When and What to Reveal:
A Privacy Primitive for Regulated Blockchains

결정론적 동형암호와 Threshold MPC를 활용한
규제 대응 가능한 온체인 프라이버시

이승환 (Seunghwan Lee)
대표, waLLLnut (월넛 주식회사)

한국통신학회 동계종합학술발표회
스타트업 특별세션

2026년 2월 5일 (목) 11:10–11:45 모나 콘도 1층 크리스탈에서 진행

발표자 소개

이승환 / 대표

소속: waLLLnut (월넛 주식회사)

약력:

2025 주식회사 waLLLnut 설립

Co-founder: Dohyuk Kim & Dong-Joon Shin

2025 한양대 융합전자공학과 박사 졸업

2025 **Crypto 2025** 논문 수록 (Top-tier)

"Actively Secure MPC in Dishonest Majority"

2025 Solana Hackathon 3등

2025 BK21 ENRICH IT AWARD

공동 연구: CCRL (한양대)

- **신동준** 교수 – Co-founder, 한양대 전자공학부
- **김도혁** – Co-founder, 한양대
- 격자 기반 암호, FHE, MPC 분야 연구

현재 사업 진행

- **Mantle** 네트워크 연동 진행 중
- **Solana** 생태계 협업 중
- **PSE** (Privacy & Scaling Explorations) 접촉 중

목차

블록체인 위 프라이버시: 현재 기술

ZKP + Mixing Pool 기반 기밀 전송

Zcash (Sasson et al., S&P 2014); Tornado Cash

- 전송 사실의 유효성을 증명
- 트랜잭션 금액 · 수신자 은닉 가능
- 그러나: 암호화된 데이터에 대한 **연산**은 불가

▶ Tornado Cash: 2022년 OFAC 제재, 개발자 기소

▶ 규제 대응 불가 ⇒ 프라이버시 = 불법 취급

FHE 기반 기밀 연산 (fhEVM)

Zama fhEVM (`github.com/zama-ai/fhevm`)

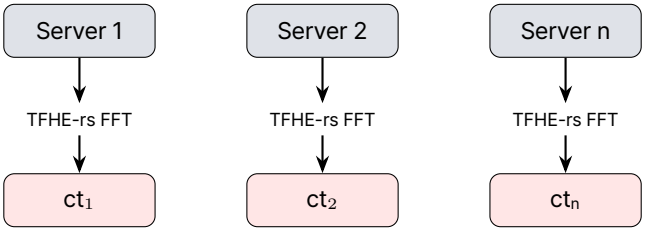
- 복호화 없이 암호문 상에서 연산 가능
- Zama의 fhEVM: Solidity 호환 동형 연산
- 그러나: FFT 기반 TFHE-rs의 비결정성 문제

핵심 문제

1. **조건부 공개 불가** – 규제 · 감사 기관에 특정 집계만 선택적으로 공개하는 메커니즘 부재
2. **암호문 합의 불가** – FFT의 부동소수점 오류로 머신마다 다른 암호문 생성 ⇒ 합의 불가
3. **연산과 프라이버시의 상충** – ZKP는 연산 불가, FHE는 합의 불가

FFT 비결정성이 블록체인에 미치는 영향

TFHE-rs: Zama (`github.com/zama-ai/tfhe-rs`); 부동소수점 비결정성: IEEE 754-2019



$ct_1 \neq ct_2 \neq ct_n$

Consensus 실패!

원인: 부동소수점 FFT는 결합법칙을 만족하지 않음

$$(a \oplus b) \oplus c \neq a \oplus (b \oplus c)$$

결과:

- 동일 입력 · 동일 키에도 머신 · 컴파일러 · ISA마다 다른 암호문
- Threshold FHE에서 복호화 불가
- 블록체인 합의와 근본적 비호환

기존 대응: LSB 트리밍 $\Rightarrow$ 추가 오류, 성능 저하

우리의 질문

"프라이버시를 유지하면서,

언제 공개할지, **무엇을** 공개할지를

온체인에서 제어할 수 있는가?"

