IBM WW Z Security Conference

October 6-9, 2020

IBM Homomorphic Encryption

Flavio Bergamaschi
Senior Research Scientist
flavio@uk.ibm.com

Eli M Dow
Senior Technical Staff Member
emdow@us.ibm.com

Rushir Patel
Offering Manager
rushir.patel@ibm.com

Agenda

Intro to Homomorphic Encryption

Use Cases, IBM HE Toolkit, Demo

Community Engagement and Openness

Question and Answer

What is Homomorphic Encryption?

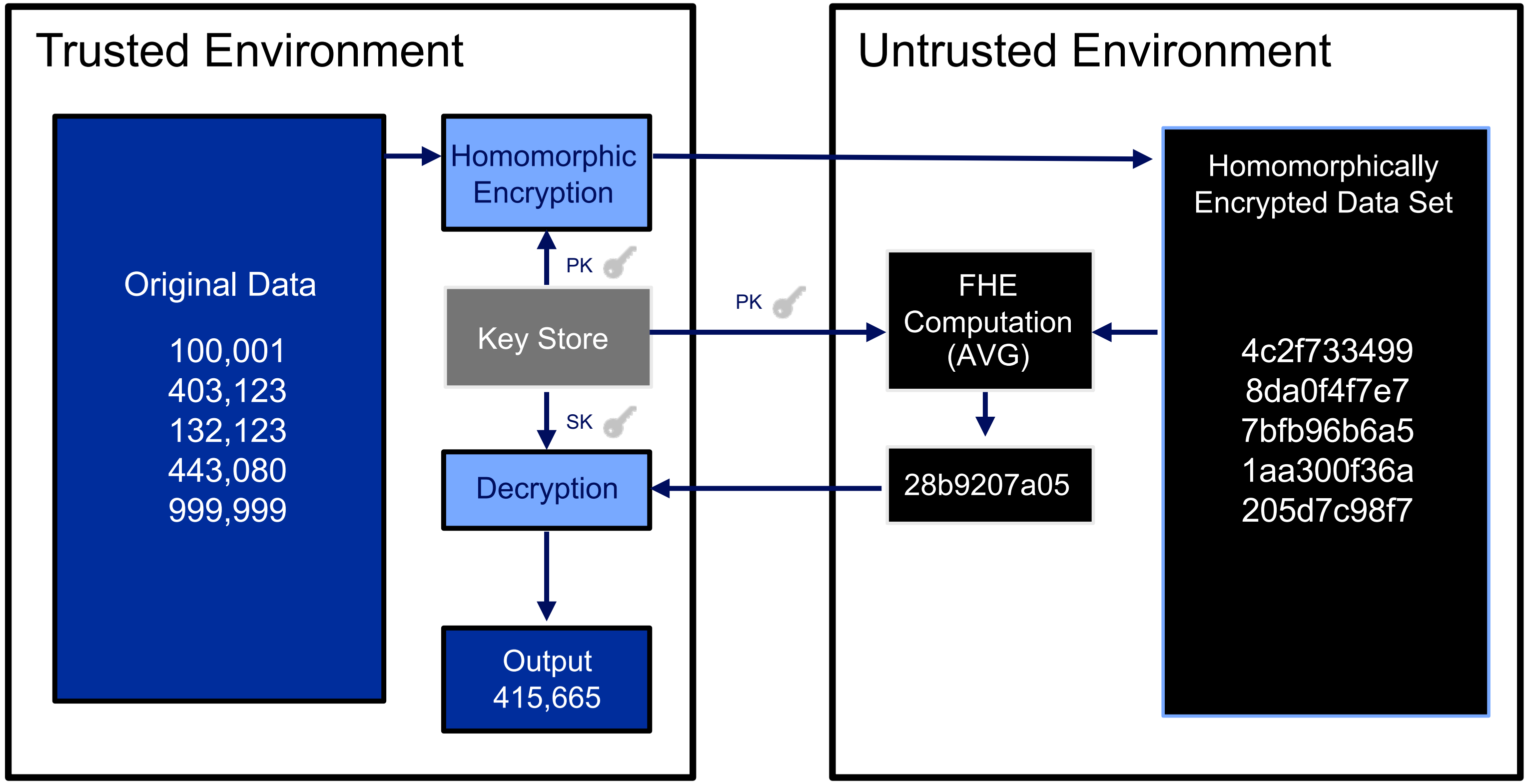
Enables the processing of data without giving access to it

