Duality

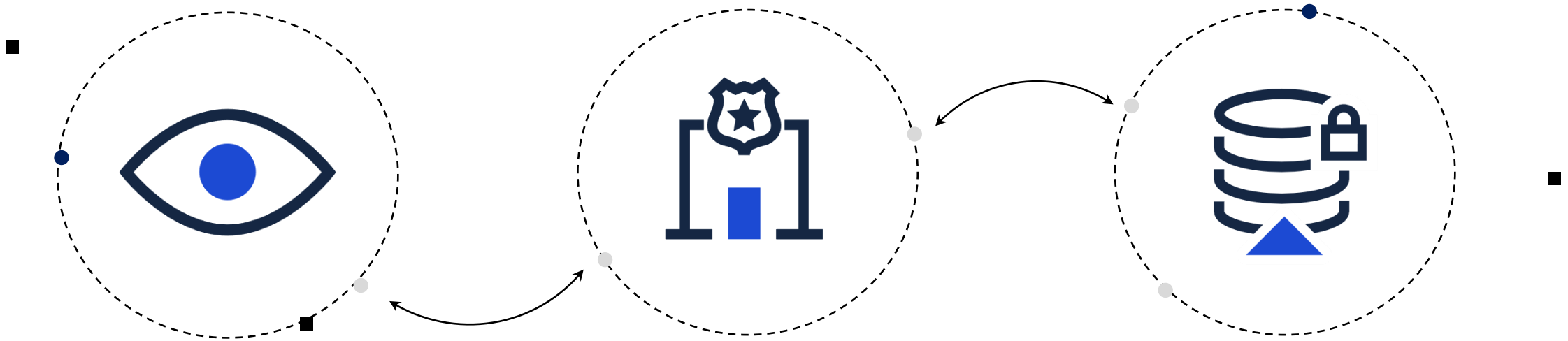
The HomomorphicEncryption.org Community and the Applied Fully Homomorphic Encryption Standardization Efforts

Kurt Rohloff
krohloff@dualitytech.com

Presentation for NIST STPPA6

07/25/2023

The Data Collaboration Challenge



What are we standardizing? Data Collaboration Tools
PETs: Enrich and Analyze Encrypted Data

Join, link, and enrich encrypted datasets

Apply analytics, ML, and AI on encrypted and/or decentralized data

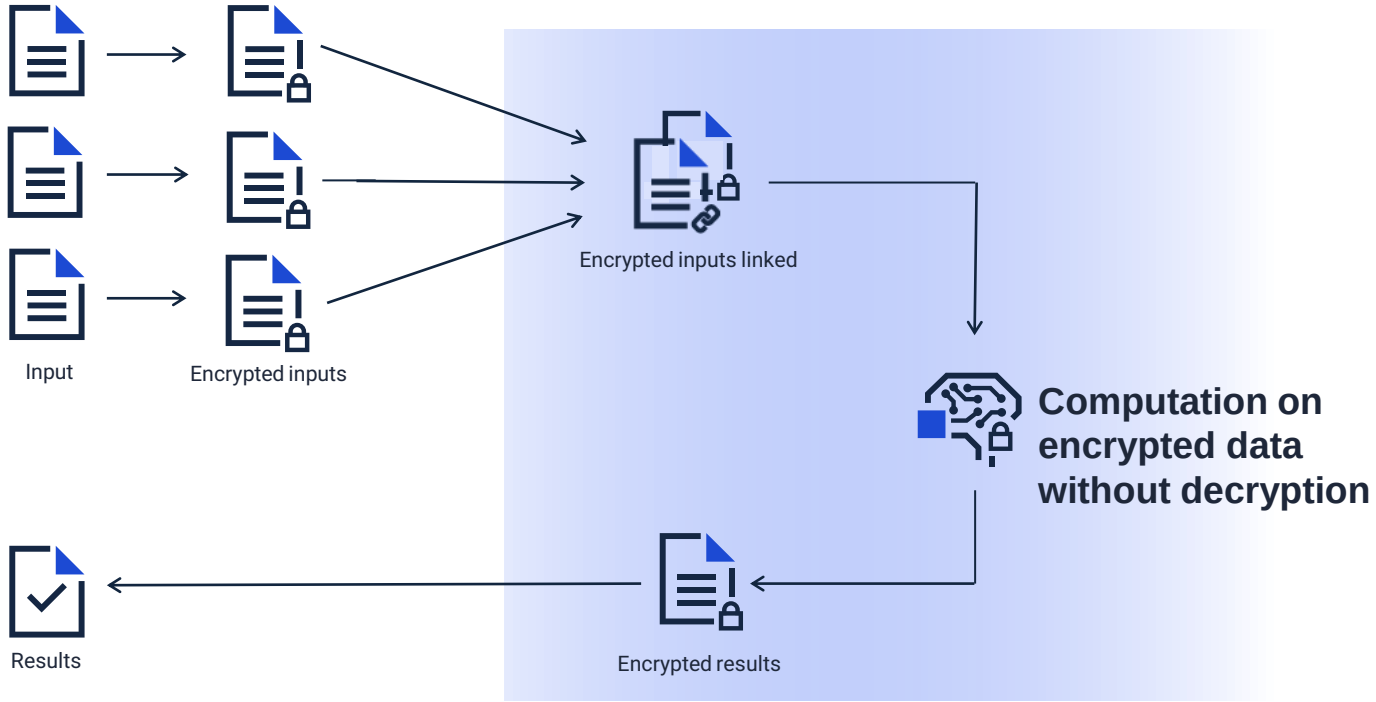
Open-source and standardized encryption trusted by enterprises and the public sector

