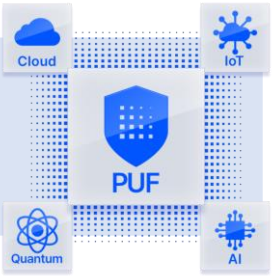
상용화 약점

PUF값 쉽게 노출

현재 업체들이 개발중인 PUF 기술은 태생적으로 **"항상성"** 문제를 지님

ICTK

경쟁사 단점을 커버하는 ICTK 기술



07 VIA PUF의 확장 가능성

다양한 첨단산업 내 VIA PUF의 가파른 수요 확장 가능성 보유

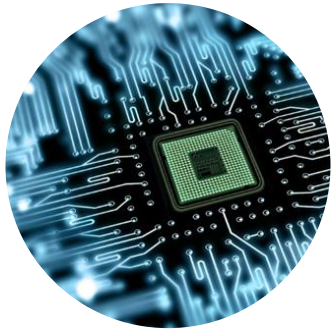
딥페이크

딥페이크 기술의 발달로 진본과 변조된 이미지의 구분이 어려워져 사회적으로 많은 문제를 야기. 미국 검찰에서는 딥페이크로 생성된 이미지로 인하여 증거 확보 및 수사에 어려움 초래

구글 등에서는 생성형 AI로 만들어진 이미지에 워터마크 삽입을 추진하고 있으나, 누구도 진본에 대한 확신을 주지 못함

VIA PUF IP로 고유한 ID 값을 부여하여 이미지 촬영시 진본임을 알 수 있는 워터마크 삽입(특허 출원중)

