Homomorphic Encryption for Cloud Privacy

Berk Sunar, ECE WPI

Supported by NSF CNS Award #1117590

crypto.wpi.edu

Cloud: Great Idea with Great Challenge

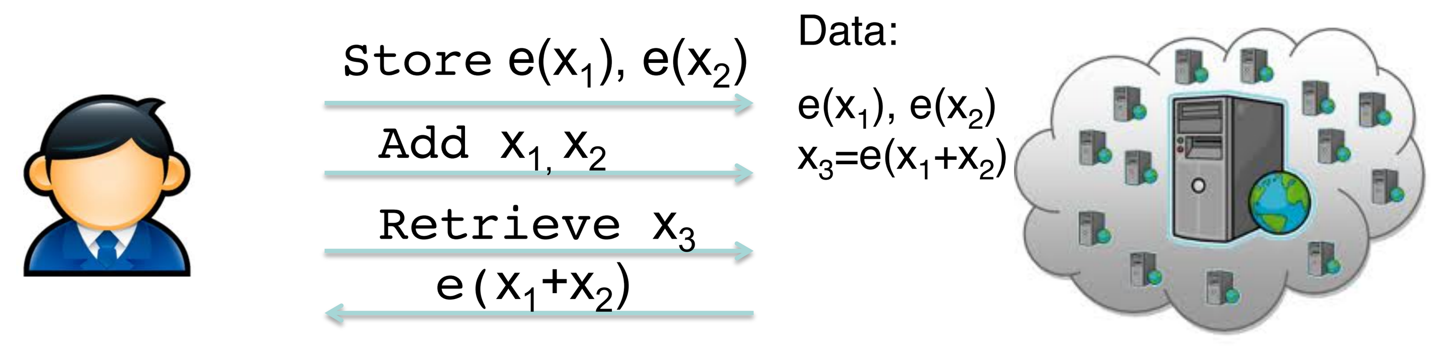
Low costs of the cloud will eventually push data to the server-side

Side-effect: to process a document you need to download it first

Bandwidth(=$) and latency problems

Solution: Perform transactions directly on encrypted data on server

Retrieve data only when user needs to access it



Extending Partial HE Schemes

Extends additive homomorphic schemes to handle arbitrary number of AND's/OR's

$f(x_0,x_1,x_2,x_3) = (x_0 \text{ XOR } x_2') \text{ AND } (x_0' \text{ XOR } x_3 \text{ XOR } x_1') \text{ AND} \ldots$

$f(x_0,x_1,x_2,x_3) = (x_1 \text{ XOR } x_2' \text{XOR } x_3') \text{ OR } (x_3 \text{ XOR } x_1) \text{ OR} \ldots$

Can be used to detect matches in large (conditional) queries

- Subtraction (Paillier) can be used to generate the initial x_i values

Probabilistic: there is a tiny failure probability ~ 2^{-w}

Bandwidth:

- Packing trick is used to reduce bandwidth
- Ciphertext size remains constant!
- E.g. using Paillier each input is mapped to ~4,096 bits

[1] Yin Hu, William J. Martin and Berk Sunar, *Homomorphically Evaluating n-DNF Formula*. Draft, 2012.

Eliminating Size Limitation on Additive Schemes

The Boneh-Goh-Nissim (2006) scheme allows efficient evaluation of 2-DNF equations, e.g.

$f(x_0,x_1,x_2,x_3,x_4) = (x_0+x_2)\bullet(x_1+x_2+x_3) + (x_1+x_2)\bullet(x_1+x_4') + \ldots$

Useful for vector comparison/determining number of matches, i.e.

$f(x,y) = \Sigma x_i y_j$

Mul:10 ms, Add: <1 ms, Decrypt: DLP in finite field ☹

Final step requires DLP; output must be small for decryption to work

- Solved using CRT trick (Hu, Sunar, Martin. ACNS 2012)

[1] Yin Hu, William J. Martin and Berk Sunar, *Enhanced Flexibility for Homomorphic Encryption Schemes via CRT*. Industrial Track, ACNS 2012.