- Regulatory Compliance and Support ✓
- End to end encryption ✓
- Exact results for general computations ✓
- Accurate for individual-level insights ✓
- Resistant to quantum computing attacks ✓
- Existing Industry Standards ✓
- Collaborate on encrypted data, models, or linked datasets ✓

Duality

Analytics and Machine Learning Application

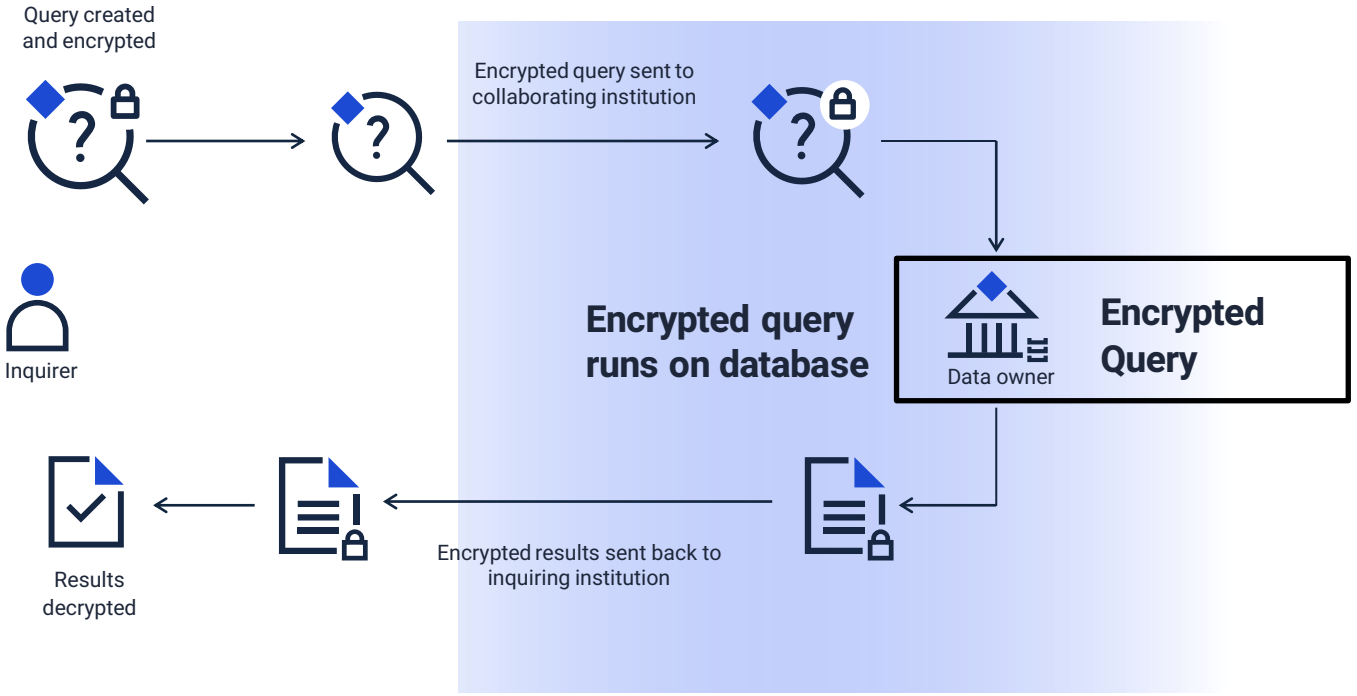
- Relies on Threshold FHE
- Aggregate encrypted data from multiple sources
- Machine learning while preserving privacy and trust