Sub 10nm

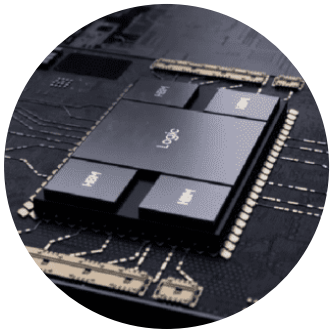


Sub 10nm 이하의 미세공정으로 갈수록 전류의 간섭으로 기존 PUF 기술로 구현시 bias 문제 발생

기존 PUF 의 경우 ECC 및 Helper data를 추가로 요구하여 100배의 추가 bit가 필요

VIA PUF IP는 구조물을 이용하여 해당 이슈가 없음
경쟁 기술 대비 경쟁우위

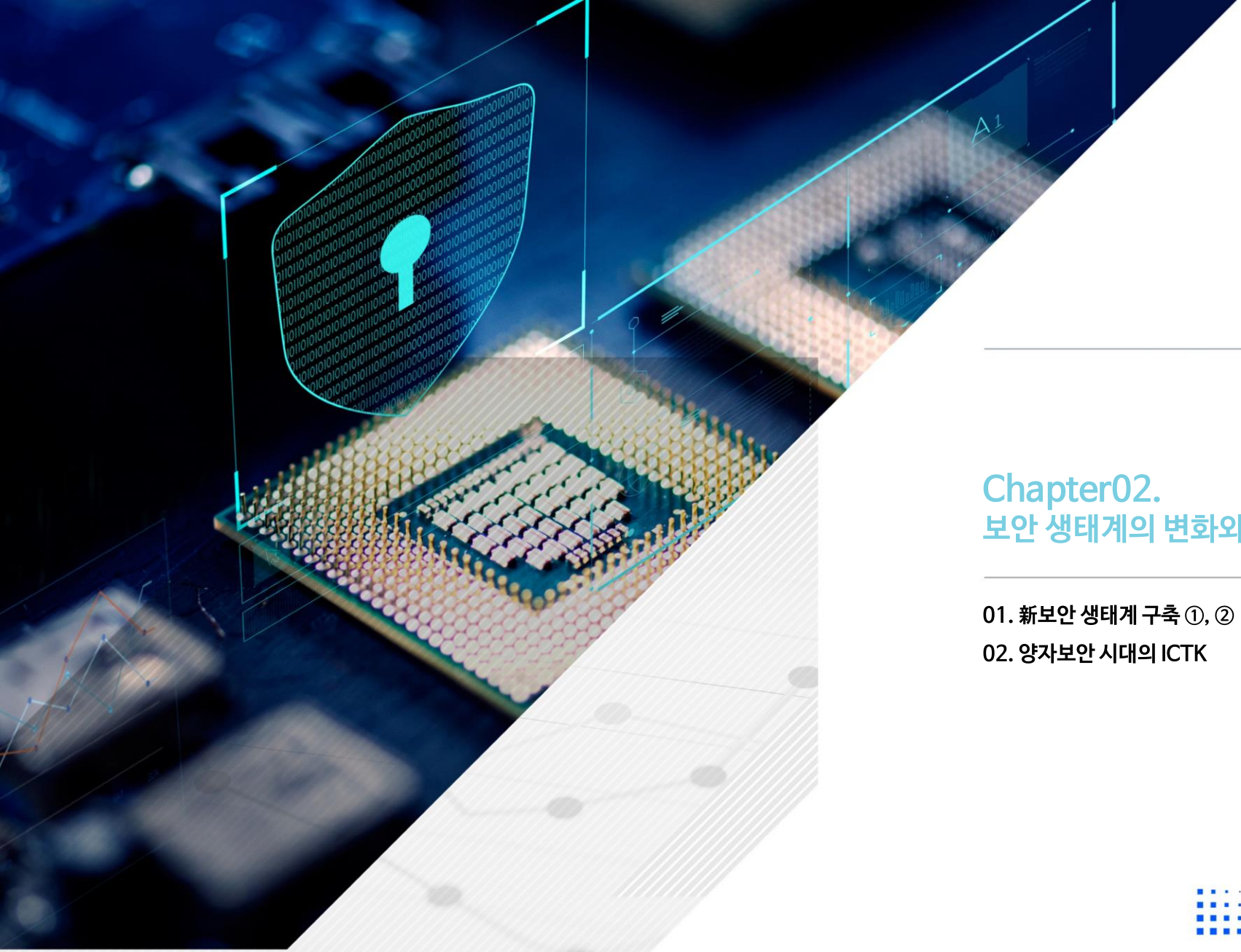
2.5D 패키징



HBM, AI 반도체의 발열문제 해결을 위해 엔비디아, TSMC, 삼성 등에서는 시스템 반도체와 메모리반도체를 하나의 패키지 안에 평행으로 배치하는 2.5D 패키징 기술 사용

AI 반도체, 데이터센터는 민감하고 해킹 시 위험성이 높으므로 변조할 수 없는 고유 식별자 필요

VIA PUF 기술을 기반으로 패키지 내에서 각 반도체 간의 보안 인증 및 추척에 활용



Chapter02.
보안 생태계의 변화와 ICTK

01. 新보안 생태계 구축 ①, ②

02. 양자보안 시대의 ICTK

ICTK
SAFE WITH US

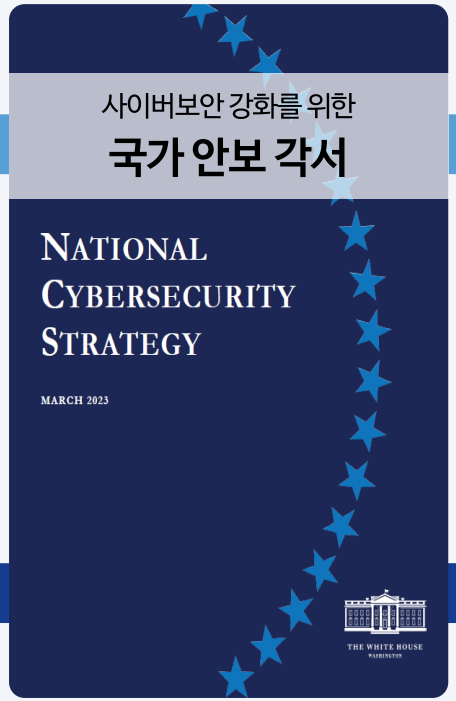
01 新보안 생태계 구축 _①Zero Trust와 Quantum

ICTK

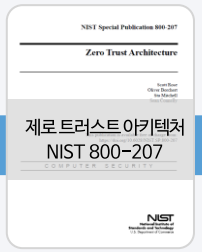
국내외 사이버보안 강화를 위한 다양한 정책 발표

Zero Trust
Architecture

Quantum
Resistant
(Protocol, Crypto)

