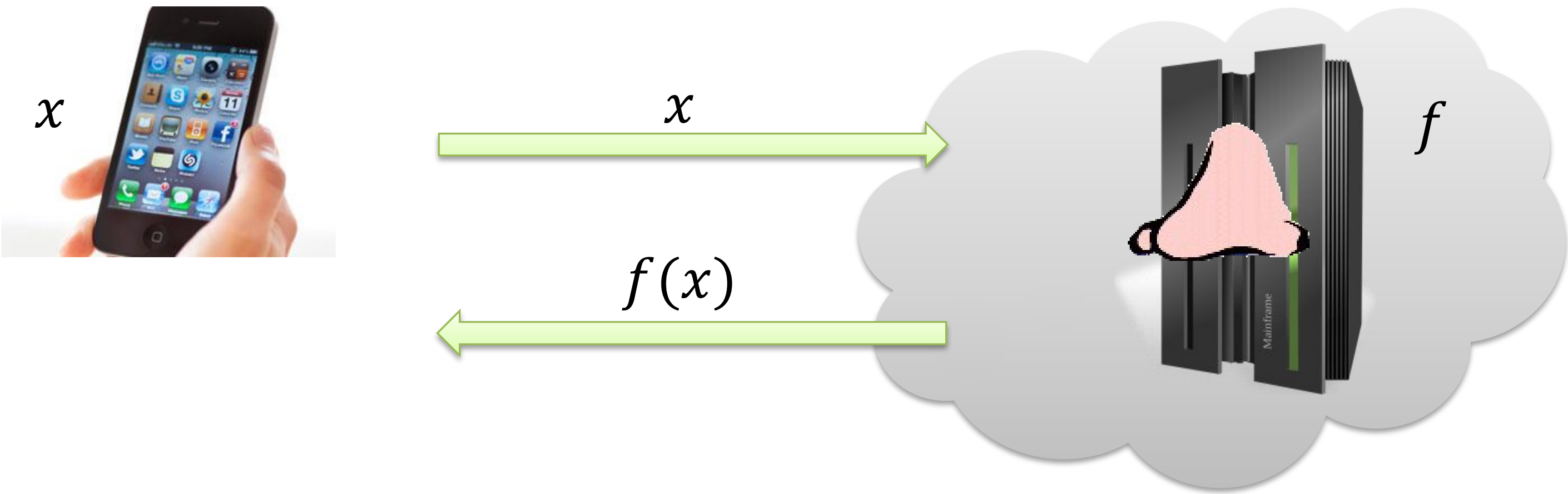
Fully Homomorphic Encryption without Modulus Switching from Classical GapSVP

Zvika Brakerski

Stanford University

CRYPTO 2012

Outsourcing Computation



Email, web-search, navigation, social networking…

Search query, location, business information, medical information…

What if x is private?

Outsourcing Computation – Privately

x

$Enc(x)$

y

$Dec(y) = f(x)$

Learns nothing on x.

f

Homomorphic Encryption

$$f, Enc(x_1), \dots, Enc(x_n) \rightarrow Enc(f(x_1, \dots, x_n))$$

We assume w.l.o.g $f \in \{+, \times\}$ (over $\mathbb{Z}_2$).

The Old Days of FHE
2009-2011

- Gentry's breakthrough [G09,G10] – first candidate.

- [vDGHV10, BV11a]: Similar outline, different assumptions.
- [GH11]: Chimeric-FHE.

- Efficiency attempts [SV10,SS10,GH10,LNV11].

2^{nd} Generation FHE

- [BV11b]: LWE-based FHE (= apx. short vector in lattice).
  - Better assumption.
  - Clean presentation: no ideals, no "squashing".
  - Efficiency improvement.

- [BGV12]: Improved performance via Modulus Switching.
  - Quantitatively better assumption.
  - "Leveled" homomorphism without bootstrapping.
  - Efficiency improvements using ideals ("batching").

[GHS11,GHS12a, GHS12b]: Efficiency improvements and optimizations using ideals.

This work:

Modulus switching is a red herring

"Scale-independent encryption"

⇒ better performance with less headache

FHE 101 [BV11b]

Security based on $LWE_{n,q,\alpha}$

The Scheme:

Secret key: $\vec{s} \in \mathbb{Z}_q^n$

Ciphertext: $\vec{c} \in \mathbb{Z}_q^n$

$$\vec{c} \cdot \vec{s} = m + 2e + qI \quad {}^{\in \mathbb{Z}}$$

small (initial) noise $|e| < B = \alpha q$

dec. if $|e|/q < \frac{1}{4}$

Encryption algorithm: Doesn't matter.

