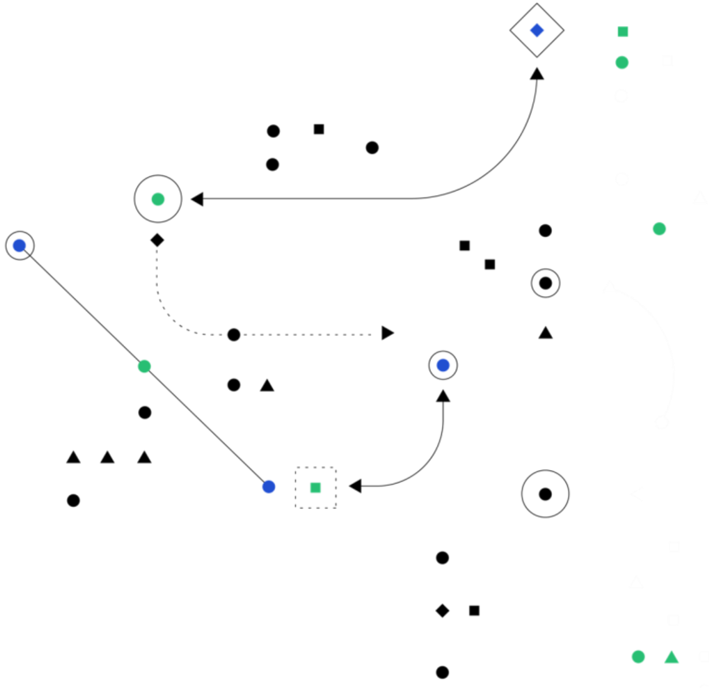
Privacy-Preserving Data Sharing across Financial Institutions

Andreea Alexandru
Cryptography Scientist
aalexandru@dualitytech.com

Kurt Rohloff
Co-founder, CTO
krohloff@dualitytech.com

Presented at NIST Workshop on Privacy-Enhancing Cryptography 2024

Agenda



1. Introduction
2. UK Information Commissioner’s Office use-case
3. Singapore IMDA PET Sandbox – Mastercard use-case
4. Driving collaboration in public-private partnerships
5. Conclusions

Introduction

- Government and financial institutions need to handle and collaborate on sensitive information.
  - Personal, financial, and proprietary data -- **breaches could have severe consequences**
  - Enterprise data resides in silos across departments, across entities and across geographies

- Ensuring that this data is **protected while still accessible** for use is critical to maintaining public trust and adhering to legal standards
  - **Sharing PII/CI**: anti-financial crime legislations such as USA PATRIOT Act and EU 5th Anti-Money Laundering Directive
  - Regulations for data privacy, data security, data sovereignty

➢ Traditional methods offer awkward **guardrails** to protect **data in-use**

  ➢ **Need for open transparent approaches to privacy-protected data collaboration.**

Introduction

- **Private search** (Private Set Intersection, Private Information Retrieval)
  - Ability to query external data without revealing:
    - The query to the data owner or
    - The dataset to the inquirer

- **Fully Homomorphic Encryption** (FHE)
  - Ability to compute and share insights between parties without either party learning the other's private data
  - Single-key and threshold-key settings

- Identify challenges and insights from real-world use-cases of fighting financial crime
- Solutions to the use-cases were implemented on top of the open-source FHE library OpenFHE

Insight/Challenge for governance/law

Insight/Challenge for cryptography

ICO private data sharing use-case

- Information Commissioner’s Office (ICO) – UK GDPR guidance and resources
- Use-case “Homomorphic encryption for data sharing” developed in collaboration with Duality

Background

- Law Enforcement Agencies and private sector partners (banks) need to share **PII** to detect and prevent financial crimes
- Investigations on suspected fraud may require data from many different entities
- Certain data **cannot be shared** until suspicion threshold is reached – which may never happen

Investigate first to confirm suspicions

Illegal to make queries in the clear

Encrypted requests comply with data protection laws

Need encrypted SQL-like queries for “suspicion confirmation”

ICO private data sharing use-case

Solution

- The inquirer deploys **homomorphically encrypted queries** to hide subjects of investigation/CI
- The consortium members return the encrypted result of the private search to the inquirer

"Has any account owned by [John Smith; NI# AB1234C, DOB 01/01/1980] received transfers from high-risk jurisdictions in the last [30] days? If so, how many transactions from how many jurisdictions?"