- Statistics & Inferences on encrypted data
- Privacy and confidentiality preserved
- Supported by regulators
- Compliant with privacy and industry regulations

Query Application

- Enabling secure collaboration on sensitive data while preserving privacy and trust



- Encrypt Queries and keep them private
- Privacy and confidentiality preserved
- Compliant with privacy and industry regulations

Public / Private Collaboration

BACKGROUND

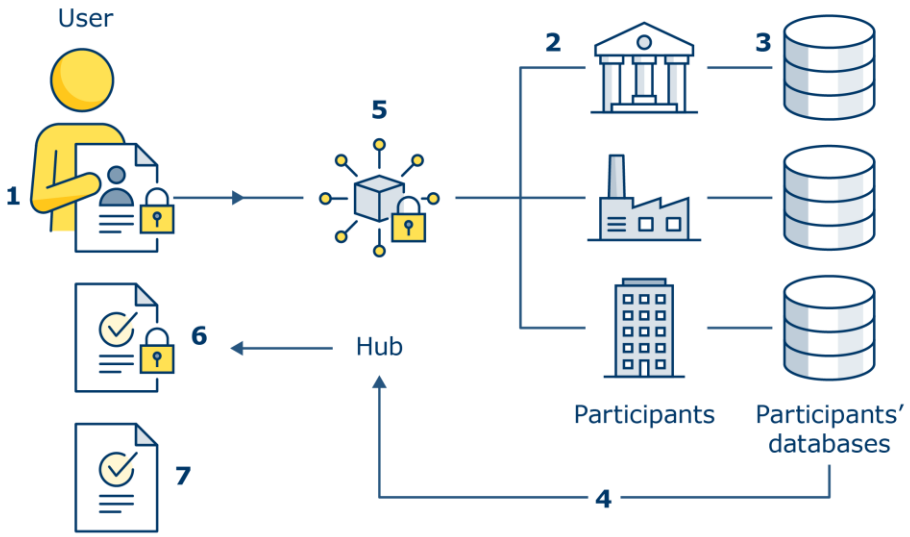
- LEA and private sector partners need to share PII to detect and prevent financial crimes, and investigate networks
- Certain data cannot be shared until suspicion threshold is reached – which may never happen

SOLUTION

- Each participant deploys **encrypted queries** to hide subjects of investigation / customer info
- Insights can be shared **without moving data**