그리고 이것이 모든 머신에서

결정론적으로 동일하게 동작할 수 있는가?

다자간 연산(MPC)의 두 가지 방식

MPC (Secure Multi-Party Computation): n명의 참여자가 각자의 비밀 입력 x_i를 공개하지 않고 공동 함수 $f(x_1, \ldots, x_n)$을 계산하는 암호 프로토콜

1. Garbled Circuits (GC)

Yao, FOCS 1986

- 회로를 "난독화"하여 전송, 상대방이 평가
- 통신량: $O(|\text{회로}|)$ — 회로 크기에 비례
- 라운드: 상수 (2–3회)
- 문제: 회로 재사용 불가, 2자 전용

2. Secret Sharing (SS)

SPDZ: Damgård et al., Crypto 2012

- 데이터를 조각으로 나눠 분산 연산
- 통신량: $O(1)$ per gate
- 라운드: $O(\text{곱셈 수})$ — **핵심 문제!**
- 문제: 매 곱셈마다 통신 필요

공통된 근본 문제

두 방식 모두 **참여자 간 통신이 필수**. 블록체인처럼 전 세계에 분산된 시스템에서는 통신 지연이 성능을 지배.

왜 SS-MPC는 블록체인에서 실패하는가

참고: Damgård et al., "Multiparty Computation from Somewhat Homomorphic Encryption," Crypto 2012

SPDZ 등 Secret Sharing 기반 MPC에서:

곱셈당 필요한 통신 라운드

2–3회 (Beaver triple 소비 + 재구성)

단순 스마트 컨트랙트

∼**100 곱셈** (잔액 확인, 서명 검증, 상태 업데이트)

글로벌 참여 시 계산

$$180\text{ms} \times 3 \times 100 = \textbf{54초}$$

단일 트랜잭션 처리: 54초

- 패킷 손실, 네트워크 혼잡이 **전혀 없는** 이상적 조건
- 사용자: 54초 대기 불가
- 검증자: 합의 타임아웃
- 블록체인: 처리량 붕괴

결론: SS-MPC는 글로벌 블록체인에서 **근본적으로 비실용적**

통신 지연의 물리적 한계

100ms+

서울 ↔ 미국 간 최소 통신 지연

광섬유에서 빛은 진공의 약 67% 속도로 이동합니다.

11,000km를 왕복하는 데 **물리적 최소 110ms**가 필요합니다.

이것은 기술 발전으로 줄일 수 없는 **물리 법칙의 한계**입니다.

출처: ITU-T G.652 광섬유 표준; 태평양 해저 케이블 경로 기준

광통신의 물리적 한계

광섬유 내 빛의 속도

- 진공: $c = 300{,}000$ km/s
- 광섬유 (굴절률 $\sim$1.5): $\sim$200,000 km/s

서울 $\leftrightarrow$ 버지니아 거리

$\sim$11,000 km (태평양 해저 케이블 경로)

이론적 최소 RTT

$$\text{RTT} = \frac{2 \times 11{,}000\text{km}}{200{,}000\text{km/s}} \approx \textbf{110ms}$$

실제 측정값 (Cloudflare Speed Test, 2024)

경로	RTT
서울 $\leftrightarrow$ 버지니아	$\sim$180ms
서울 $\leftrightarrow$ 프랑크푸르트	$\sim$250ms
서울 $\leftrightarrow$ 도쿄	$\sim$30ms

핵심 통찰

라우터 지연, 패킷 처리 등으로 실제 RTT는 이론값의 1.5$\sim$2배. 이것은 **기술 발전으로 개선 불가**한 물리적 한계.

