A Working Implementation of Fully Homomorphic Encryption

Craig Gentry, Shai Halevi

IBM T.J. Watson Research Center

Implemented a Variant of [G'09]

- Somewhat Similar to [Smart-Vercauteren'10]
- Initially planned to use IBM's Blue-Gene, ended up not needing it
  - Implementation using NTL/GMP
  - Timing on a “strong” 1-CPU machine

- Xeon E5440 / 2.83 GHz (64-bit, quad-core)
- 24 GB memory

- Generated/tested instances in 4 dimensions:
  - Toy (2^9), Small (2^{11}), Medium (2^{13}), Large (2^{15})
- Assuming exponential hardness of SVP / BDD
  - Different dim's ↔ different const's in the exponent

Underlying “Somewhat HE”

- PK: two integers, SK: one integer

Dimension	KeyGen	Enc (amortized)	Dec	degree
512 200,000-bit integers	0.16 sec	4 millisec	4 millisec	~200
2048 800,000-bit integers	1.25 sec	60 millisec	23 millisec	~200
8192 3,200,000-bit integers	10 sec	0.7 sec	0.12 sec	~200
32768 13,000,000-bit integers	95 sec	5.3 sec	0.6 sec	~200

Fully-Homomorphic Scheme

- Re-Crypt polynomial of degree 15

Dimension	KeyGen	PK size	Re-Crypt
512	2.4 sec	17 MByte	6 sec
2048	40 sec	70 MByte	31 sec
8192	8 min	285 MByte	3 min
32768	2 hours	2.3 GByte	30 min

We Plan to have Challenges Ready in Time for CRYPTO