RESULTS

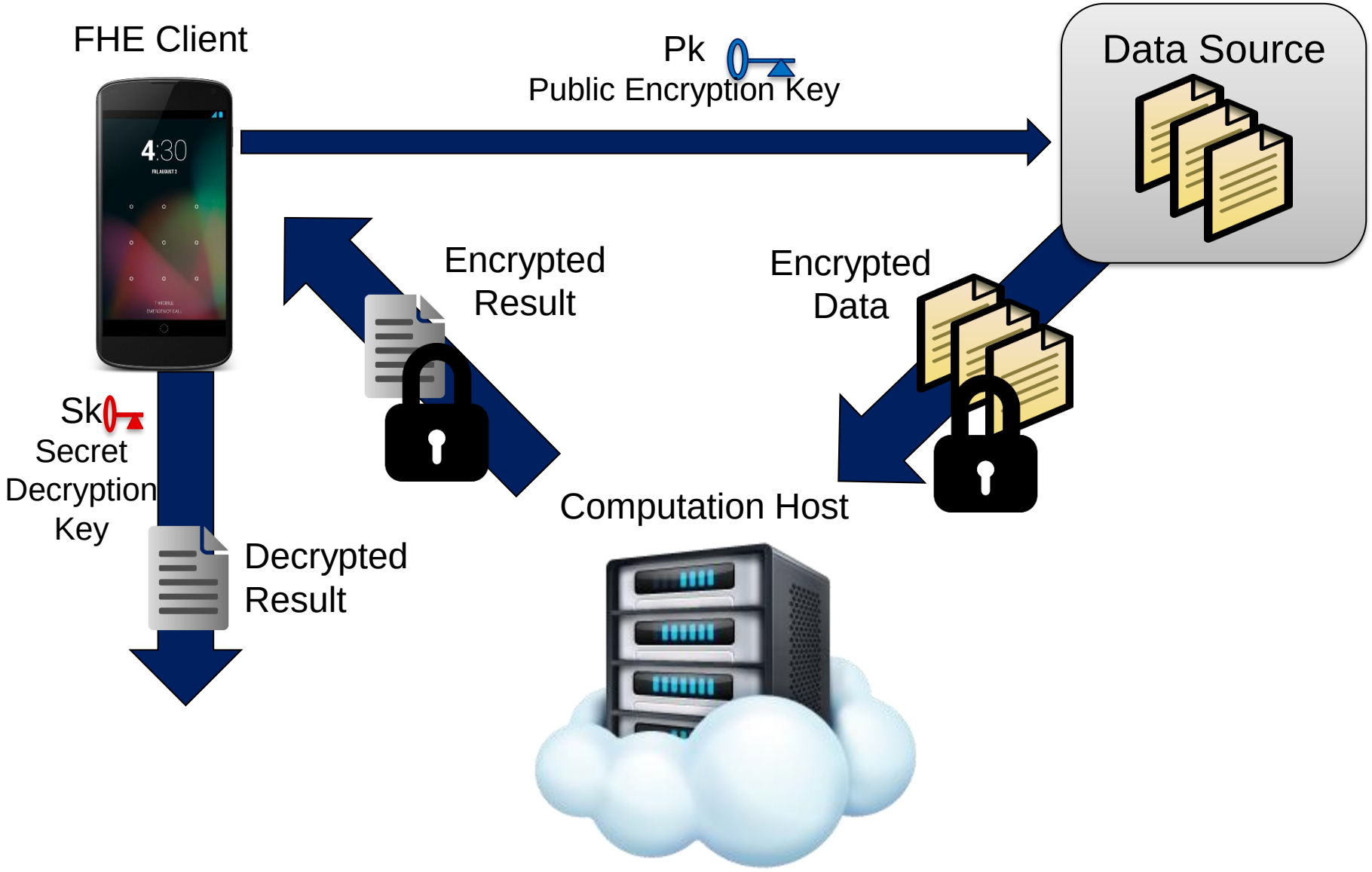
- **Ability to share data – even "pre suspicion"**
- **Responses in minutes** rather than weeks
- **Improved attribution and case building**
- Ability to collaborate **in compliance with GDPR**



"If your organisation shares large volumes of data, particularly special category data, **we recommend that… you start considering using PETs**."