참고: ITU-T G.652 광섬유 표준, 해저케이블 경로 TeleGeography Submarine Cable Map

MPC vs FHE: 통신 복잡도 비교

항목	SS-MPC	Garbled Circuits	FHE
연산 중 통신	매 곱셈마다 필요	초기 전송 필요	**불필요**
라운드 복잡도	O(곱셈 깊이)	$O(1)$	**$O(1)$**
통신량	$O(n)$ per gate	$O(\|회로\|)$	**입출력만**
다자간 확장	통신량 증가	복잡도 급증	**영향 없음**
글로벌 블록체인	비실용적	비실용적	**가능**

결론

FHE는 **통신 라운드** $O(1)$와 **연산 게이트당 비용** $O(1)$을 동시에 달성하는 유일한 암호 연산 방식. 각 검증자가 **독립적으로, 통신 없이** 동일한 연산을 수행하고 동일한 결과에 도달.

결정적 연산: 합의의 핵심

TFHE-rs (FFT 기반)

부동소수점 반올림이 달라짐:

- CPU 아키텍처 (x86 vs ARM)
- 컴파일러 버전 및 최적화

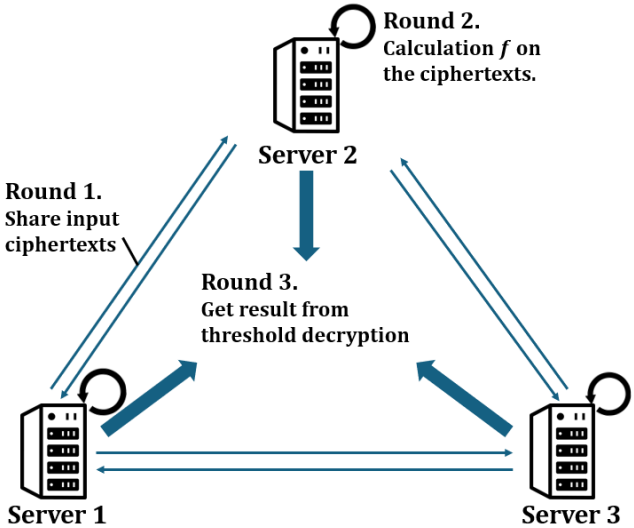
⇒ **합의 실패**

FHE16 (정수 기반)

모든 연산이 정수 모듈러 산술:

- 같은 입력 → 같은 출력
- 플랫폼, 컴파일러 무관

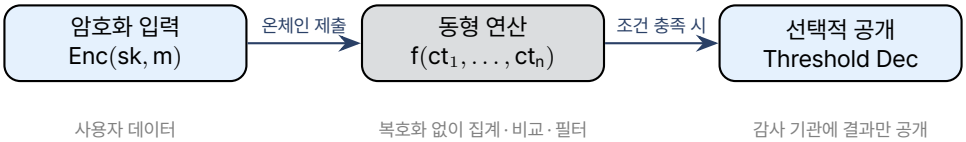
⇒ **합의 성공**



LatticA 개요

핵심 아이디어

동형암호(FHE)로 데이터를 암호화한 채 연산하고, Threshold MPC로 **조건부 복호화**를 수행하여 **"언제, 무엇을"** 공개할지를 프로토콜 수준에서 제어한다.



결정론적 연산

16비트 정수 연산만 사용
모든 노드에서 bit-exact 동일 결과

Threshold 복호화

다수 참여자 합의 필요
단일 주체 데이터 탈취 방지

규제 대응

감사 요청 시 특정 집계만 공개
조건부 공개 프로토콜

활용 시나리오

시나리오 1: 기밀 DeFi 거래

1. 사용자가 거래 금액을 FHE 암호화하여 온체인 제출
2. 스마트 컨트랙트가 암호문 상에서 잔액 검증 및 이체 수행
3. 거래 상대방만 결과를 복호화
4. **감사 요청 시**: Threshold 복호화로 특정 기간 총 거래량만 공개

시나리오 2: 규제 대응 투표/거버넌스

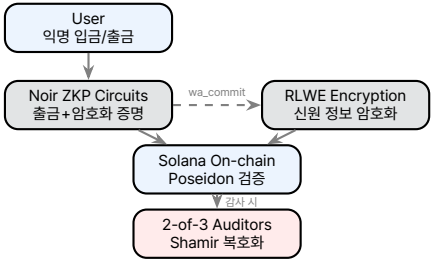
1. 투표 내용을 FHE 암호화하여 제출
2. 동형 연산으로 암호화 상태에서 집계
3. 투표 종료 후 Threshold 복호화로 결과만 공개
4. 개별 투표 내용은 영구 비공개