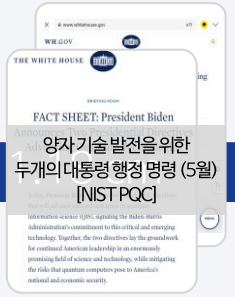


미국



제로 트러스트 아키텍처
NIST 800-207

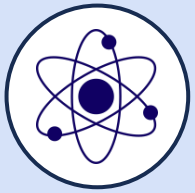
제로 트러스트 원칙을 기반으로
데이터 유출 사고를 방지하고,
내부 이동을 제한하도록 설계된
기업 사이버 **보안** 아키텍처



양자기술 발전을 위한
두개의대통령 행정 명령 (5월)
[NIST PQC]

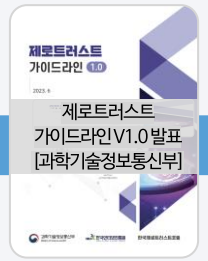
대응 기술

VIA PUF



Post-Quantum
Cryptography

국내



제로트러스트
가이드라인V1.0 발표
[과학기술정보통신부]

양자내성암호 전환 추진
로드맵발표(7월)
[국가정보원]

2024. 08
'양자 과학기술 플래그십 프로젝트 사업'
예비 타당성 조사 면제 추진

첫번째, "양자정보과학과 그 기술 응용분야에서
미국의 주도권이 계속되도록 조치"하기 위한 행정명령

두번째, "양자정보과학에서 미국의 경쟁 우위를 유지하는 한편
미국의 사이버, 경제, 국가 안보에 미치는 양자 컴퓨터의
위험을 완화하는 데 필요한 핵심 조치"를 기술한 국가안보공문

01 新보안 생태계 구축 _②RoT&PQC 표준화

ICTK

글로벌 빅테크 및 미국, 유럽 등 주요국가 新 보안 생태계 구축

Root of Trust 표준화 진행

GSA (Global Semiconductor Alliance)

IoT 보안과 표준화 선도

ICTK

전통적인 칩 제조사 외 스마트 팩토리, 금융, 클라우드 등의 서비스 기업 참여
SIEMENS, ARM 등과 Root of Trust 표준화 진행
다양한 서비스 플랫폼 구현을 위한 기술백서를 선도
(BOSCH, NXP 등 글로벌기업 공동 저자로 참여 예정)

AMD, SAMSUNG, SIEMENS, intel, ERICSSON, BOSCH, ARM, IBM, Alibaba.com, Alipay, Qualcomm, NVIDIA, Baidu 百度

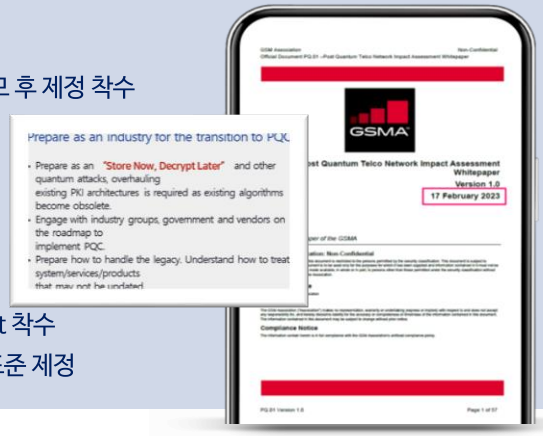
미국, 유럽 등 주요 국가의 PQC 표준화

미국 국립표준기술연구소 (NIST)에서 주도

- 2016년 現 주요 암호 알고리즘이 양자컴퓨터의 공격에서 안전하지 않다고 판단, 새로운 안전한 알고리즘을 공모 후 제정 착수
- **2024년 8월 , 세계 최초 PQC 표준 알고리즘 3종 제정**
  : ML-KEM, ML-DSA, SLH-DSA
- 추가 알고리즘 표준화 진행 중

유럽전기통신표준화기구 (ETSI)에서 주도

- 2004년 양자암호통신 테스트베드 구축을 위해 SECOQC(Secure Communication based on Quantum Cryptography) project 착수
- 다양한 OKD 프로토콜 구성을 바탕으로 양자암호키 생성 및 연동 실험을 추진, 이를 기반으로 ETSI ISG QKD 표준 제정