~John Edwards, UK Information Commissioner

Fully Homomorphic Encryption

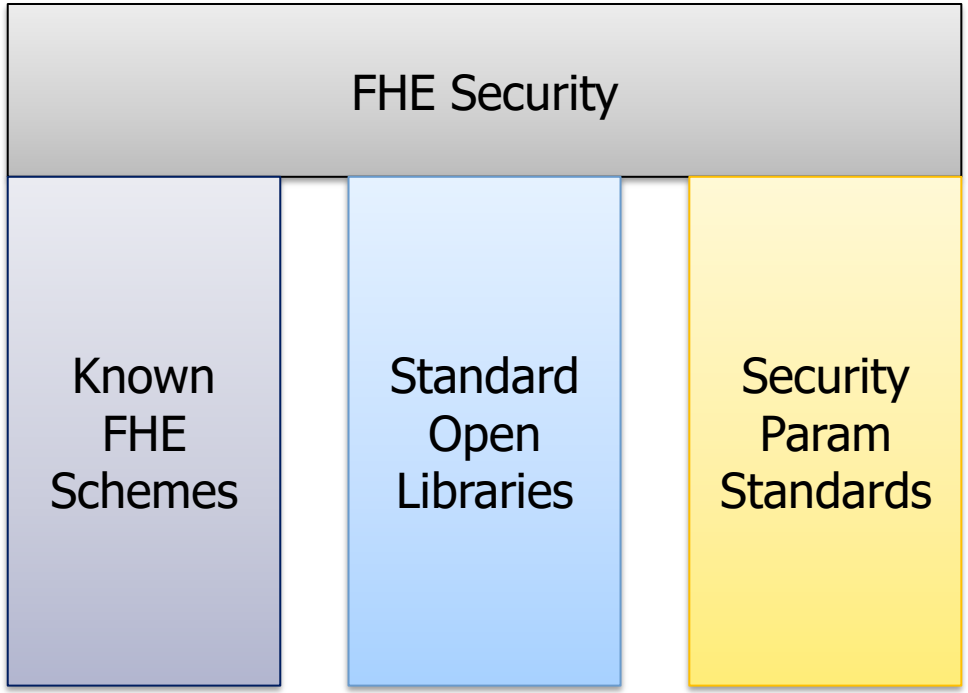


Duality

Security and Trust – This REALLY Matters

Adoption of PETS and FHE is a three-legged stool

- Imperative to use general, certified techniques.
  - Avoid customizations and short-cuts that impact security.
- Use ONLY Known and Vetted FHE Schemes
  - BGV / BFV, CKKS and TFHE / FHEW - All use same security properties
- Standard Open-Source Libraries
  - Need to be able to trace contributions



- Security Standards
  - For FHE - homomorphicencryption.org
  - Standard provides scheme designs and security parameters.
  - ***Religiously follow ALL security standards***

http://homomorphicencryption.org/wp-content/uploads/2018/11/HomomorphicEncryptionStandardv1.1.pdf

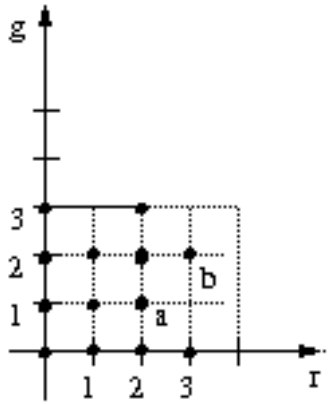
Duality

FHE Schemes

- Earliest: Craig Gentry Thesis (2009)
  - Early implementation by Shai Halevi and Gentry
  - Inefficient runtime, ½ hour for bitwise AND operation on encrypted data.
  - Innovation: Bootstrapping
- 2nd generation: BV/BGV schemes (2011), NTRU/LTV (2011), GSW
  - BV/BGV is one of the main practical schemes used now.
    - Innovation: “Leveling” to allow practical Somewhat Homomorphic Encryption (SHE) without bootstrapping. Enables depth-n computations, as long as n is less than 16 or so.
- 3rd generation : BFV, BFV_rns, CKKS, FHEW, TFHE
  - All of these schemes are currently widely used.
  - Different applications for different FHE protocols.