"Has any account owned by [*****; NI# *****, DOB *****] received transfers from high-risk jurisdictions in the last [*****] days? If so, how many transactions from how many jurisdictions?"

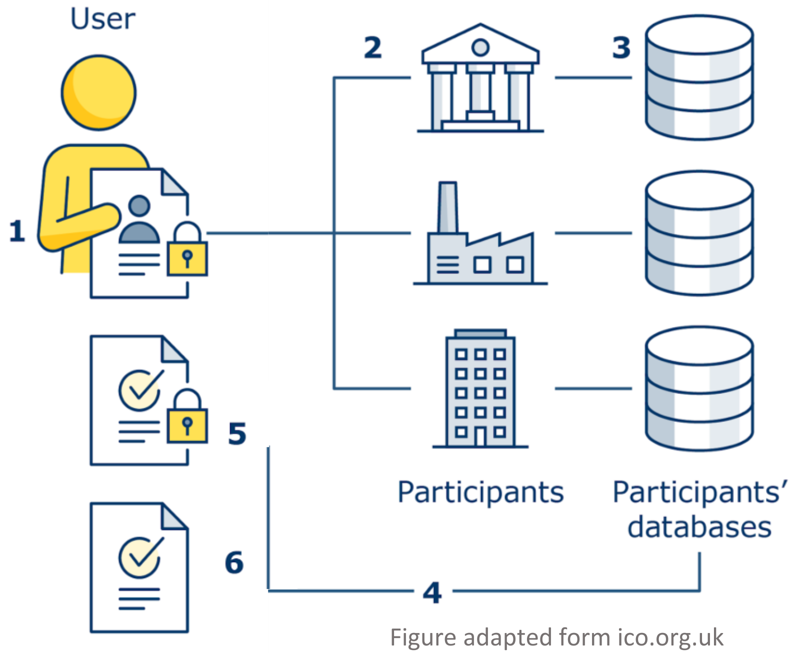


Figure adapted form ico.org.uk

Results

- **Ability to securely share insights** – even "pre-suspicion" and without moving the data
- **Responses in minutes** rather than weeks
- Ability to collaborate **in compliance with GDPR**

Coordinate the entities and aggregate responses

Allow only lawful queries

Validation and guardrails

ICO private data sharing use-case

- **Hub**
  - Establish the allowed query formats
  - Restrict the number and rate of queries
  - Hide the roles of the parties (inquirer/data owner)
  - Aggregate results (without ability to decrypt)

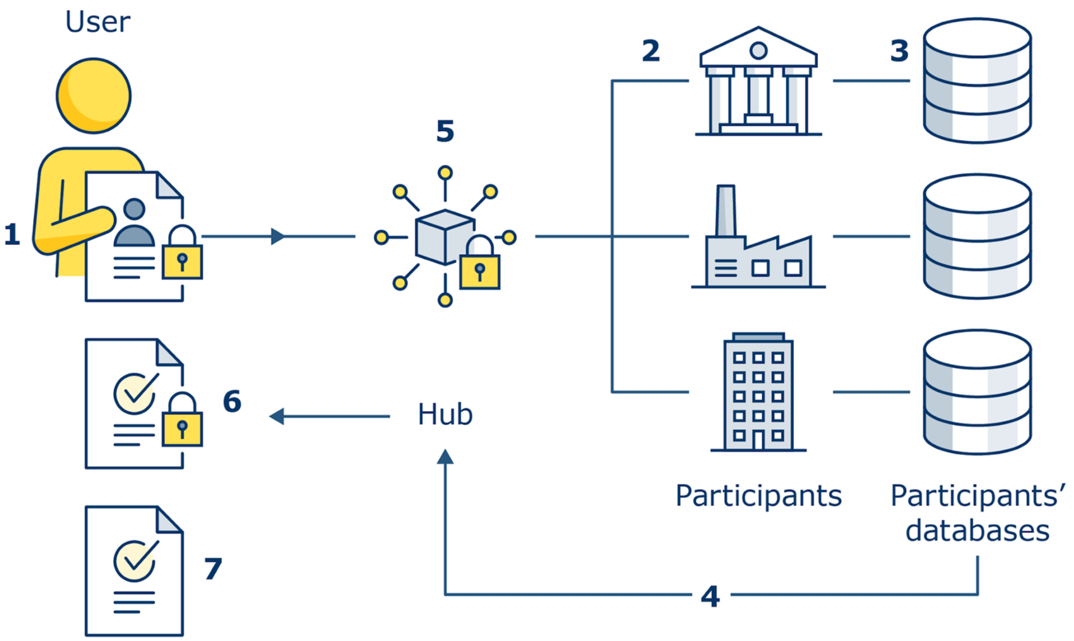


Figure taken from ico.org.uk

Trust Assumptions and Guarantees

- **Query privacy** guaranteed even against malicious users
- **Response correctness** against malicious users requires verifiable computation and/or legal deterrents
- **Database privacy** against malicious users requires verifiable computation and/or disallowing functionalities that reveal "too much"
- Non-collusion

