Development and Evaluation of Next Generation Homomorphic Encryption Schemes

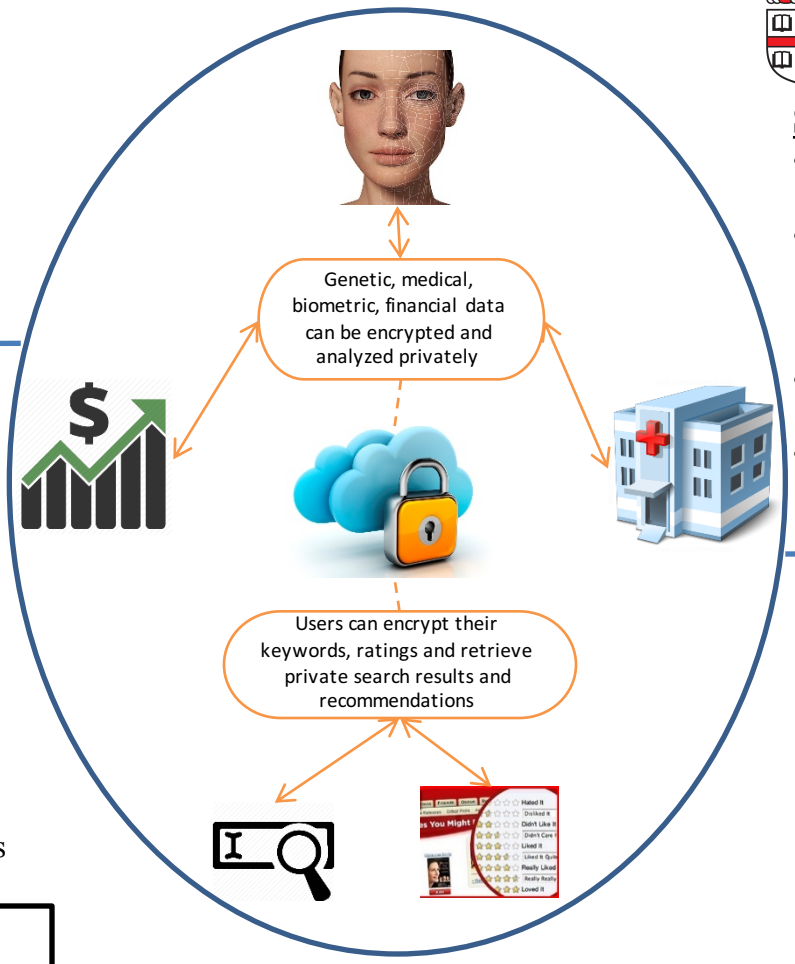
Hoffstein J., Silverman J. , Sunar B.

Challenge:

- Making homomorphic encryption (HE) both secure and efficient.
- Protect FF-Encrypt against existing and potential attacks.
- Mitigate the noise growth.
- Turn FF-Encrypt into a leveled and a bootstrapped FHE.
- Efficiently implement FF-Encrypt for many applications.

Solution:

- Determine optimal parameter sizes and retain desired attack lattice dimension, for both public and symmetric key FF-Encrypt.
- Rejection sampling in encryption.
- Precisely establish the noise growth relative to circuit depth, in order to tailor the parameters.
- Investigate noise mitigation techniques, such as modulus switching, ciphertext flattening, and bootstrapping algorithms.
- Develop optimized software libraries for CUDA-enabled GPUs.



BROWN WPI

Scientific Impact:

- Improve the balance between security and efficiency.
- Tackle challenges that will potentially guide future theoretic research and hardware/software designs in many fields.
- Investigate HE schemes based on the hidden isomorphism problem.
- Better understand the interplay between the public and symmetric key schemes in private computing.

Broader Impact:

- Transform the way sensitive data is shared and computed in an insecure environment.
- Advance may other sub-disciplines.
- Provide more insight on relationships between the security level, performance and circuit depth in FHE schemes.
- Include lessons learned from this project in course materials.
- Mentor graduate research assistants.
- Plan to organize a workshop.

Award Number: #1561536

PI: Jeffrey Hoffstein

Mahtematics Department, Brown University,

Box 1917, 151 Thayer Street, Providence, RI 02912

Phone: (401)863-1127 Fax: (401)863-9013