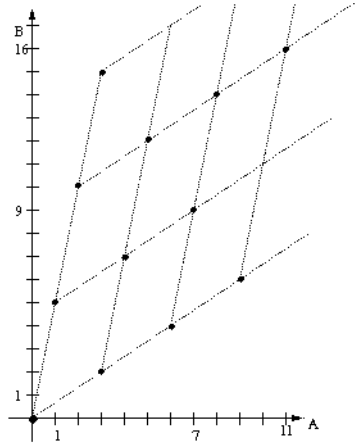
Lattice Encryption Intuition?

- Encryption, Decryption, etc… are primarily composed of linear transforms over large integer vectors.



Plaintext space

Linear transforms and add noise

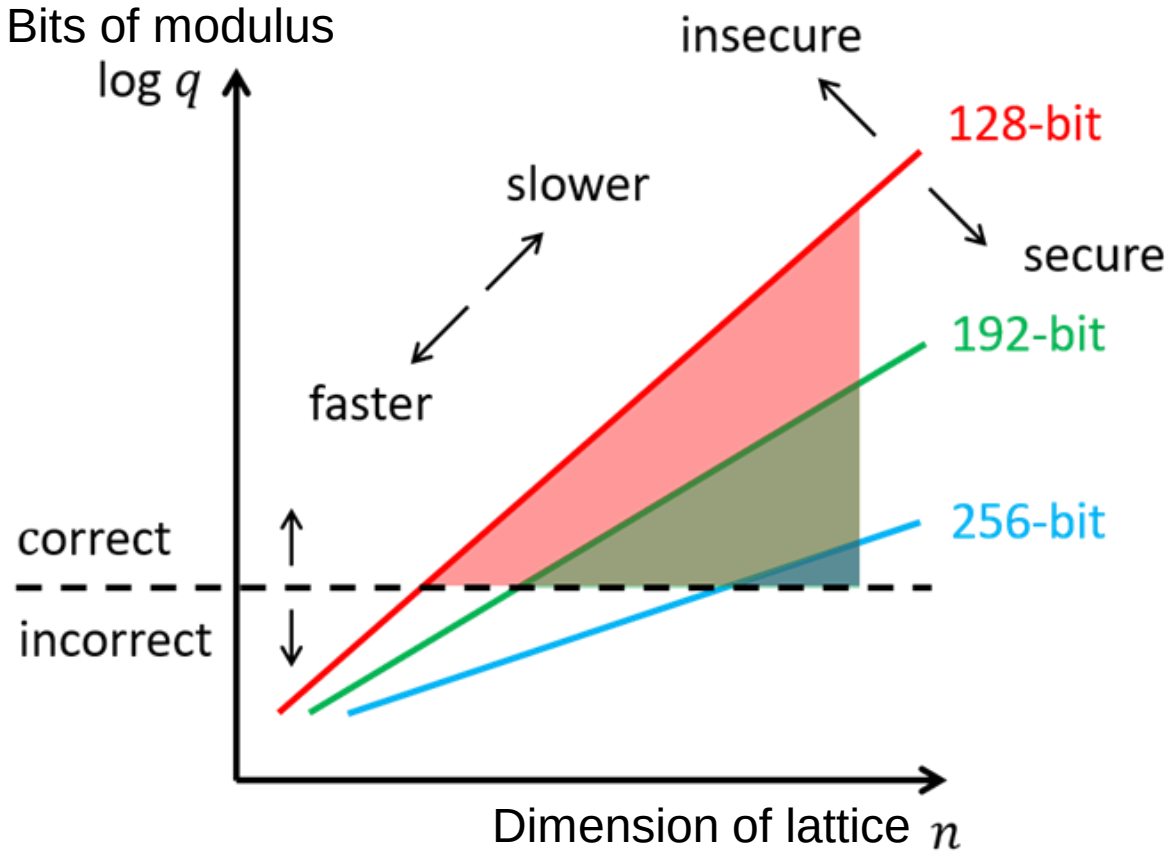


Ciphertext space

Duality

Security, Correctness and Performance Tradeoffs

- Need to maximize performance while guaranteeing correctness and security.
- Security in FHE is captured by “bits of security”.
  - Comes from “brute force attack estimates.”
  - FHE resistant to quantum computing attacks.