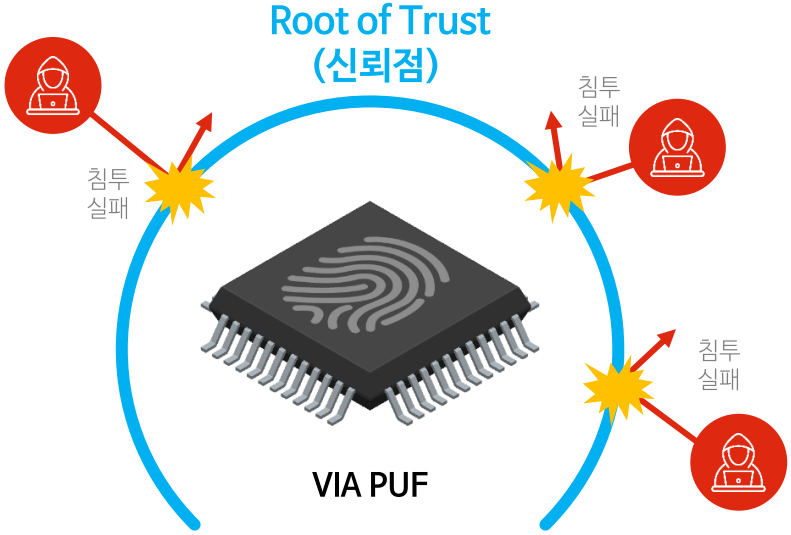


02 양자보안시대의 ICTK

양자보안시대를 선도하는 ICTK

복제 불가능한
H/W 신뢰점
(Root of Trust) 필요

PQC
(Post-Quantum
Cryptography) 필요



당사 PUF 기술로 해킹 원천 방지 가능

- LG 유플러스 PQC PUF 칩 및 응용서비스 공동개발 협약

➔ 기존 Module 형태에서 SoC 형태로 전환
➔ LG유플러스의 입장에서 최소 70% 원가 절감 가능

- 세계최초 양자보안칩 Giant 5 개발 (2022.07)

➔ Giant 5 기반 eSIM/USIM 출시

- 양자보안 VPN 서버 qTrustNet VPN 개발

➔ LG유플러스 지능형 CCTV 관제용으로 공급 중

- LG유플러스 양자 인증 솔루션 개발

- PQC 양자암호통신 구축 정부 사업 참여

➔ 2020~2023 양자암호통신 인프라 구축사업 진행
(LG유플러스, 하이브, 카카오 모빌리티, 전남도청 등이 참여)
➔ 2024 개방형 양자 테스트베드 구축·운영
(PQC TLS 서버 및 CA 서버 개발)
➔ 2024 양자내성알고리즘이 탑재된 PUF 기반의 PCIe HSM 국산화 개발

Chapter03.
본격적인 성과 발생

01. 전방시장 성장에 따른 수혜
02. VIA PUF 기술의 적용 및 사업분야
03. 검증된 글로벌 Track Record
04. 사업 확대 전략
05. 해외 시장 진출