IMDA PET SANDBOX - Mastercard

Background

- Infocomm Media Development Authority (Singapore government) PET Sandbox Program
  - “**safe space to trial PETs**”

- Mastercard seeks to work **across jurisdictions** to prevent, detect, and investigate financial crimes
  - US
  - Singapore
  - UK
  - India

- Comply with all data protection, data privacy, data sovereignty, and financial industry regulations across the four jurisdictions

Data localization: cross-border exchanges

Encrypted queries and aggregated responses

Reduced communication and interactions

IMDA PET SANDBOX - Mastercard

Solution

- Deploy FHE-encrypted queries **without exposing investigation targets** or **moving data**
- FHE-encrypted queries and responses are **safe to move across jurisdictions**
- **One-hop** private search solution with reduced online/offline communication

Results

- **Compliance with all applicable laws** in Singapore, UK, USA, and India
- **Responses in minutes** rather than weeks
- Enhanced **data quality** and **insights**

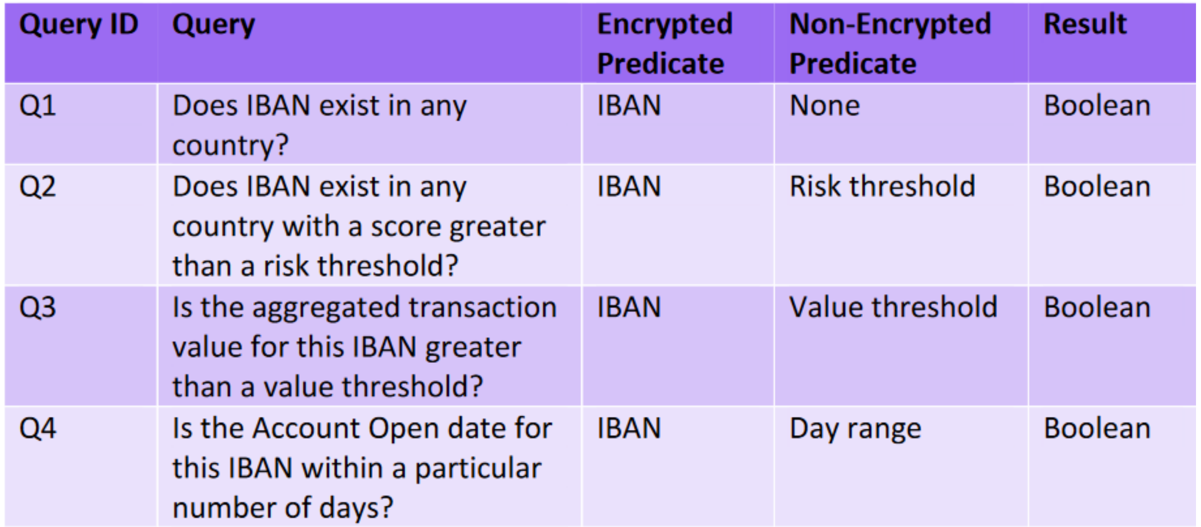
IMDA PET SANDBOX

Governance Assessment

- It is crucial that the response (True/False) to the query reveals **minimal customer information**
- A response might divulge a (non-public) relationship between the customer and the bank
- It was deemed by IMDA that only receiving the **aggregated** response does **not breach secrecy** of CI

Technical Assessment

- Node locations affect round-trip time
- Compound queries to reduce searched data
- Governance processes need to be updated to accommodate management of FHE keys



Query ID	Query	Encrypted Predicate	Non-Encrypted Predicate	Result
Q1	Does IBAN exist in any country?	IBAN	None	Boolean
Q2	Does IBAN exist in any country with a score greater than a risk threshold?	IBAN	Risk threshold	Boolean
Q3	Is the aggregated transaction value for this IBAN greater than a value threshold?	IBAN	Value threshold	Boolean
Q4	Is the Account Open date for this IBAN within a particular number of days?	IBAN	Day range	Boolean