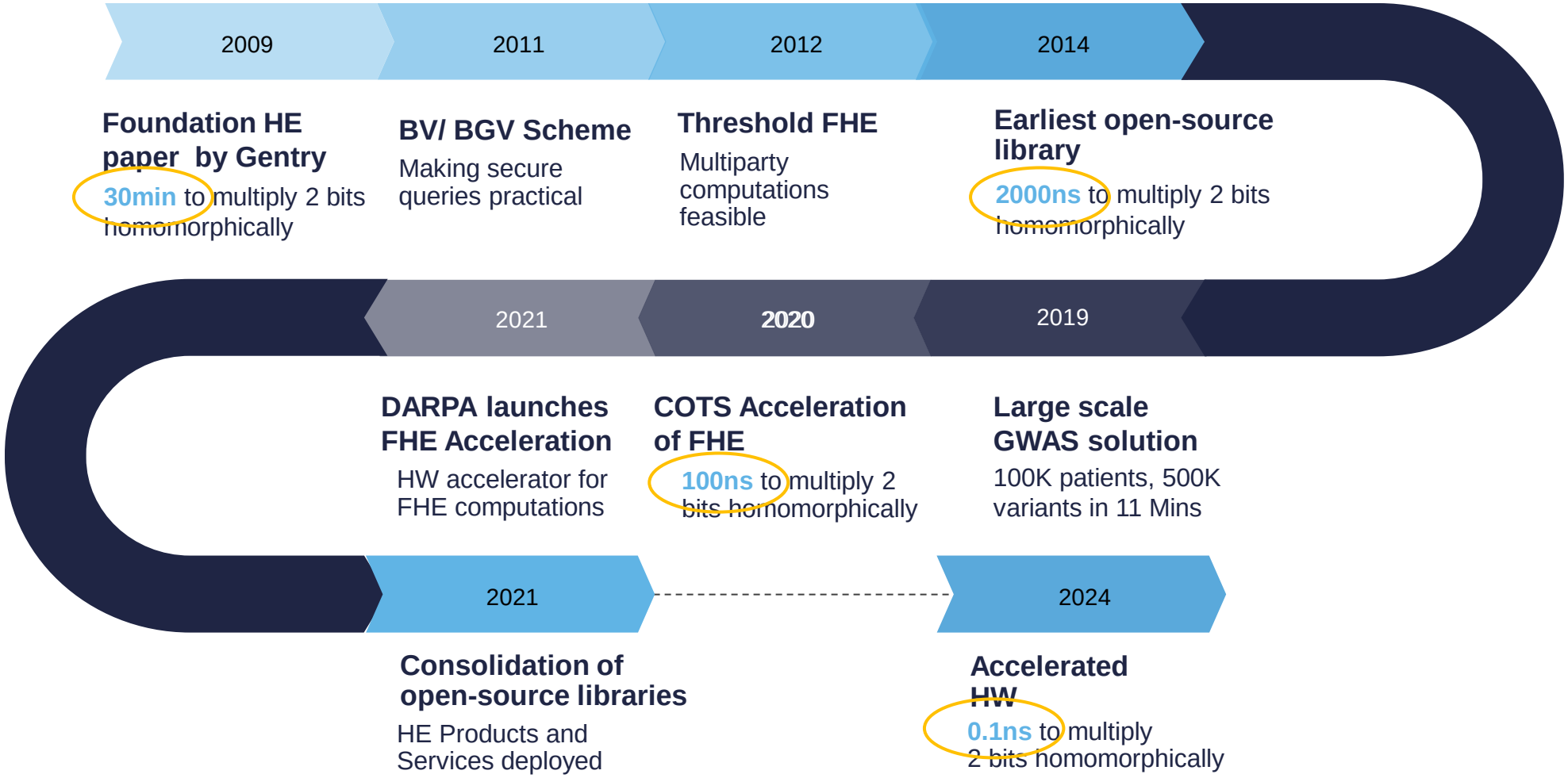


Duality

Libraries

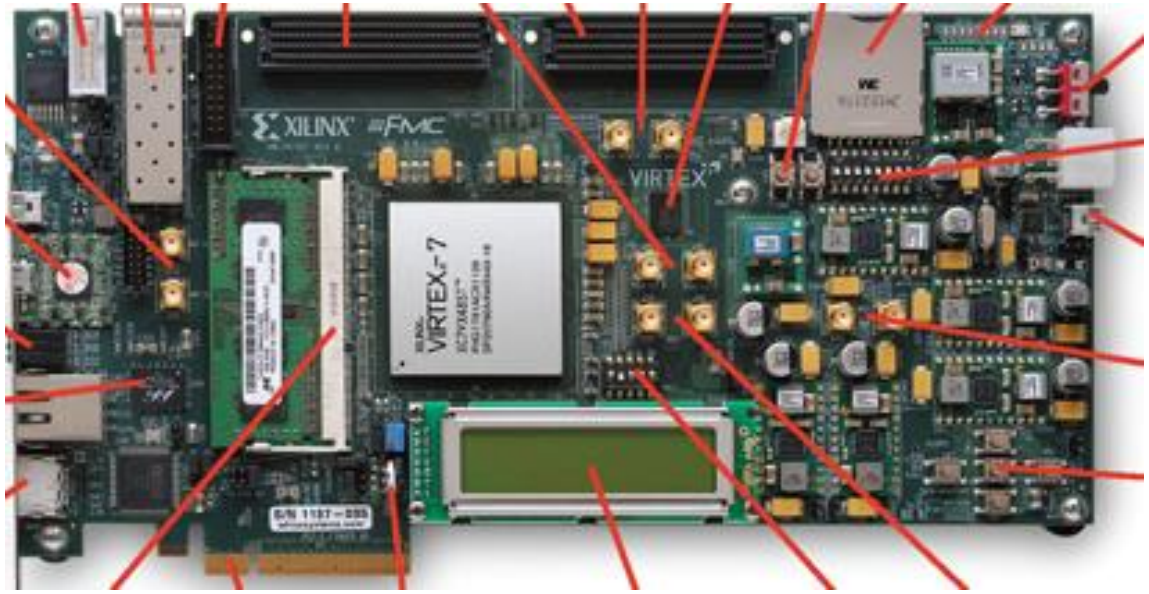
- OpenFHE / PALISADE
  - What we use at Duality. Came out of DARPA community.
- HELib
  - by IBM. The oldest active library supports BGV.
- SEAL
  - by Microsoft Research supports CKKS. Less actively developed now.
- LattiGo
  - implements major schemes in Go
- HEANN
  - Korean approximate scheme with CKKS.
- TFHE and Concrete
  - Implement the TFHE protocol.

Performance and Maturity Over Time



Hardware Acceleration

- This is a major emerging topic in the FHE community.
- We're tracking this closely to support interoperability between libraries and hardware.
- Duality, Intel, Cornami, Optalysys, ChainReaction, etc…



Duality

HomomorphicEncryption.org Standards

- Standards compliance provides crypto-agility, resilience and trust
    - Security standards defined by the HomomorphicEncryption.org consortium

- Consortium is organically led and includes leading government, private sector, and academic organizations:
    - Intel, IBM, Microsoft, Samsung, SAP, Google, Inuit, and many more…
    - NIH, NIST, CSE and many more…
    - MIT, NJIT, UCSD, and many more…

- Standard is in the process of being adopted by major international standards bodies, notably the UN-ITU and ISO

15
Duality

Proposed Drafts (1/2)

- Use Cases and Threat Models
  - Genome Wide Association Studies
  - VoIP Mixing
  - Health Risk Scores
  - ML Inference
  - ML Training

Thank you!

- Kurt Rohloff
  - krohloff@dualitytech.com