공통 요구사항

모든 노드가 **동일한 암호문**을 생성해야 합의 가능 $\Rightarrow$ **결정론적 FHE**가 필수

Auditable Dark Pool: 실제 구현 데모

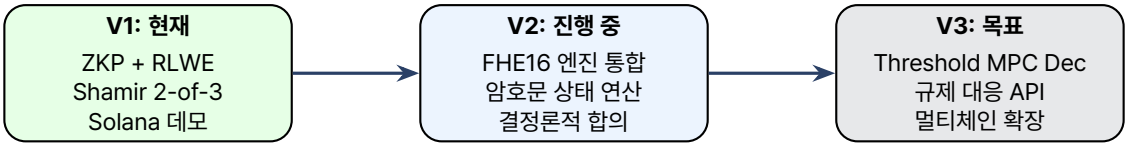
https://github.com/Ham3798/auditable-dark-pool



핵심 설계:

- **Noir 회로** 2개: 출금+암호화
  (Aztec Noir)
- **wa_commitment**: Poseidon 연결
  (Grassi et al., USENIX 2021)
- **RLWE**: 격자 기반 신원 보호
  (Lyubashevsky et al., Eurocrypt 2010)
- **2-of-3 Threshold**: Shamir
  (Shamir, CACM 1979)
- 제약 조건 **42**× 축소

Auditable Dark Pool → FHE16 통합 로드맵



V1 성과

- Solana 위 동작 확인
- Noir + RLWE 연동
- Solana **Startup-Village에서 3등** 수상

V2 목표

- FHE16로 RLWE 교체
- 암호문 상태에서 잔액 연산
- Mantle / Solana 연동

V3 비전

- Crypto 2025 MPC 적용
- 분산 키 생성
- PSE 생태계 통합

CCRL 합동 연구에 따른 학술적 성과

한양대학교 암호학 연구실 (CCRL)
신동준 교수 · 이승환 · 김도혁

FHE16 · Primitive Gate · Actively Secure MPC

FHE16: 설계 철학

Lee, Kim, Shin. “Fast and Compact Bootstrapping Using 16-bit Integer Arithmetic,” ePrint 2024/1916.

핵심 원칙

부트스트래핑의 **모든 연산**을 16비트 정수 곱셈과 덧셈으로 수행한다.

기존 접근법의 문제:

- OpenFHE: NTT 기반 $\Rightarrow$ 결정론적이나 **느림**
- TFHE-rs: FFT 기반 $\Rightarrow$ 빠르지만 **비결정론적**
- NTRU: 빠르고 컴팩트하나, fatigue point로 인해 파라미터 확장에 불리

FHE16의 접근:

- 모듈러스 $q = q_1 \cdots q_n$ (16비트 소수의 곱)
- Incomplete NTT (NTT_w)로 다항식 곱셈
- 부동소수점 **완전 배제**
- Signed Montgomery Reduction (SM)
- Intel vpmulhw 명령어로 단일 명령 구현

FHE16: 5가지 핵심 연산

- NTT_w, $INTT_w$: $X^d + 1$이 $\mathbb{Z}_{q_i}$에서 완전 분해되지 않을 때, 차수 w까지만 분해
- MUL_w: NTT 공간에서 Karatsuba 곱셈
- **External Product** $\boxdot$:
  $\text{Decom} \to NTT_w \to MUL_w \to INTT_w$

- AUT_w: NTT_w 공간에서 직접 automorphism – AP^+ blind rotation에 필수
- Decom: RNS에서 부동소수점 없이 gadget 분해 – 정확성 수학적 증명 (Theorem)
- 모든 연산이 16비트 SM으로 구현