Technically achieved by computing on encrypted data

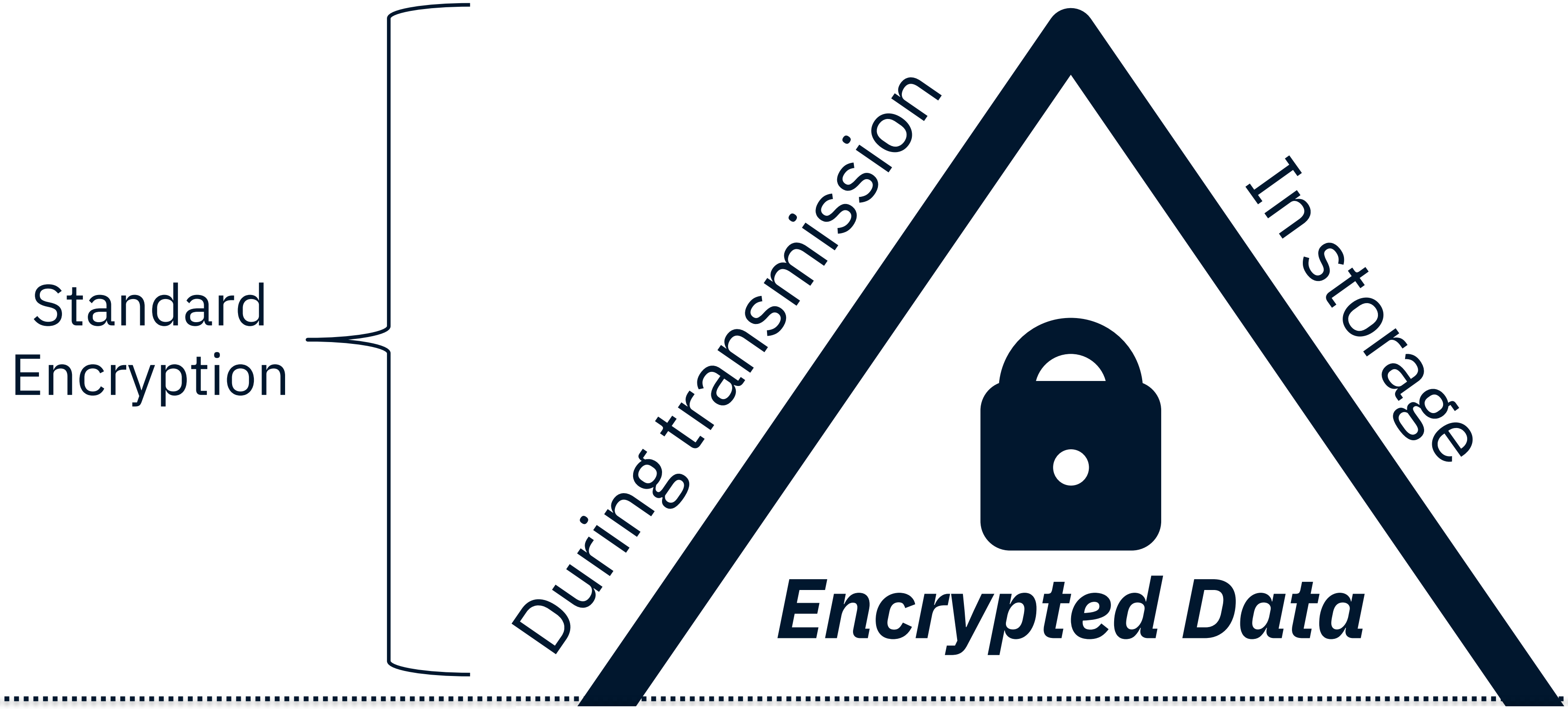
Resolves the paradox of “need to know” vs “need to share”