Decryption algorithm: $\left(\vec{c} \cdot \vec{s} \ \ (mod\ q)\right)\ (mod\ 2)$.

FHE 101 [BV11b]

The Scheme:

Secret key: $\vec{s} \in \mathbb{Z}_q^n$

Ciphertext: $\vec{c} \in \mathbb{Z}_q^n$

$$\vec{c} \cdot \vec{s} = m + 2e + qI \quad {\in \mathbb{Z}}$$

small (initial) noise $|e| < B = \alpha q$

dec. if $|e|/q < \frac{1}{4}$

Additive Homomorphism:

That again? Just add'em, dude…

$$\vec{c}_1, \vec{c}_2 \Rightarrow \vec{c}_1 + \vec{c}_2 \ (mod\ q)$$

FHE 101 [BV11b]

The Scheme:

Secret key: $\vec{s} \in \mathbb{Z}_q^n$

Ciphertext: $\vec{c} \in \mathbb{Z}_q^n$

$$\vec{c} \cdot \vec{s} = m + 2e + qI \quad {\scriptstyle \in \mathbb{Z}}$$

small (initial) noise $|e| < B = \alpha q$

dec. if $|e|/q < \frac{1}{4}$

Multiplicative Homomorphism:

sk changed…

but we can bring it back

(we have the technology)

$\vec{c}_2$ $(mod$

l cross term

noise blows up!

$$\boldsymbol{B \to B^2 \to \cdots \to B^{2^d}}$$

dec. if $B^{2^d}/q < \frac{1}{4}$

$$(\vec{c}_1 \otimes \vec{c}_2) \cdot (\vec{s} \otimes \vec{s}) = (\vec{c}_1 \cdot \vec{s}) \cdot (\vec{c}_2 \cdot \vec{s}) = (m_1 + 2e_1) \cdot (m_2 + 2e_2) \ (mod\ q)$$

$$= m_1 m_2 + 2 \cdot \underbrace{O(e_1 e_2)}_{\sim B^2} \ (mod\ q)$$

Modulus Switching [BGV12]

Idea: Bring noise back down by dividing the entire ciphertext by B.

$\vec{c} \in \mathbb{Z}_q^n$ with noise $|e| < B^2$ $\xrightarrow{/B}$ $\lfloor \vec{c}\,/B \rceil \in \mathbb{Z}_{q/B}^n$ with noise $|e| < B$

(make sure not to harm the message bit m)

Noise/modulus evolution:

$$(\boldsymbol{B}, \boldsymbol{q}) \rightarrow (\boldsymbol{B}, \boldsymbol{q}/\boldsymbol{B}) \rightarrow \cdots \rightarrow (\boldsymbol{B}, \boldsymbol{q}/\boldsymbol{B}^{\boldsymbol{d}})$$

dec. if $B^{d+1} < q/4$

My Problems with Modulus Switching

1. Modulus switching is scale-dependent.
   - Scaling B, q changes performance:

     Smaller $B, q \Rightarrow$ smaller $B^{d+1}/q \Rightarrow$ better homomorphism.

2. What does modulus switching really do?

   ← nothing...

   - Same as a scaling factor in the tensoring process ($\vec{c}_1, \vec{c}_2 \ \Rightarrow \ \tau \cdot \vec{c}_1 \otimes \vec{c}_2 \ (mod\ q)$).
   - In a “correct” scale, this factor should be 1.

Our Solution: Scale-Independent FHE

Secret key: $\vec{s} \in \mathbb{Z}^n$

Ciphertext: $\vec{c} \in \mathbb{R}_2^n$

real numbers $mod\ 2 \equiv (-1,1]$

$\vec{c} \cdot \vec{s} = m + \epsilon + 2I$ $\in \mathbb{Z}$

small (initial) noise $|\epsilon| < 2\alpha$

dec. if $|\epsilon| < \frac{1}{2}$

Divide original ciphertext by $q/2$

Compare with previous:

Secret key: $\vec{s} \in \mathbb{Z}_q^n$

Ciphertext: $\vec{c} \in \mathbb{Z}_q^n$

$\vec{c} \cdot \vec{s} = m + 2e + qI$ $\in \mathbb{Z}$

small (initial) noise $|e| < B = \alpha q$

dec. if $|e|/q < \frac{1}{4}$

Hardness assumption is the same $LWE_{n,q,\alpha}$.