Composite Modulus와 RNS 구조

모듈러스 구성:

$$q_2 = p_{14} \times p_{25} = 10753 \times 12289$$

- 각 p_i는 $p = \theta \cdot 2^m + 1$ 형태의 NTT-friendly 소수
- $4p_i < 2^{16}$ 보장 $\Rightarrow$ 4회 덧셈까지 오버플로우 없음
- $d = 512$에서 $NTT_w(w = 1)$ 완전 분해 가능

RNS 병렬 처리:

$$\mathbb{Z}_q[X]/\langle X^d + 1\rangle \cong \bigoplus_{i=1}^{n} \mathbb{Z}_{q_i}[X]/\langle X^d + 1\rangle$$

각 $\mathbb{Z}_{q_i}$ 연산은 **완전히 독립** $\Rightarrow$ GPU/멀티코어 병렬화에 유리

idx	p	m	bits
p_1	257	8	9
p_3	3329	8	12
p_{13}	7681	9	13
p_{14}	**10753**	**9**	**14**
p_{20}	13313	10	14
p_{24}	18433	11	15
p_{25}	**12289**	**12**	**14**

25개의 NTT-friendly 16비트 소수 후보

파라미터 최적화 전략

	sk_1	k_1	q_1	sk_2	d	k_2	B_2^A	B_2^B	l_2^A / l_2^B	λ
OpenFHE GINX	T	503	2^{14}	T	1024	1	2^9	2^9	2 / 2	121
TFHE-rs GINX	B	811	2^{32}	B	512	3	2^{10}	2^{10}	2 / 2	132
FHE16 GINX	B	585	2^{14}	Q	512	2	2^9	2^{10}	2 / 1	128
FHE16 AP$^+$	2.19	472	2^{14}	1.15	512	2	2^9	2^{10}	2 / 1	128

FHE16의 파라미터 전략:

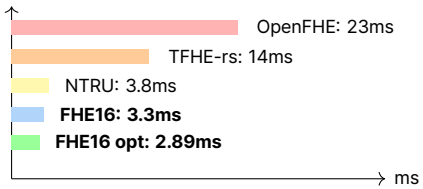
- sk_1 과 sk_2 에 **서로 다른 support** 사용 $\Rightarrow$ 보안 유지 + 속도 최적화
- $l_2^A > l_2^B$: b 파트의 external product 횟수 감소 $\Rightarrow$ 키 크기 및 속도 동시 개선
- 두 종류의 gadget parameter로 정밀한 오류 제어:

$$\sigma_{\boxdot}^2 = \frac{k_2 d}{12}\left(l_2^A (B_2^A)^2 \sigma_{bl}^2 + D_2^A \sigma_{sk}^2\right) + \frac{d}{12}\left(l_2^B (B_2^B)^2 \sigma_{bl}^2 + D_2^B\right)$$

성능 비교: 부트스트래핑 시간

출처: Lee et al., ePrint 2024/1916 Table 4; OpenFHE v1.1.2; TFHE-rs v0.5; NTRU FHE (Kluczniak, Asiacrypt 2022)

라이브러리	AVX2	AVX512
OpenFHE GINX	35 ms	23 ms
OpenFHE AP^{+}	34 ms	20 ms
TFHE-rs GINX	16.6 ms	14 ms
NTRU FHE	5.5 ms	3.8 ms
FHE16 GINX	**4.9 ms**	**3.3 ms**
FHE16 최적화	**3.5 ms**	**2.89 ms**



AVX512 기준, 단일 스레드

$d = 512$, $\lambda \geq 128$, $p_{fail} < 2^{-32}$

속도 비교 요약

OpenFHE 대비 **6.2**× | TFHE-rs 대비 **4.0**× | NTRU 대비 **1.1**×

성능 비교: 키 크기 및 결정론성

출처: Lee et al., ePrint 2024/1916 Table 5; OpenFHE (Al Badawi et al., 2022); TFHE-rs v0.5

	OpenFHE	TFHE-rs	NTRU	**FHE16**
BL 키 (GINX)	26.4 MiB	55 MiB	—	**14.4 MiB**
BL 키 (AP^{+})	12.3 MiB	—	—	**11.8 MiB**
결정론적?	✓	×	✓	✓