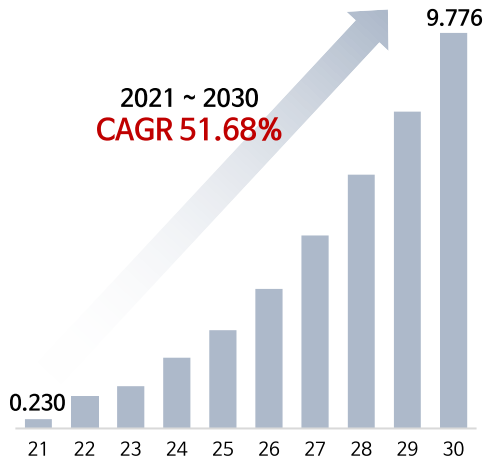
ICTK
SAFE WITH US

01 전방시장 성장에 따른 수혜

양자보안, IoT 시장의 성장은 Mega Trend로 보안칩 시장 필연적 성장

양자보안 시장 규모

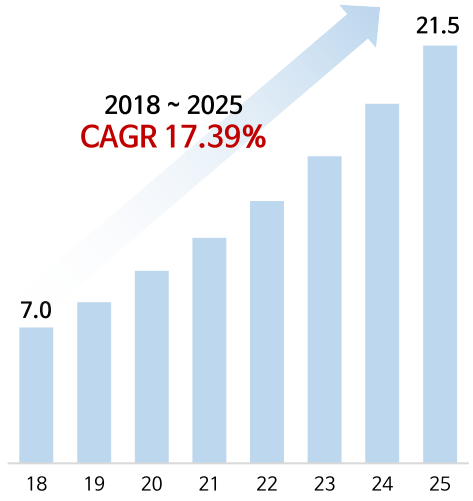
단위: 십억달러



출처: Statista

글로벌 IoT 디바이스 수

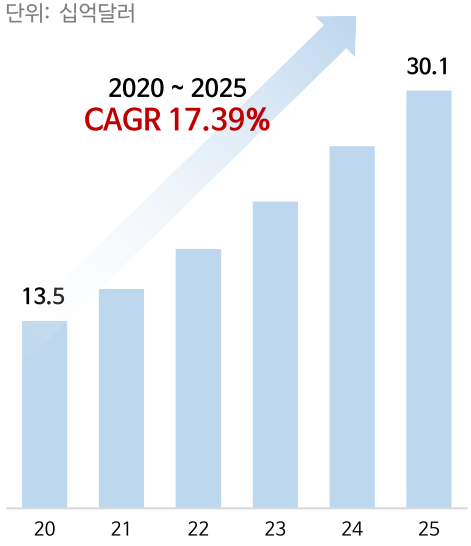
단위: 십억개



출처: IoT Analytics Research 2018

글로벌 IoT 보안 시장 규모

단위: 십억달러



출처: Statista

양자보안, IoT 시장 확대 가속화에 따른
보안칩 시장의 본격적 개화로 ICTK 직접적 수혜

02 VIA PUF 기술의 적용 및 사업분야

ICTK

VIA PUF 기술로 가장 안전한 네트워크 환경을 구축

IoT, Connected 기반 새로운 보안 **솔루션** 필요

(기기 식별, 원천적 신뢰성 확보)

Root of Trust / Inborn ID

금융·결제

- 복제불가능한 IC 카드
- 전자 신분증(eID)
- 금융기관용 암호키 보안모듈

정품인증

- IoT 디바이스 정품 인증
- 배터리 정품 인증
- 프린터 카트리지 정품 인증
- 카지노칩, 주류 정품 인증
- 산업용 로봇 인증

네트워크 해킹방지

- 무선공유기, 통신 모뎀 보안
- CCTV, 로봇청소기 보안
- 개인용 PC 보안
- PQC 인증 및 터널 서버 (qTrustNet VPN)

국방 및 공공 기관

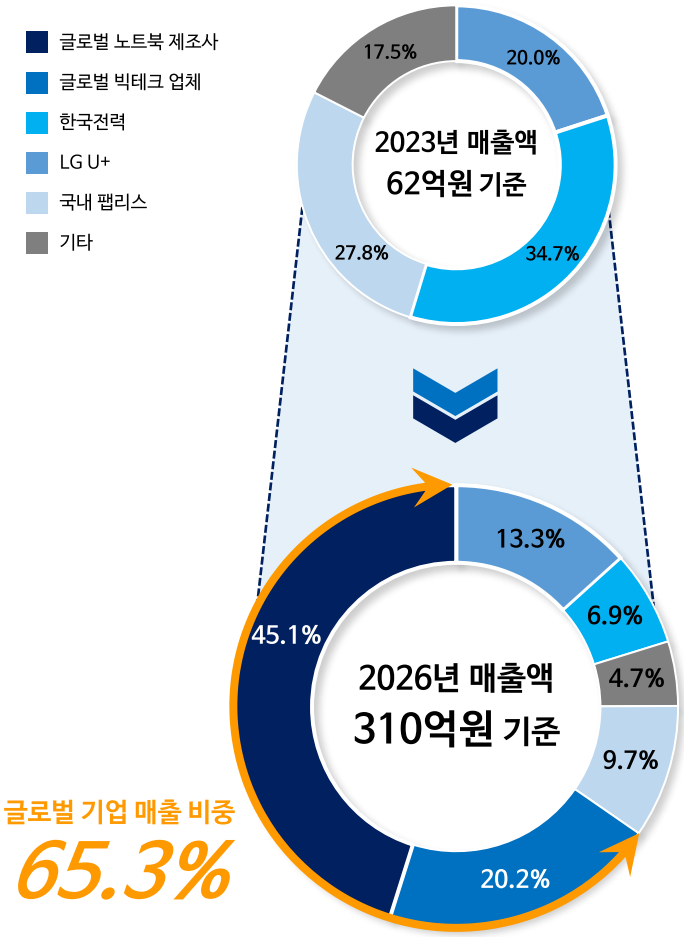
- 한국전력 AMI 사업 공급
- 조달청 업체 등록 진행
- 미국 및 한국 방위사업체와 사업 추진
- 드론 및 군사장비 탈취 무력화