Figure taken form imda.gov.sg

Driving collaboration in public-private partnerships

Background

- When government agencies conduct investigations, nobody outside the agency should be aware of who is under investigation
- Traditionally, agencies **purchase entire datasets** from data brokers and transfer to internal storage
- **Entity resolution** is a real need

➢ Law Enforcement Agencies are hesitant to leverage cloud/OSINT data for investigations

Reluctance to move data from cloud to premises

Private access to third-party data

Reduced storage on premises, reduced interaction

Entity resolution and analytics on encrypted data

Driving collaboration in public-private partnerships

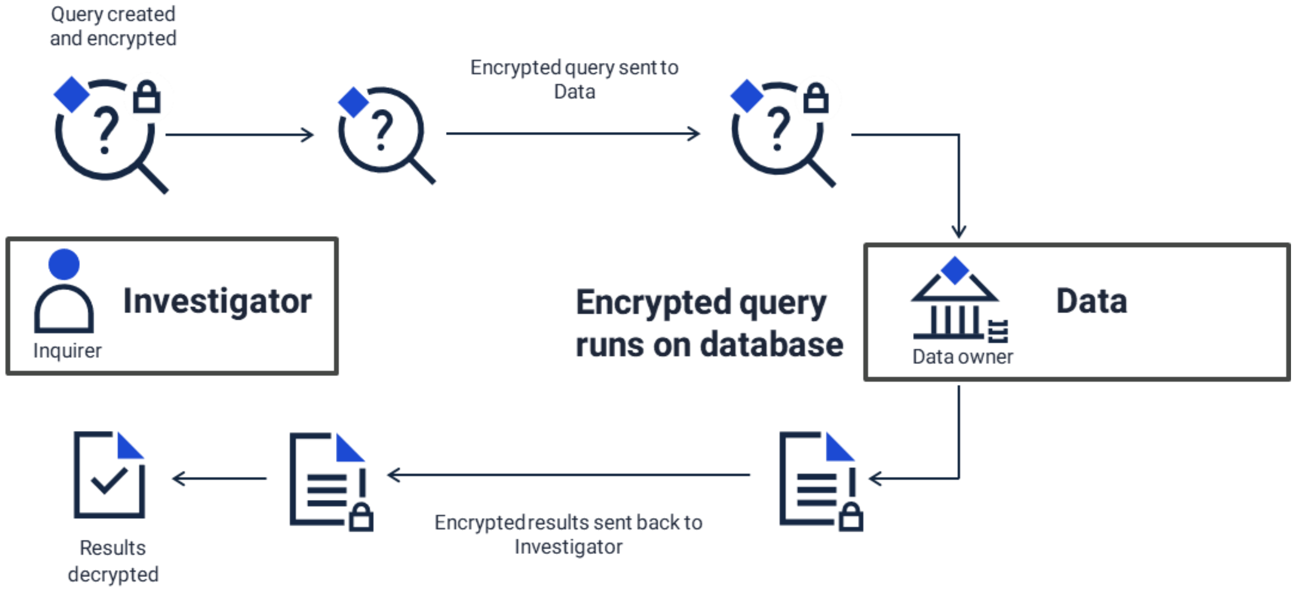
London Stock Exchange Group acts as a data broker for government agencies via Duality

Solution

- FHE-encrypted queries with **encrypted analytics** over the data

Results

- Enhanced **data quality**
- Significantly **reduced cost**
- Ability to maintain **operational security**

