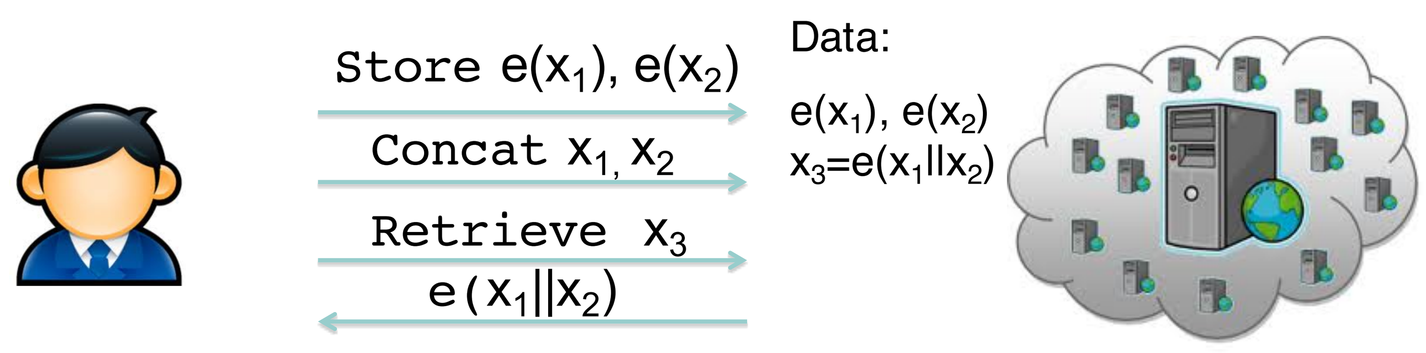
Development and Evaluation of Next Generation Homomorphic Encryption Schemes

Hoffstein J., Silverman J.
Brown University

Sunar B.
Worcester Polytechnic Institute

Fully Homomorphic Encryption (FHE)



- Allows computation over encrypted data without the secret key.
- Distributed applications where sensitive data is protected: Semi-trusted cloud servers.
- Any function can be evaluated using homomorphic primitives.

Objective

Investigate and develop next generation HE schemes with no heavy computation or evaluation keys.

- First Generation(previous schemes):
  - Large evaluation keys (in Gigabytes)
  - Costly multiplicative operations
  - Fast noise growth with multiplications
- Second Generation (GSW[1], FHEW[2], F-NTRU[3]):
  - No evaluation keys, no relinearization
  - Large parameter sizes for security
- Next Generation (FF-Encrypt):
  - No evaluation keys, fast evaluations
  - Affordable parameter sizes

FF-Encrypt

Proposed by the PIs; based on the difficulty of recovering an unknown isomorphism between finite fields; multiplicative evaluations without costly operations; adequate security with much smaller parameter sizes.

Three Modules of The Project

- Theoretical foundation of FF-Encrypt:

  security analysis, selection of parameters, noise mitigation techniques;
- Comparison with existing schemes, scalability of the scheme, optimized software libraries;
- A test drive of the schemes, applications in semi-trusted cloud servers.

FF-Encrypt Scheme

- Create irreducible polynomials
  $$\boldsymbol{f}(x) \in \mathbb{F}_q[x] \text{ and } \mathbf{h}(y) \in \mathbb{F}_q[y]$$
- Fix isomorphism
  $$\phi(\psi(x)) \equiv x \bmod \boldsymbol{f}(x)$$
  $$\psi(\phi(y)) \equiv y \bmod \boldsymbol{h}(x)$$
- Isomorphism
  $$\frac{\mathbb{F}_q[x]}{(\boldsymbol{f}(x))} \longrightarrow \frac{\mathbb{F}_q[y]}{(\boldsymbol{h}(y))}$$
  $$\boldsymbol{m}(x) \bmod \boldsymbol{f}(x) \longmapsto \boldsymbol{m}(\phi(y)) \bmod \boldsymbol{h}(y)$$
- Inverse-Isomorphism
  $$\frac{\mathbb{F}_q[y]}{(\boldsymbol{h}(y))} \longrightarrow \frac{\mathbb{F}_q[x]}{(\boldsymbol{f}(x))}$$
  $$\boldsymbol{c}(y) \bmod \boldsymbol{h}(y) \longmapsto \boldsymbol{c}(\psi(y)) \bmod \boldsymbol{f}(x)$$
- Underlying hard problem: secret isomorphism between finite fields
- Lattice attacks alone appear to be insufficient to locate a secret field isomorphism and break scheme

- Encryption
  - fix $\boldsymbol{p}(x) \in \mathbb{F}_q[x]$ with small coefficients
  - randomly sample:
    $\boldsymbol{r}(x) \in \mathbb{F}_q[x]$ with small coefficients
  - compute
    $$\boldsymbol{e}(x) = \boldsymbol{p}(x)\boldsymbol{r}(x) + \boldsymbol{m}(x) \pmod{\boldsymbol{f}(x)}$$
    $$\boldsymbol{c}(y) = \boldsymbol{e}(\phi(y)) \pmod{\boldsymbol{h}(y)} \in \mathbb{F}_q[y]/(\boldsymbol{h}(y))$$
- Decryption
  - compute
    $$\begin{aligned}\boldsymbol{a}(x) &\equiv \boldsymbol{c}(\psi(x)) \pmod{\boldsymbol{f}(x)}\\ &\equiv \boldsymbol{p}(x)\boldsymbol{r}\left(\phi(\psi(x))\right) + \boldsymbol{m}\left(\phi(\psi(x))\right) \pmod{\boldsymbol{f}(x)}\\ &\equiv \boldsymbol{p}(x)\boldsymbol{r}(x) + \boldsymbol{m}(x) \pmod{\boldsymbol{f}(x)}\end{aligned}$$
- Noise Mitigation Techniques
  - modulus switching [4]
  - ciphertext Flattening [1]
- Move FF-Encrypt from a leveled to a bootstrapped FHE

Bibliography

1. Gentry, C., Sahai, A., Waters, B.: Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based. In: CRYPTO. pp. 75–92. Springer (2013).
2. Ducas, L., Micciancio, D.: FHEW: Bootstrapping homomorphic encryption in less than a second. In: Advances in Cryptology–EUROCRYPT 2015, pp. 617–640. Springer (2015).
3. Doroz, Y., Sunar, B.: Flattening NTRU for evaluation key free homomorphic encryption. Cryptology ePrint Archive. Report 2016/315. http://eprint.iacr.org/2016/315 (2016).
4. Brakerski, Z., Vaikuntanathan, V.: Efficient fully homomorphic encryption from (standard) LWE. In: Ostrovsky, R. (ed.) FOCS. pp. 97–106. IEEE (2011).

Interested in meeting the PIs? Attach post-it note below!

The 3rd NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
January 9-11, 2017
Arlington, Virginia