03 검증된 글로벌 Track Record

ICTK

글로벌 빅테크 기업 중심으로 매출 포트폴리오 구축

고객사별 매출 비중 전망



글로벌 기업 매출 비중
65.3%

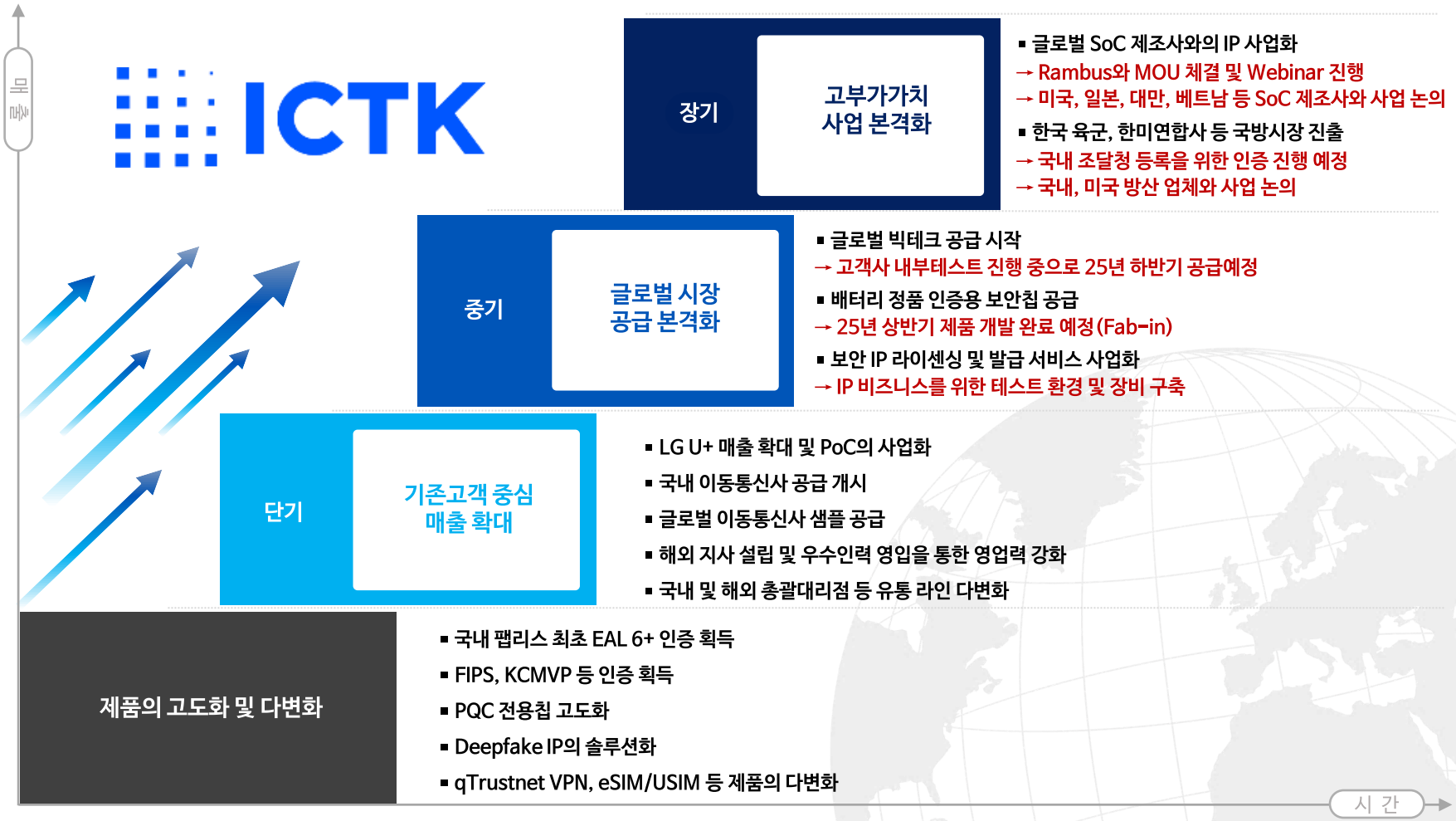
고객사별 레퍼런스

IP		보안칩	
Rambus	MOU 체결 & 공동영업	LG U+	AP, CCTV 보안칩 M2M용 eSIM
국내 팹리스	SoC 설계 계약	I&C TECHNOLOGY	한전 AMI PLC 모뎀
HYUNDAI	신소자 PUF IP 개발	글로벌 빅테크 업체	IoT Device Acc. 정품인증
eyenix	28nm 공정 VIA PUF 기술 이전	글로벌 노트북 제조사	PC 보안용 보안칩

모듈/디바이스		솔루션/플랫폼	
LG U+	qTrustNet VPN 공급	LG U+	인증플랫폼, MPC, KMS 개발
Doosan Robotics	로봇 인증 모듈	한국전력공사	네트워크 보안, 신재생에너지 보안
HDC	스마트도어락		

04 사업 확대 전략

다양한 제품/솔루션 개발 및 공급 개시로 본격적 매출 발생



05 해외 시장 진출

미국, 일본, 중국, 아시아 등 글로벌 파트너십 확대

대만 및 아시아

- 아시아 지역 팹리스 기업 IP 공급
- 현지 네트워크 장비 제조사 등과 협업
- 현지 Agent 업체 통한 고객사 발굴

미국

- PC 보안 분야 점유율 확대
- 국방, 항공으로 시장 확대
- 반도체 제조사향 IP 영업 진행

글로벌 빅테크 업체 | 글로벌 노트북 제조사

유럽

- 글로벌 통신사 신기술(PQC) 도입에 대한 협력 관계 구축
- 현지 제조사 대상 영업활동

일본

- 현지 유통업체 통해 마케팅
- 미국 레퍼런스 기반 영업 확대
- 다양한 분야 고객사 Target

중국

- 현지 유통업체 통해 마케팅 확대
- 스마트카드, 스마트도어락, 전기오토바이 제조사 등에 칩 공급 진행 또는 논의중
- 적극적 고객사 발굴 지속

Appendix