Reducing FHE bandwidth by Scheme Conversion

FHE schemes huge message expansion

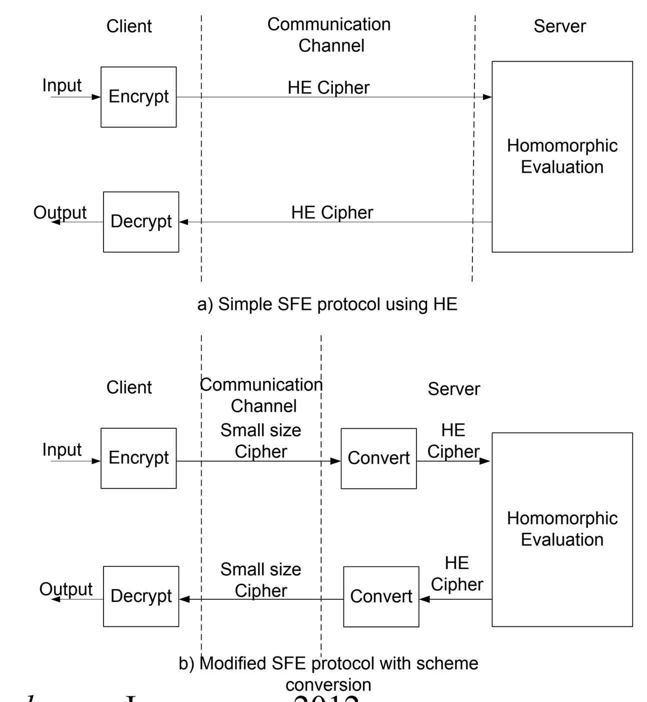
- E.g. the GH-FHE scheme encrypts a single bit into a million-bit ciphertext.

Partial HE and symmetric schemes have shorter ciphertexts

- E.g. the Paillier requires ~4,096 bits and stream ciphers only need 1 bit.
- But, are not fully homomorphic.

The Solution: Scheme Conversion

- FHE for computation
- Others for communication



[1] Yin Hu and Berk Sunar, *Reducing the bandwidth of FHE schemes.* In progress, 2012.

Implementing the Gentry-Halevi FHE

Computations in GH-FHE primitives requires costly modular additions and multiplications. Optimizations

- FFT based multiplication algorithms
- GPUs and hardware for better parallelism.
- Delayed modular reductions to reduce the number modular reductions and IFFT computations.

Software Implementation with GPUs

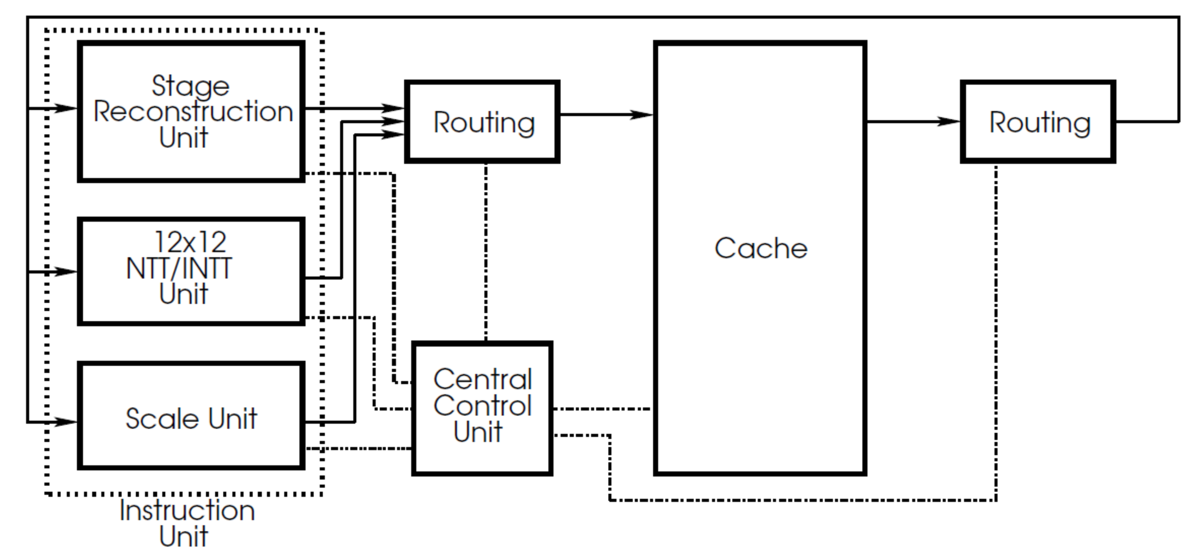
	CPU Gentry & Halevi	GPU Our impl.	Speedup
Platform	Intel Core i7 3770K running at 3.5 GHz with 8 GB RAM Build with NTL/GMP	NVIDIA GTX 690, 3072 CUDA cores, 1.02 GHz, 4GB GDDR5* memory	
Encryption	1.08 sec	6.2 ms	x174
Decryption	14 ms	1.84 ms	x8
Recryption	17.8 sec	1.3 sec	x14