키 크기 절감 요인:

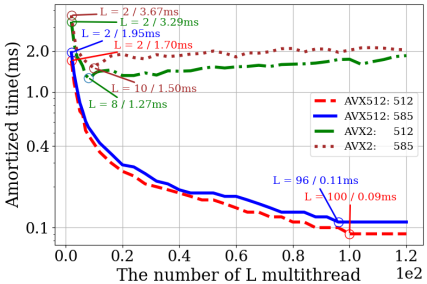
- TFHE-rs: $q_2 = 2^{32}$ 고정 $\Rightarrow$ $k_2 = 3$ 필요 $\Rightarrow$ 키 크기 증가
- FHE16: composite modulus $q_2 \approx 2^{28} \Rightarrow k_2 = 2$로 충분
- $l_2^{B} = 1$로 MGSW 암호문 열 수 최소화

블록체인 환경에서의 의미

부트스트래핑 키는 **모든 노드**가 보유해야 함. TFHE-rs 대비 **3.8× 키 크기 절감**은 네트워크 대역폭 · 저장 비용에 직접 영향.

멀티스레드 성능

출처: Lee et al., ePrint 2024/1916 Figure 6; Intel Xeon Gold 6248R (48코어)



멀티스레드 성능

- 48코어 서버, $L = 96$ 스레드
- Amortized: **0.09 ms/bootstrap**
- 단일 스레드(3.5ms) 대비 **38**×
- RNS 독립 처리 $\Rightarrow$ 확장성 우수

하드웨어 가속 가능성

16비트 MAC 연산만 사용 $\Rightarrow$ FPGA DSP 슬라이스 1개로 구현 가능. 각 $\mathbb{Z}_{q_i}$ 연산이 완전히 독립 $\Rightarrow$ GPU 병렬화 최적.

기존 TFHE 게이트의 한계

Kim, Kim, **Lee**, Shin. “Low-Latency FHE Arithmetic Using Parallel Prefix Group Circuit with Primitive Gate Bootstrapping,” ePrint 2025/2150.

기존 TFHE: 2-input Boolean 게이트

- 한 번의 부트스트래핑 = 2입력 게이트 1개 (AND, OR, NAND, XOR)
- 복잡한 산술 $\Rightarrow$ 깊은 Boolean 회로
- 32비트 가산기 = 수십 번 부트스트래핑

Latency 병목

- 게이트 깊이가 산술 연산의 병목
- 동형 정수 연산 latency = (게이트 깊이) $\times$ (부트스트래핑 시간)

“한 번의 부트스트래핑으로 더 강력한 게이트를 평가할 수 없는가?”

Primitive Gate Family (PGF)

핵심 아이디어

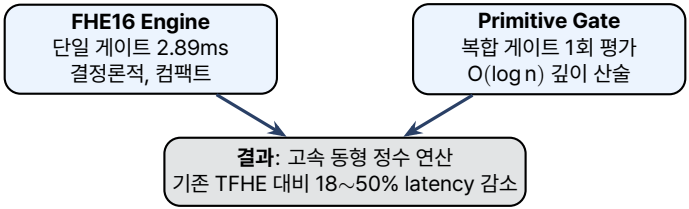
Blind rotation에서 평가 가능한 함수를 대수적으로 형식화하여 (**Blind-Rotational Function Family**), 단일 부트스트래핑으로 평가 가능한 **Primitive Gate Family (PGF)** 정의.

게이트	기존 TFHE	PGF (1회 부트스트래핑)
2-input AND, OR, XOR	✓	✓
ℓ-input XOR	$\ell - 1$회	✓ 1회
3-input Majority	4회	✓ 1회
AND-XOR (hybrid)	2회	✓ 1회

Parallel Prefix 구조와 결합:

- PGF 게이트를 Parallel prefix adder 노드에 배치 $\Rightarrow O(\log n)$ 깊이
- 2-input adder: 기존 TFHE 대비 **18∼50% latency 감소**
- $d = 512$ 단위 게이트 조합으로 임의 정밀도 동형 정수 산술 체계적 구성 가능

Primitive Gate + FHE16 시너지



블록체인 적용 의미

동형 정수 산술의 latency가 줄어들면, 온체인에서 복잡한 금융 로직(잔액 비교, 한도 검증, 집계 등)을 암호화 상태로 실행하는 것이 실용적 범위에 진입.