01. 회사 개요
02. 성장 연혁
03. 제품 라인업
04. 요약 재무제표

ICTK
SAFE WITH US

01 회사 개요

Company Profile

회사명	아이씨티케이 주식회사
대표이사	이정원
설립일	2017년 10월 18일
자본금	66.1억(2024. 09. 30 기준)
임직원	62명(2024. 09. 30 기준)
사업분야	보안 IP/칩/모듈 연구 개발 및 제조, 보안플랫폼 개발 및 공급
본사위치	서울특별시 강남구 강남대로84길 16, 14층
홈페이지	http://ictk.com/

CEO Profile

대표이사 이정원

- 하버드대학교사회학과 학사
- 하버드대학원정치학수료
- 호서대학교겸임교수
- 호서벤처투자투자전략
- B Square Lab (싱가포르)

주요 임직원 현황

성명	직책	담당업무	주요 경력
이경택	전무	CSO	• 서울대학교 전자공학 학사 • 텍사스오스틴 대학교 전기공학 박사 • Intel (Altera) • IBM
강봉호	전무	CTO	• 부산대학교 전자계산학 석사 • SK텔레콤 • Cisco Systems • Estorm
박윤배	이사	CFO	• 아주대학교 경영학 학사 • 삼정회계법인 • 프레스티지바이오로직스 • 한국머크

02 성장 연혁

독보적인 VIA PUF 기술력을 기반으로 성장 지속

태동기(2007 ~ 2017)

- 2017
  - 세계 최초로 PUF 칩 양산 성공(G1) 및 영업 개시
  - PUF 보안 개발 사업 집중을 위해 ICTK PUF사업부 분사
- 2016
  - 유럽 Security Week Conference 혁신상 수상
- 2015
  - VIA PUF 상용칩 (Draco) 개발 성공
- 2014
  - 한양대와 보안 SoC R&D 센터 설립
- 2009
  - VIA PUF에 대한 연구를 시작
- 2007
  - Invert PUF, Diff Amp PUF 등 PUF에 대해서 연구시작
- 2001
  - 스마트카드 인증기관으로 ICTK 최초 설립

