

DETECTING MONEY LAUNDERING ACROSS BANKS, WITHOUT COMPROMISING PRIVACY

Privacy-preserving Anti-Money Laundering (AML) and Anti-Terrorist Financing (ATF) detection using post-quantum cryptography.

THE EUROPEAN LANDSCAPE



**€750
BILLION**

Estimated illicit funds flowing through Europe's financial system annually.

Source: Nasdaq Verafin, 2024 Global Financial Crime Report



90%

Of alerts flagged by traditional AML transaction monitoring systems are false positives.

Source: Murphy, Robu & Steinert, "The investigator-centered approach to financial crime: Doing what matters", McKinsey & Company, 2020



**€20
BILLION**

Annual AML compliance costs for European banks.

Source: AML Watcher, 2026



4,633

Credit institutions operating in the EU as of January 2026.

Source: European Central Bank



0.1%

Of laundered money is successfully recovered globally.

Source: R. F. Pol, "Anti-money laundering: The world's least effective policy experiment? Together, we can fix it", Policy Design and Practice, 2020

HOW DOES MONEY LAUNDERING CROSS BANKS?

01 | FUNDS ENTER



Illicit money enters a bank account.



02 | MONEY MOVES

Transactions pass between banks, potentially obscuring the origin of the funds.



03 | THE PICTURE IS FRAGMENTED

Each bank sees only part of the transaction network.



WHY IS DETECTION DIFFICULT?



DATA PRIVACY

Regulations such as the GDPR and PSD2 restrict the sharing of sensitive customer data.



FRAGMENTED MONITORING

Traditional AML systems primarily analyse transactions within individual institutions.



FALSE POSITIVES

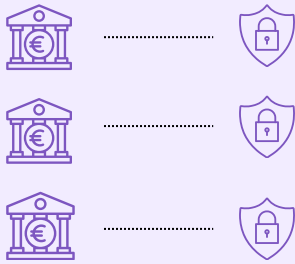
Many alerts require manual investigation but do not reveal criminal activity.

COLLABORATIVE RISK ANALYSIS THROUGH POST-QUANTUM CRYPTOGRAPHY

Q-FENCE enables banks to detect suspicious activity across their combined transaction networks without sharing customers' raw data.

01 | ENCRYPT

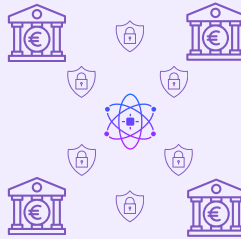
Each bank encrypts its account risk scores using Fully Homomorphic Encryption (CKKS), based on lattice cryptography.



DATA ENCRYPTED

02 | COMPUTE TOGETHER

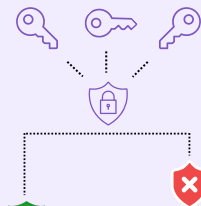
Banks exchange encrypted scores and calculate risk across inter-bank transactions without revealing the underlying scores.



COMPUTATION ON
ENCRYPTED DATA

03 | REVEAL THE RISK CATEGORY

Cooperative threshold decryption reveals only whether an account's estimated risk crosses a reporting boundary. No single bank can decrypt the result alone.



LOW

HIGH

CATEGORISATION

THE TECHNOLOGIES BEHIND THE APPROACH

FULLY HOMOMORPHIC ENCRYPTION



Enables calculations directly on encrypted data.

LATTICE-BASED CRYPTOGRAPHY



Provides the basis for the post-quantum security approach.

THRESHOLD DECRYPTION



Requires cooperation to reveal the permitted risk category.

POST-QUANTUM SIGNATURES AND AUDIT TRAIL



Support verification of computations without exposing private customer data.

PROTOTYPE TARGETS

3+

Simulated banking parties.

10,000+

Synthetic AML transactions for benchmarking.

OPENFHE

Framework used to implement the prototype.

EXPECTED BENEFITS

CROSS-BANK ANALYSIS

Assess suspicious transaction patterns across multiple institutions.

DATA CONFIDENTIALITY

Assess customer data and risk scores encrypted during collaborative analysis.

COMPATIBILITY

Apply an encrypted scoring approach that is agnostic to the underlying local AML scheme.

REGULATORY VERIFICATION

Support verification of computations without requiring access to private customer data.



Use case lead: University of Luxembourg (UL)



Participating organisations: UL · MI · RHI · SETU · FIPMS



Sector: Financial services and banking



Region: Luxembourg / European Union



FIND OUT MORE



@Q-FENCE

www.qfence-project.eu