Uses Lattice Cryptography -> Quantum Resistant

Different sub-types of HE: Fully, Partial, Somewhat

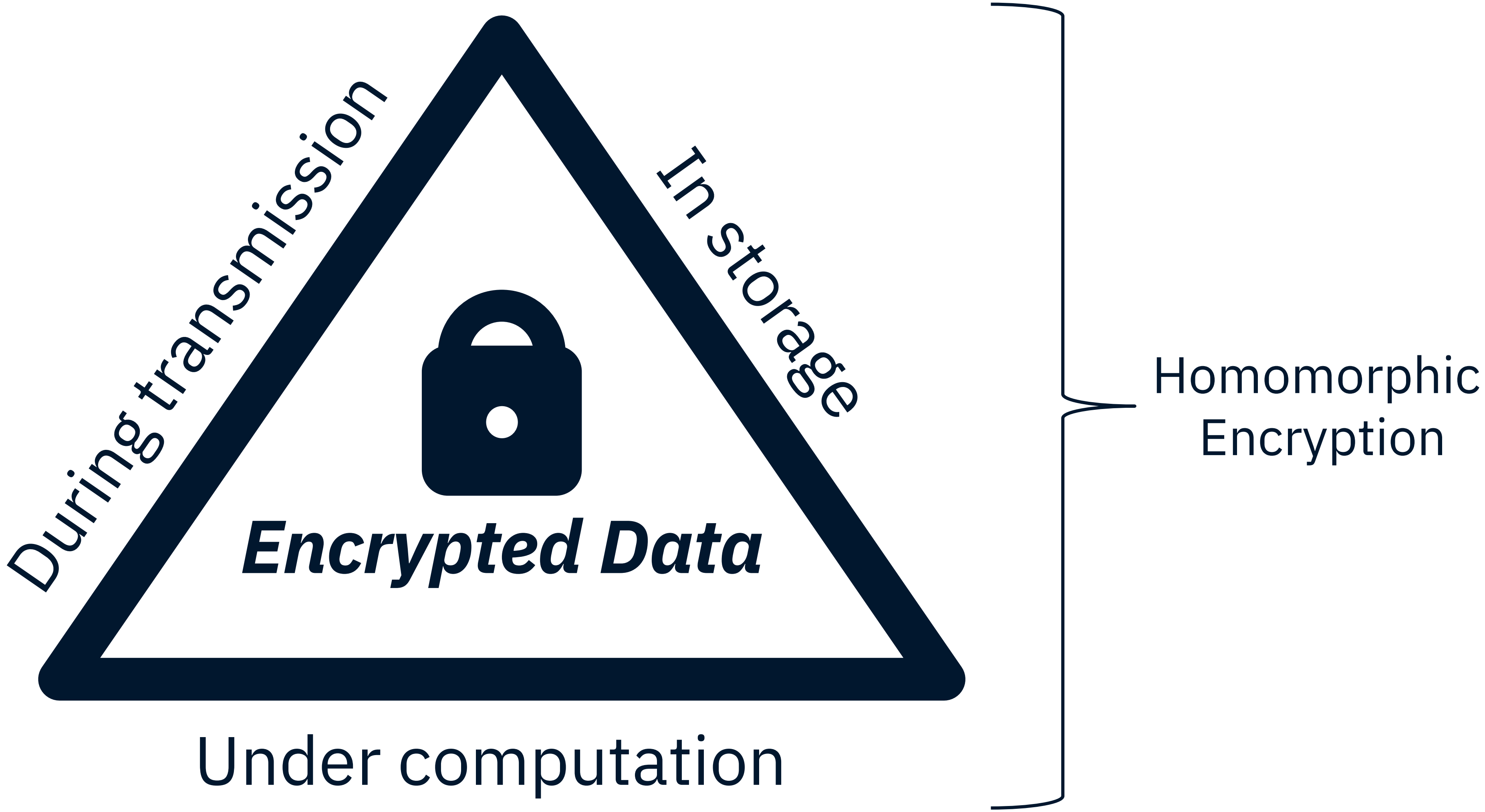


Shifting the Encryption Paradigm



Data needs to be decrypted at some point to do useful computation whether done internally or outsourced in a cloud