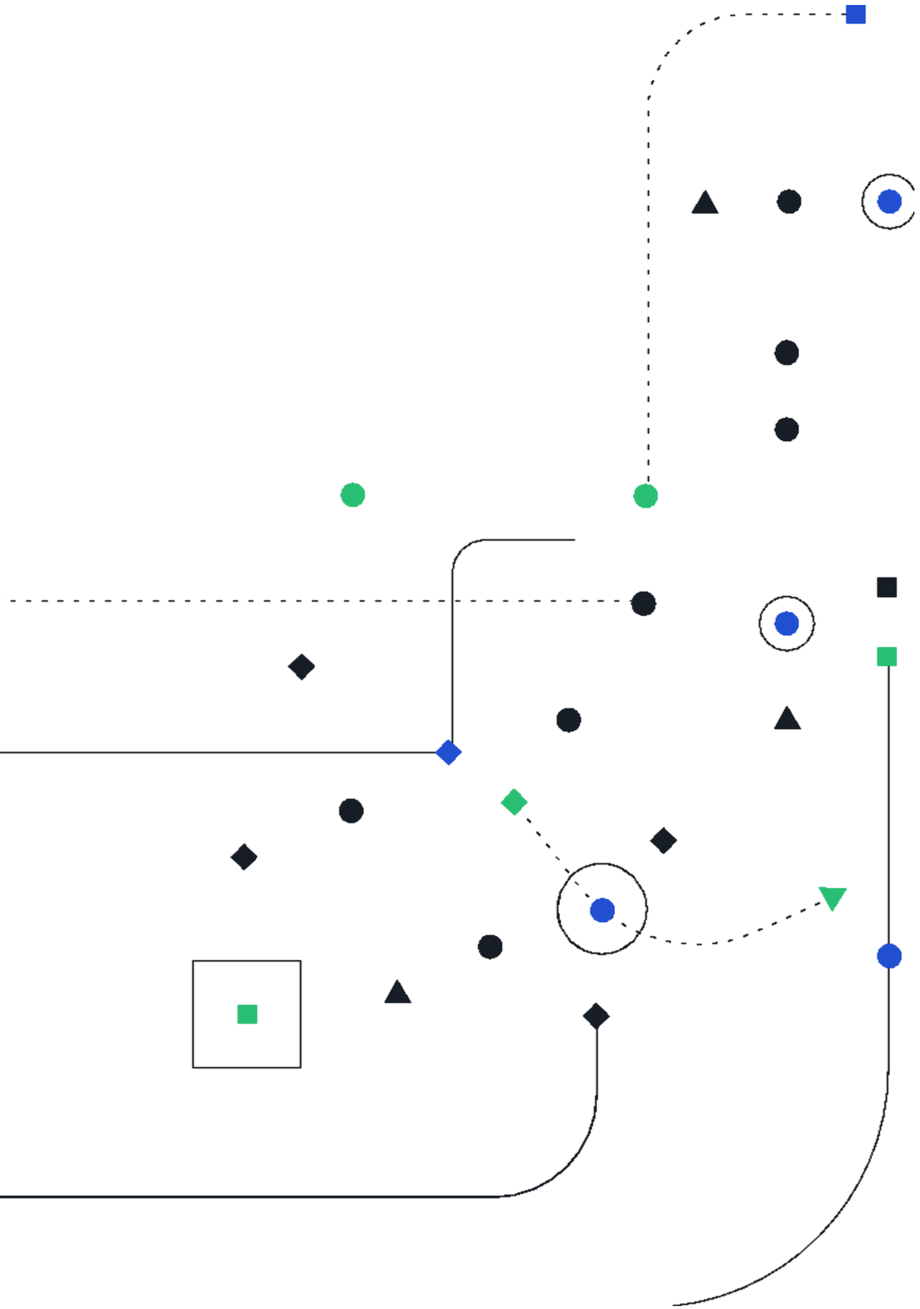

Query created and encrypted
Encrypted query sent to Data
Investigator
Inquirer
Encrypted query runs on database
Data
Data owner
Encrypted results sent back to Investigator
Results decrypted

Conclusion: **Both governance and advanced technologies** are necessary to unlock the value of data for collective benefit

- **Enhanced Data Infrastructure and Skills**
  - Developing advanced cross-domain data infrastructure can improve capabilities in cybersecurity, threat detection, informed policymaking, efficient public service delivery, and reduced operational costs
- **High Data Protection Standards**
  - Adopting strong, FHE-based data protection measures ensures that sensitive data is safeguarded, maintaining the integrity and security of operations
- **Market Need for Standardization**
  - Transparent, secure and standardized data practices build public trust, encouraging citizen participation in data-sharing initiatives

Acknowledgments and References

- Thank you to Yuriy Polyakov, Ronen Cohen, Derek Wood and Rina Shainski for providing slides material
- ICO use-case: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies/case-studies/homomorphic-encryption-for-data-sharing/
- Mastercard use-case: https://www.imda.gov.sg/-/media/imda/files/programme/pet-sandbox/imda-pet-sandbox--case-study--mastercard.pdf
- LSEG/Refinitiv collaboration: https://dualitytech.com/blog/how-to-grow-government-data-contracts-with-zero-footprint-investigations-zero-trust/, https://solutions.lseg.com/LP=20457



Duality

OpenFHE

Thank you!

Andreea Alexandru
Cryptography Scientist
aalexandru@dualitytech.com

Kurt Rohloff
Founder, CTO
krohloff@dualitytech.com