Compliant Transaction Privacy at ACM: Operator-Blind Computation and Regulator Forced Decryption via Threshold FHE and Association-Set Privacy Pools

ACM Global Tech

Abstract

ACM Global Tech licenses a regulated banking and digital-securities stack that treats privacy and compliance as complementary rather than opposed. As a W3A (`w3a.foundation`) member, ACM licenses this IP and partners to resell and co-build for regulated institutions, shipping a Stripe-class payment service provider, a full Banking-as-a-Service product, and a real-time AI/ML AML and transaction-monitoring engine. The stack is built on Lux (blockchain, post-quantum cryptography, and FHE), Hanzo (AI and data), and Zen (LLMs). This white paper describes ACM's privacy layer: an operator can compute over encrypted financial data without seeing plaintext, while a regulator holding a threshold of key shares retains the ability to force decryption for lawful inspection. The construction draws on threshold Fully Homomorphic Encryption (FHE) for regulatory compliance [1], the underlying torus-threshold FHE scheme [2], and compliant privacy pools that let users transact privately while proving non-association with illicit addresses [3].

1 The Problem: Privacy Versus Oversight

Regulated finance has historically forced a false choice. Full transparency exposes balances, counterparties, and strategies to the operator and to the public, which is unacceptable for institutional flow such as dark-pool matching or sealed-bid auctions. Full opacity, by contrast, defeats the lawful oversight that regulators require and creates a haven for illicit activity. A workable Digital Securities Platform must keep sensitive data confidential during ordinary operation while preserving a controlled, auditable path for lawful inspection—and it must do so without trusting a single operator or a single regulator with unilateral power over plaintext.

2 ACM's Approach

ACM's privacy layer combines two complementary mechanisms from the source research.

Operator-blind computation with forced decryption.
ACM uses threshold FHE so that an operator evaluates arbitrary boolean circuits on encrypted data without ever seeing plaintext, while a regulator holding t of n key shares can force decryption for lawful inspection [1]. The scheme combines TFHE gate evaluation (AND, OR, NOT, NAND, MUX over LWE ciphertexts on the torus $\mathbb{T}$) with Shamir-based threshold decryption, and is proven to satisfy operator blindness, threshold decryptability, and privacy below threshold [1]. The underlying primitive evaluates circuits via programmable bootstrapping with no inter-party interaction during computation [2].

Compliant privacy pools.
For value transfer, ACM uses privacy pools in which users transact privately yet prove, in zero knowledge, that they are not associated with sanctioned or illicit addresses [3]. A withdrawal requires a zero-knowledge proof of (i) a valid Merkle-tree deposit, (ii) membership in a curated association set of compliant addresses, and (iii) a fresh nullifier, and the system is proven sound, zero-knowledge, and complete [3].

Together these give ACM a privacy posture that is *compliance-first*: confidentiality is the default, but lawful inspection (via regulator threshold decryption) and provable non-association with illicit actors (via association-set proofs) are built in rather than bolted on.

3 Cryptographic Foundation

- **Threshold FHE with regulator forced decryption.** *Threshold FHE for Regulatory Compliance: Operator-Blind Computation with Forced Decryption* [1] presents the scheme, proves operator blindness, threshold decryptability, and privacy below threshold, and instantiates it across seven applications including private balance, encrypted transfer, sealed-bid auction, dark-pool matching, and compliance screening, at NIST Level 1 security.
- **Underlying torus-threshold FHE.** *Torus Threshold Fully Homomorphic Encryption: Boolean Circuits on Encrypted Data with Distributed Decryption* [2] provides the t-of-n TFHE primitive, evaluating boolean circuits via programmable bootstrapping with IND-CPA security under the LWE assumption.
- **Compliant privacy pools.** *Privacy Pools on Lux: Compliant Transaction Privacy with Association Sets* [3] extends the Privacy Pool framework of Buterin et al. with curated association sets and Groth16 zk-SNARKs over BLS12-381, and proves the withdrawal protocol sound, zero-knowledge, and complete.

4 Outcomes

1. **Confidentiality without trusting the operator.** The operator computes over ciphertext and never sees plaintext, so sensitive financial data stays confidential during ordinary operation [1, 2].
2. **Lawful inspection without a master key.** Forced decryption requires a regulator to assemble t of n shares, so oversight is possible but no single party can unilaterally decrypt below the threshold [1].
3. **Privacy that screens out illicit actors.** Association-set proofs let honest users keep transaction privacy while demonstrating non-association with sanctioned addresses, aligning privacy with AML expectations [3].
4. **Breadth of regulated use cases.** The threshold-FHE scheme is demonstrated across multiple financial applications (e.g., dark-pool matching, sealed-bid auctions, compliance screening), indicating the privacy layer's applicability beyond a single workflow [1].

References

[1] Z. Kelling. *Threshold FHE for Regulatory Compliance: Operator-Blind Computation with Forced Decryption*. Lux Industries, Inc. Source: `lux:threshold-fhe-compliance/threshold-fhe-compliance.tex`.

[2] Z. Kelling. *Torus Threshold Fully Homomorphic Encryption: Boolean Circuits on Encrypted Data with Distributed Decryption*. Lux Industries, Inc. Source: `lux:lux-tfhe/lux-tfhe.tex`.

[3] Z. Kelling. *Privacy Pools on Lux: Compliant Transaction Privacy with Association Sets*. Lux Industries, Inc. Source: `lux:lux-privacy-pool/lux-privacy-pool.tex`.