Full Lifecycle Protection with HE



During transmission

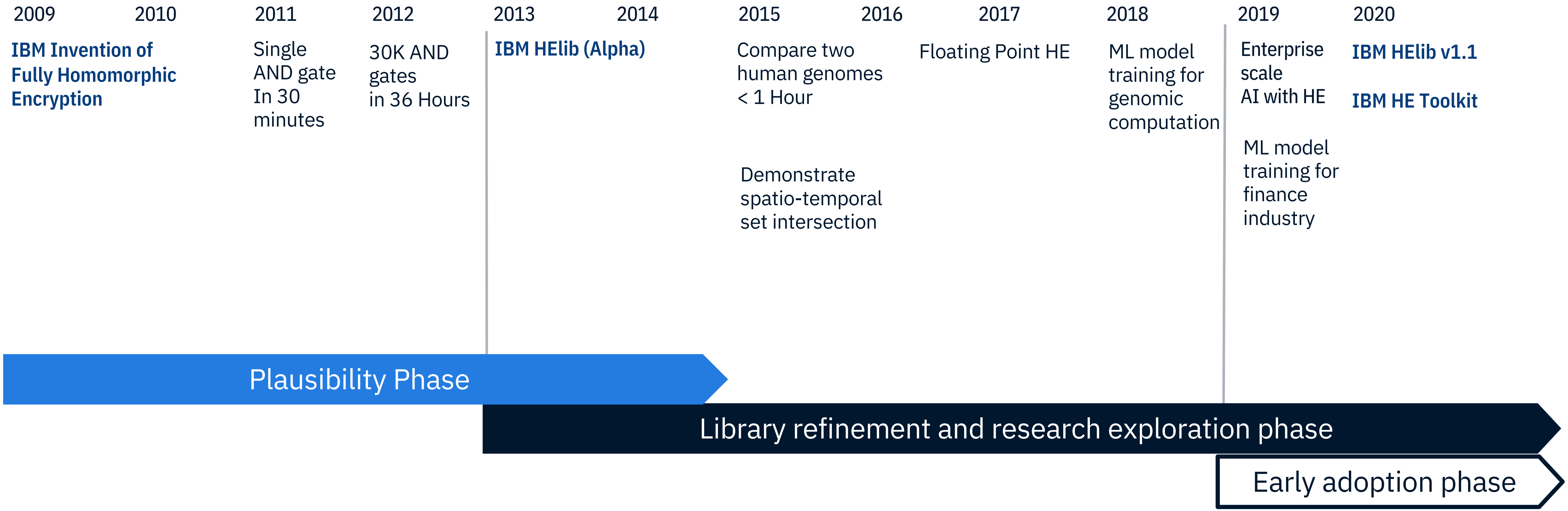
In storage

Encrypted Data

Under computation

Homomorphic Encryption

A brief history of Homomorphic Encryption



2009 2010

IBM Invention of Fully Homomorphic Encryption

2011

Single AND gate In 30 minutes

2012

30K AND gates in 36 Hours

2013 2014

IBM HElib (Alpha)

