Practical, Secure Computing through Fully Homomorphic Encryption

Kurt Rohloff
krohloff@duality.cloud

Redhat 2019
“Your previous provider refused to share your electronic medical records, but not to worry
—I was able to obtain all of your information online.”
Encryption?

A method to “hide” information.

Use cases:

- Hide information so it can be used later only by you.
  - Ex: protecting your legal files.

- Hide information except for an intended recipient.
  - Ex: send financial transaction requests to ONLY your broker.

Symmetric Encryption

Public-Key Encryption

Homomorphic Encryption

- Hide information so you can out-source processing.
  - Cloud computing with encrypted data!!
  - Ex: spam filtering e-mail without reading e-mail.
Fully Homomorphic Encryption

FHE Client

Data Source

Ppk
Public Encryption Key

Encrypted Data

Computation Host

Encrypted Result

Decrypted Result

Sk
Secret Decryption Key
Out-Sourced Computation??

- Until very recently, once data is encrypted, there was basically no way to manipulate it.
  - Minor exceptions, of course.

- Fully Homomorphic Encryption (FHE)
  - Give data to cloud provider you don’t need to trust.
  - Provider can perform arbitrary computations for you.

- Examples:
  - Send video to a contractor for facial recognition analysis, but don’t need contractor to “see” the video.
  - Securely store and query a large, sensitive DB “in the cloud.”
  - Outsourced spam filtering of encrypted e-mail.
FHE Is Now Possible

• Discovery of a possible scheme in 2009
  – Craig Gentry from Stanford/IBM
  – Most important CS breakthrough of 21st century.
  – Very different computation model.

• There have been additional theoretical improvements since then.

• Practical computation challenges…
  – Slow-down
  – Ciphertext expansion
  – Different compute model
Lattice-based encryption

- FHE schemes are lattice-based encryption schemes.

- Lattice schemes form a “new” family of encryption.
  - Built on lattice mathematics.
    - Lattices are integer vectors.
  - They are resistant to quantum computing attacks.
Lattice Encryption Intuition?

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

- Plaintext are integer vectors, modulus small p.
- Ciphertext are integer vectors modulus very large q.
Security?

• Key length is a heuristic for security provided.
  – It is effective for RSA, AES, etc…

• “Real” security is “work factor”
  – Amount of computational effort required to “crack” a key, ciphertext, etc…
Post-Quantum

• Quantum attacks:
  – Shor showed quantum algorithms for factoring.
  – Grover showed a quadratic speedup relative to search algorithms.

• Modern lattice encryption security proofs built on hardness of Shortest Vector Problem (SVP).
  – Best known quantum result is that we can provably find a shortest vector in time $2^{(C*n+o(n))}$.
  – Resistance to quantum attacks is still a conjecture.
    • Similar to conjecture that factoring is hard for classical computers.
**Computing on Encrypted Data**

**Messages**
- Lists of real numbers
- E-mails in ASCII text
- JPEG images

**Plaintext**
- Strings of mod \( p \) integer vectors
  - Examples:
    - \([1 0 0 0]\)
    - \([1 3 5 43 23]\)

**Ciphertext**
- Strings of mod \( q \) integer vectors
  - Examples:
    - \([311 231 3256 7697]\)
    - \([1673 3213 67354 323]\)

- **Message-Plaintext encodings** determined by translation of program into EvalAdd, EvalMult operations.
- **Coding** is an open research topic and drastically impacts effective runtime.

- **Plaintext-Ciphertext encryption/decryption** defined by FHE scheme.

- **Operations on ciphertexts**
Secure Programs with FHE

• Very different computation model.
• Base operations on ciphertext:

- Integer Addition mod p
- Integer Convolution mod p
- EvalAdd
- EvalMult

• Much of our innovations come from developing novel algorithms and data structures that are efficient for homomorphic computing model

• Conditional “if” statements on encrypted data not permitted.
Looking Forward

- **Software**
  - Smaller, Faster, Better!

- **Hardware**
  - Fit everything on board.

- **Applications/Demos**
  - Secure string searching (aka simple spam filtering) over encrypted ciphertext.

- **Transition & Broader Adoption**
“Your previous provider refused to share your electronic medical records, but not to worry
—I was able to obtain all of your information online.”
Questions?

Kurt Rohloff
krohloff@duality.cloud