성장기 & 확장기 (2018~현재)

- 2024
  - 코스닥 상장
  - EAL 6+ Site Audit 수검(11월 인증서 발급 예정)
  - 미국 현지법인 설립
- 2023
  - 미국 산호세 소재 Rambus와 MoU 체결 및 공동 IP 제안 진행
  - 국내 팹리스와 EAL 6+ 보안칩 설계 용역 계약 체결
  - 미국 산호세 소재 Rambus와 MoU 체결 및 공동 IP 제안 진행
- 2022
  - 글로벌 빅테크 업체 및 글로벌 노트북 제조사 보안칩 공급을 위한 테스트 진행
  - 글로벌 빅테크 업체 Acc. 정품 인증용 보안칩 공급 계약 체결
  - G3 - KCMVP 인증 획득
  - 세계 최초 PUF-VPN 개발 및 LG U+ 납품
- 2021
  - 세계 최초 PUF 기반 USIM 개발 완료
  - 한국기업 최초 eSIM 제조업체등록 및 세계최초 PUF-eSIM 개발
  - PQC 양자내성 보안 기술 개발 및 상용화
- 2020
  - PUF 보안기술의 ISO (국제기술표준기구) 정식 등재 ISO 20897-1
- 2019
  - GSA (Global Semiconductor Alliance) IoT Security Working Group 내 Root of Trust 요구 조건 구축 담당업체로 선정
- 2018
  - 주력제품 G3 (Giant-3) 보안칩 양산
  - LG U+ PUF기반 보안플랫폼 구축 및 납품

03 제품 라인업

IP를 통한 칩, 모듈/디바이스, 솔루션/프로젝트까지 One-Stop 솔루션 제공

보안솔루션/프로젝트

- ISF_FOTA (Firmware Over the Air)
- ISF_KMS (Key Management System)
- ISF_AUTH (FIDO, HMAC Authentication)
- PQC (Post Quantum Cryptography)

보안모듈/디바이스


USIM/eSIM


qTrust PCI


qTrust Net


LTE/5G Module


qTrust USB

보안칩(SoC)


Giant1


Giant3


Giant5


MTR

자체 IP

VIA PUF IP	RoT(신뢰점) IP	Cyrptographic Algorithm(암호 알고리즘) IP	TRNG(진난수생성기) IP
PUF 기술의 난제인 보정값 문제를 수동소자를 사용하여 해결한 독보적 기술	암호화 키를 이용하여 데이터를 암호화하고 디지털서명 생성 및 서명 확인과 같은 기능 수행	다양한 사용성을 가진 암호 알고리즘 IP를 다수 보유중	대칭키 방식 등에서 사용되는 키는 진난수가 필요하며 TRNG는 난수를생성시키는중요한보안IP

요약 재무상태표

(단위: 백만원)

구분	2024.3Q	2023	2022
유동자산	37,052	7,978	7,968
비유동자산	9,377	2,435	1,873
자산총계	46,429	10,413	9,841
유동부채	1,337	791	40,720
비유동부채	1,732	214	250
부채총계	3,068	1,005	40,969
자본금	6,611	5,552	3,042
자본잉여금	86,309	48,616	2,374
이익잉여금	(37,618)	(32,351)	(23,321)
기타포괄 손익누계액	19	19	94
기타자본항목	(12,030)	(12,428)	(13,318)
자본총계	43,360	9,408	(31,128)

요약 포괄손익계산서

(단위: 백만원)

구분	2024.3Q	2023	2022
매출액	4,290	6,187	2,567
매출원가	2,289	2,824	1,541
매출총이익	2,001	3,363	1,026
판매비와관리비	7,930	5,728	4,360
영업이익	(5,928)	(2,365)	(3,335)
영업외수익	867	289	242
영업외비용	205	6,955	7,679
법인세비용 차감전순이익	(5,266)	(9,091)	(10,772)
법인세비용	-	-	-
당기순이익	(5,266)	(9,091)	(10,772)

서울특별시 강남구 강남대로84길 16, 14층 | **Tel. 02-569-0010**
http://ictk.com/