2015 2016

Compare two human genomes < 1 Hour

Demonstrate spatio-temporal set intersection

2017

Floating Point HE

2018

ML model training for genomic computation

2019

Enterprise scale AI with HE

ML model training for finance industry

2020

IBM HElib v1.1

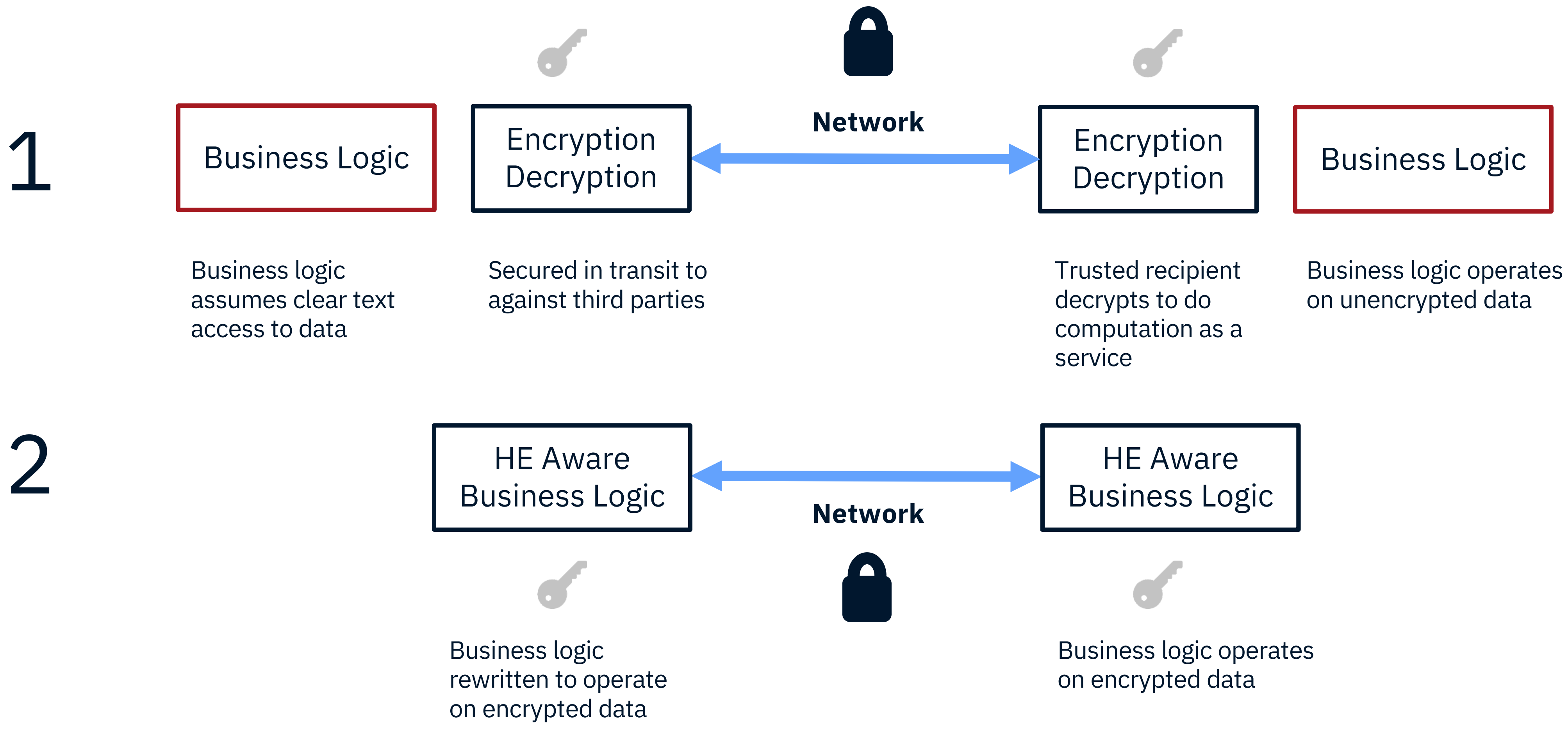
IBM HE Toolkit

Plausibility Phase

Library refinement and research exploration phase

Early adoption phase

Business Logic with HE



1

Business Logic

Business logic assumes clear text access to data

Encryption Decryption

Secured in transit to against third parties

Network

Encryption Decryption

Trusted recipient decrypts to do computation as a service

Business Logic

Business logic operates on unencrypted data

2

HE Aware Business Logic

Business logic rewritten to operate on encrypted data

Network

HE Aware Business Logic

Business logic operates on encrypted data

Use Case Archetypes

Oblivious Query
Search without revealing intent

Set Intersection
Determining overlap without disclosure

Extracting Value from Private Data
ML without revealing data or models

Secure Outsourcing & Insourcing
Enabling hybrid cloud adoption

IBM Homomorphic Encryption Toolkit

What platforms are supported?

Github source code or pre-built Docker container

- ✓ Linux (x86, s390x, Power*, multi-arch)
  - Ubuntu
  - CentOS
  - Fedora
  - Alpine
- ✓ z Container Extensions
- ✓ IBM Hyper Protect Virtual Servers
- ✓ MacOS / iOS

The IBM Homomorphic Encryption Toolkit enables a cutting-edge technology from IBM Research to demonstrate how we can solve real world business challenges

Toolkit is designed to ease adoption for enterprise developers through a docker runtime and native IDE Project files to get you started