Actively Secure MPC for Threshold FHE

Lee, Noh, Kim, Kim, Shin. "Actively Secure MPC in the Dishonest Majority Setting," **Crypto 2025**. ePrint 2025/810

왜 MPC가 필요한가?

- 블록체인 FHE: **분산 키 생성** + **Threshold 복호화** 필수
- 단일 주체 비밀키 보유 $\Rightarrow$ 프라이버시 불가
- n명 공동 키 생성, t명 합의 시 복호화

핵심 아이디어

- **Eval/Public Key**: 기존 MPC로 분산 생성
- **One-bit Random Sampler**: 단일 사용자 파라미터 유지
- Dishonest Majority + **Active Security**

	통신	연산	라운드	입력
SPDZ	$O(n)$	$O(1)$	$O(d)$	$O(1)$
BMR	$O(n^2)$	$O(n)$	$O(1)$	$O(n)$
FHE (기존)	$O(1)$	$O(1)$	$O(1)$	$O(1)$
Ours	$O(1)$	$O(1)$	$O(1)$	$O(1)$

기존 MPC의 한계

SPDZ: 상수 라운드 미달성
BMR: $O(n^2)$ 통신

FHE 기반: 능동 보안 미달성

$\Rightarrow$ **Threshold FHE 키 생성**에 직접 활용

Actively Secure MPC: 벤치마크

Lee et al., "Actively Secure MPC in the Dishonest Majority Setting," Crypto 2025. ePrint 2025/810

프로토콜	온라인 통신	게이트당 연산	라운드 복잡도	능동 보안
SPDZ (Crypto'12)	$O(n)$	$O(1)$	$O(\text{depth})$	✓
BMR (STOC'90)	$O(n^2)$	$O(n)$	$O(1)$	✓
SSFHE (TCC'12)	$O(1)$	$O(1)$	$O(1)$	×
Ours (Crypto'25)	$\mathbf{O(1)}$	$\mathbf{O(1)}$	$\mathbf{O(1)}$	✓

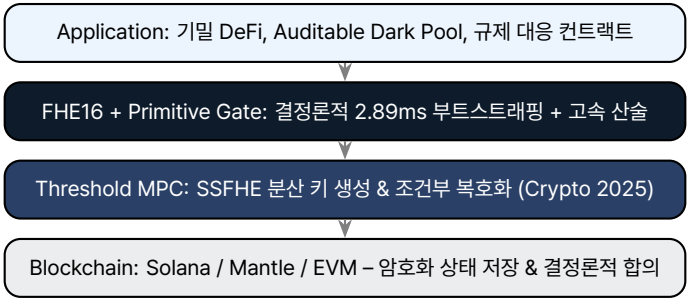
핵심 기여

- Dishonest majority에서 **능동 보안** 달성
- 통신/연산/라운드 **모두 상수 복잡도**
- Composite modulus에서 one-bit sampler

블록체인 적용

- Threshold FHE 키 분산 생성
- 악의적 참여자 대응 가능
- 글로벌 검증자 네트워크에서 실용적

FHE16 + Threshold MPC = 블록체인 프라이버시 스택



기술 특성

- **결정론적**: bit-exact ⇒ 합의 호환
- **고속**: 2.89ms (단일), 0.11ms (멀티)
- **컴팩트**: BL 키 14.4 MiB
- **안전**: 128비트, Dishonest majority

사업 특성

- **Mantle** 연동 진행 중
- **Solana** 생태계 협업 (Dark Pool)
- **PSE** 접촉 중
- 멀티체인 확장 로드맵

waLLLnut (월넛 주식회사)

팀 & 연구 성과

- **이승환** – 대표 / 한양대 박사
- **김도혁** – Co-founder / 한양대
- **신동준** – Co-founder / 한양대 교수