[1] Wei Wang, Yin Hu, Lianmu Chen, Xinming Huang and Berk Sunar, *Accelerating Fully Homomorphic Encryption Using GPU*, Proceedings of 2012 IEEE High Performance Extreme Computing Conference – HPEC' 12, 2012.

[2] Wei Wang, Yin Hu, Lianmu Chen, Xinming Huang and Berk Sunar, *Exploring the Feasibility of Fully Homomorphic Encryption through GPU Acceleration*, Draft, 2012.

Hardware Implementation

Our current implementation focuses on low-cost and small-footprint. However, the architecture is flexible and the operations can be speedup further by using more hardware resources for computations and higher bandwidth for data transactions.



- The Million-bit multiplier is crucial for every operation
- Encryption, Decryption and Recryption uses the same multiplier

[1] Yarkin Doroz, Erdinc Ozturk and Berk Sunar, *An Efficient Architecture for Million-bit Multiplication.*. Submitted to Arith 2012, 2012.

	Time	Area (Gates)
Multiplication	7.74 ms	25.20 Million
Encryption	31.09 ms	0.206 Million + Multiplier
Decryption	23.22 ms	1000 + Multiplier
Recryption*	~10 sec	~2 Million + Multiplier

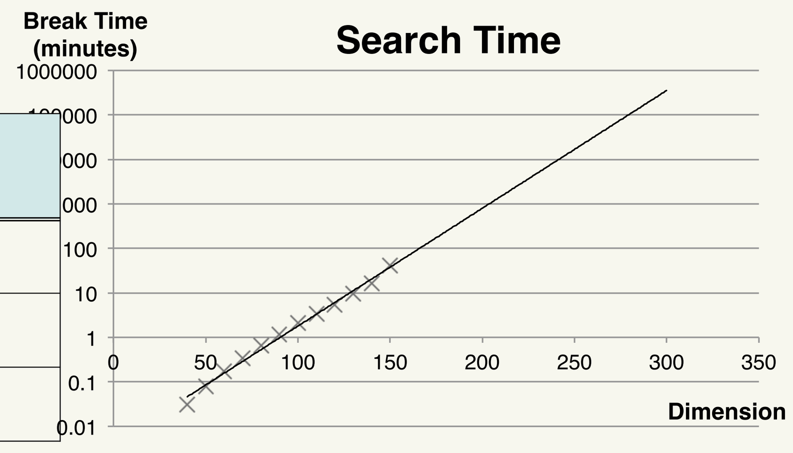
[*] Preliminary results

Implementing the NTRU-Based Multikey FHE scheme

The multikey FHE by Lopez-Alt, Tromer and Vaikuntanathan offers better possibilities. However, concrete parameters are lacking.

Using NTL/LLL we evaluated the time required to break the scheme for various parameter choices.

Dimension	Estimated Break Time
256	17 days
384	117 years
512	280,657 years



Preliminary CPU implementation for N=512, |q| =256 bit, B = 4

We expect significant speedup with further optimizations on GPUs

KeyGen	0.84 sec
Encryption	1.08 ms
Multiplication	1.5 ms
Switch Keys	0.52 sec
Decryption	2.3 ms

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

National Science Foundation
WHERE DISCOVERIES BEGIN

NSF Secure and Trustworthy Cyberspace Inaugural Principal Investigator Meeting
Nov. 27 -29th 2012
National Harbor, MD

WPI