10 Min

5 Demos

Demo

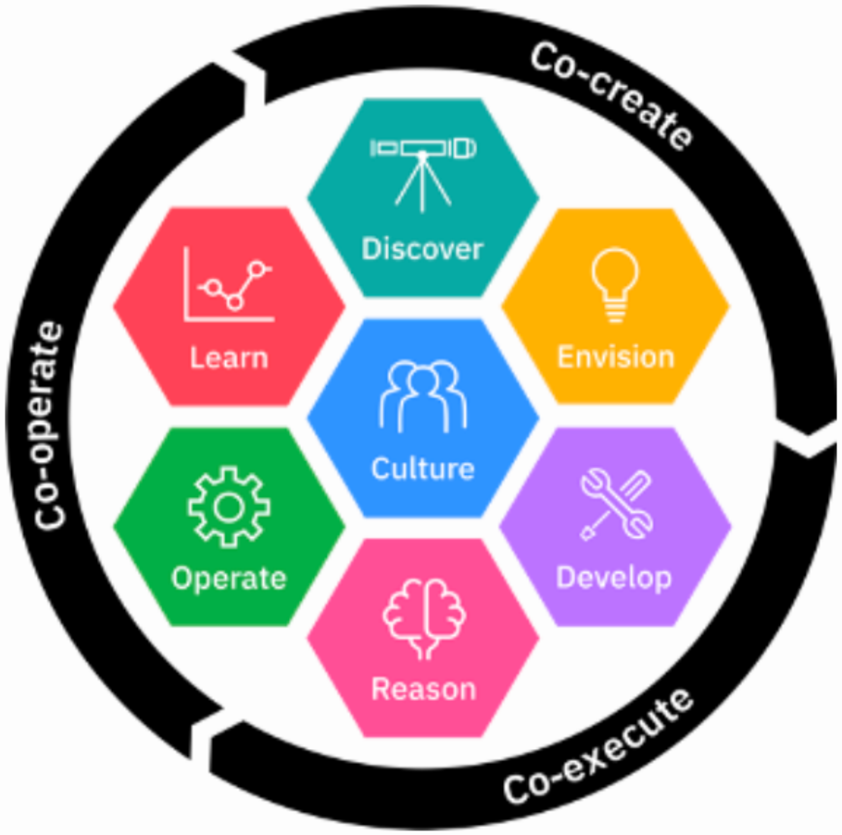
IBM Z Sponsor User Program

Sponsor Users are “clients” (customers, non-customers, business partners, end users, or organizations) who provide domain expertise to our team.

A Sponsor User Program is a formal agreement to derive insights from our users to inform our user experience, roadmap, and requirements. **The program is free of charge**, and only requires your time and active participation.

Our goal is to co-create and deliver world-class HE user experiences for our customers and foster rich innovation in the open source community.

Let’s design the user experience and build more secure software together.



Learn more

Read

IBM Developer Blog:
https://developer.ibm.com/blogs/new-open-source-security-tools-let-you-develop-on-encrypted-data/

Linux Announce Blog:
https://www.ibm.com/blogs/research/2020/07/homomorphic-encryption-comes-to-linux-on-ibm-z/

MacOS/iOS Announce Blog:
https://www.ibm.com/blogs/research/2020/06/ibm-releases-fully-homomorphic-encryption-toolkit-for-macos-and-ios-linux-and-android-coming-soon/

Ars Technica:
https://arstechnica.com/gadgets/2020/07/ibm-completes-successful-field-trials-on-fully-homomorphic-encryption

Participate

IBM FHE Experience:
https://fhe-website.eu-gb.mybluemix.net/

FHE Linux Toolkit Repo:
https://github.com/IBM/fhe-toolkit-linux/

IBM Advanced Security Survey:
https://www.surveygizmo.com/s3/5731822/Advanced-Security-And-Encryption-Survey-2020

Media

Terminal Talk Podcast:
https://www.terminaltalk.net/e/eli-dow-fully-homomorphic-encryption/

IBM YouTube:
https://www.youtube.com/playlist?list=PL0VD16H1q5IOEQuRdgRVt1M8uQSbpVzTb

AT&T YouTube:
https://www.youtube.com/watch?v=874w_J2aWUY

Connect

Eli M Dow
Senior Technical Staff Member
emdow@us.ibm.com

Rushir Patel
Offering Manager
rushir.patel@ibm.com

Thank you

Flavio Bergamaschi
Senior Research Scientist
—
flavio@uk.ibm.com

Eli Dow
Senior Technical Staff Member
—
emdow@us.ibm.com

Rushir Patel
Offering Manager
—
rushir.patel@ibm.com