논문 파이프라인:

1. **FHE16** – ePrint 2024/1916, IEEE Access
2. **Primitive Gate** – ePrint 2025/2150
3. **Actively Secure MPC – Crypto 2025**
4. Threshold FHE Key Gen – 연구 진행 중

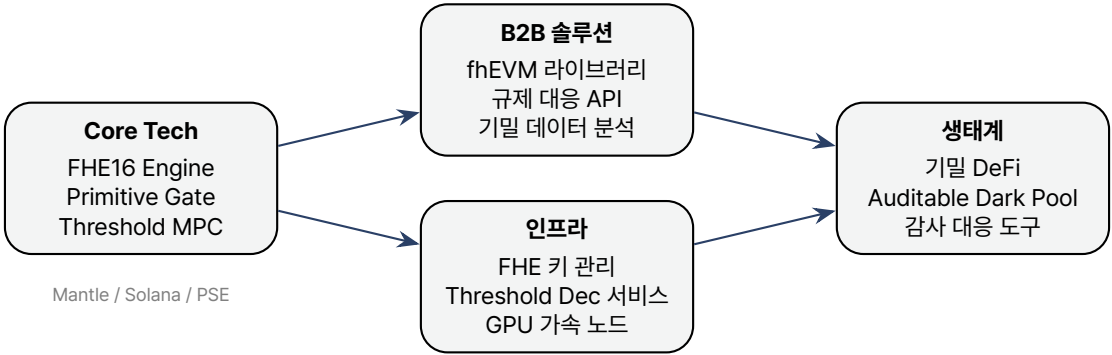
사업 현황

- **Mantle**: 네트워크 연동 진행 중
- **Solana**: Auditable Dark Pool 데모 완성, 생태계 협업 진행
- **PSE**: Privacy & Scaling Explorations 접촉 중

비전

격자 암호학(Lattice Cryptography)을 핵심 역량으로, 블록체인과 규제 환경에서 작동하는 **프라이버시 인프라**를 구축

사업 방향


Core Tech
FHE16 Engine
Primitive Gate
Threshold MPC
Mantle / Solana / PSE
B2B 솔루션
fhEVM 라이브러리
규제 대응 API
기밀 데이터 분석
인프라
FHE 키 관리
Threshold Dec 서비스
GPU 가속 노드
생태계
기밀 DeFi
Auditable Dark Pool
감사 대응 도구

요약

1. **블록체인 프라이버시의 근본 문제**: ZKP는 연산 불가, 기존 FHE(FFT)는 합의 불가
2. **LatticA**: “언제, 무엇을 공개할지” 온체인 제어 – 동형암호 + Threshold MPC
3. **Auditable Dark Pool**: Solana 위 ZKP + RLWE + Threshold 프로토타입 데모
4. **FHE16**: 16비트 정수만으로 2.89ms 부트스트래핑, 결정론적, 키 1/4
5. **Primitive Gate**: 단일 부트스트래핑 복합 게이트 $\Rightarrow$ latency 18∼50% 감소
6. **Actively Secure MPC** (Crypto 2025): Threshold FHE 키 생성 기반
7. **waLLLnut**: Mantle 연동, Solana 협업, PSE 접촉 – 격자 암호 기반 프라이버시 인프라

감사합니다

이승환
대표, waLLLnut (월넛 주식회사)

shlee@walllnut.com | t.me/scarrots

Q&A 환영합니다

References:

[1] Lee, Kim, Shin. “Fast and Compact Bootstrapping Using 16-bit Integer Arithmetic,” ePrint 2024/1916
[2] Kim, Kim, Lee, Shin. “Low-Latency FHE Arithmetic via Primitive Gate Bootstrapping,” ePrint 2025/2150
[3] Lee, Noh, Kim, Kim, Shin. “Actively Secure MPC in the Dishonest Majority Setting,” Crypto 2025
[4] Auditable Dark Pool: `https://github.com/Ham3798/auditable-dark-pool`