Scale-Independent Multiplication

$|m + 2I| \approx |\vec{c} \cdot \vec{s}| \leq \|\vec{s}\|_1$

Secret key: $\vec{s} \in \mathbb{Z}^n$

Ciphertext: $\vec{c} \in \mathbb{R}_2^n$

real numbers $mod\ 2 \equiv (-1,1]$

$\vec{c} \cdot \vec{s} = m + \epsilon + 2I$ ($\in \mathbb{Z}$)

small (initial) noise $|\epsilon| < 2\alpha$

dec. if $|\epsilon| < \frac{1}{2}$

Multiplicative Homomorphism:

$\vec{c}_1, \vec{c}_2 \Rightarrow \vec{c}_1 \otimes \vec{c}$

Careful!

$mod\ 2)) \neq 1\ (mod\ 2)$

$(\vec{c}_1 \otimes \vec{c}_2) \cdot (\vec{s} \otimes \vec{s}$

Noise blowup: $\boldsymbol{\alpha} \rightarrow \boldsymbol{\alpha} \cdot \|\vec{\boldsymbol{s}}\|_1$

$= (m_1 + \epsilon_1 + 2I_1) \cdot (m_2 + \epsilon_2 + 2I_2) \quad (mod\ 2)$

$= m_1 m_2 + \epsilon_1 \cdot (m_2 + 2I_2) + \epsilon_2 \cdot (m_1 + 2I_1) + \epsilon_1 \epsilon_2 \quad (mod\ 2)$

$\sim\alpha \cdot |m + 2I| \lesssim \alpha \cdot \|\vec{s}\|_1$

$\sim\alpha^2$ = tiny!

Scale-Independent Multiplication

Secret key: $\vec{s} \in \mathbb{Z}^n$

Ciphertext: $\vec{c} \in \underbrace{\mathbb{R}_2^n}$

real numbers $mod\ 2 \equiv (-1,1]$

$\vec{c} \cdot \vec{s} = m + \epsilon + 2I$ $\quad \in \mathbb{Z}$

small (initial) noise $|\epsilon| < 2\alpha$

dec. if $|\epsilon| < \frac{1}{2}$

Multiplicative Homomorphism:

$$\vec{c}_1, \vec{c}_2 \;\Rightarrow\; \vec{c}_1 \otimes \vec{c}_2 \ (mod\ 2) \in \mathbb{R}_2^{n^2}$$

Noise blowup: $\boldsymbol{\alpha \to \alpha \cdot ||\vec{s}||_1}$

Not good enough: $||\vec{s}||_1 \approx nq$

Solution: Decompose the elements of $\vec{s}$ into $n \log q$ bits.

Binary Decomposition

$$\vec{s} = (s[1], s[2], \dots)$$

$$\vec{c} = (c[1], c[2], \dots)$$

$$\vec{s} \cdot \vec{c} = s[1] \cdot c[1] + s[2] \cdot c[2] + \cdots$$

$$\vec{s} = \left(s[1]_0, \dots, s[1]_{\log q}, s[2]_0, \dots, s[2]_{\log q}, \dots\right)$$

$$\vec{c} = \left(c[1], 2c[1], \dots, 2^{\log q} c[1], c[2], 2c[2], \dots, 2^{\log q} c[2], \dots\right)$$

$$\vec{s} \cdot \vec{c} = \textstyle\sum_i s[1]_i \cdot 2^i c[1] + \sum_i s[2]_i \cdot 2^i c[2] + \cdots$$

$$= s[1] \cdot c[1] + s[2] \cdot c[2] + \cdots$$

Scale-Independent Multiplication

$\|\vec{s}\|_1 \le n \log q$

Secret key: $\vec{s} \in \{0,1\}^{n \log q}$

Ciphertext: $\vec{c} \in \mathbb{R}_2^{n \log q}$

real numbers $mod\ 2 \equiv (-1,1]$

$\vec{c} \cdot \vec{s} = m + \epsilon + 2I$ $\in \mathbb{Z}$

small (initial) noise $|\epsilon| < 2\alpha$

dec. if $|\epsilon| < \frac{1}{2}$

Multiplicative Homomorphism:

$$\vec{c}_1, \vec{c}_2 \Rightarrow \vec{c}_1 \otimes \vec{c}_2 \ (mod\ 2) \in \mathbb{R}_2^{n^2}$$

Noise blowup: $\boldsymbol{\alpha \to \alpha \cdot (n \log q) \le \alpha \cdot n^2}$

For depth d circuit: $\alpha \to \alpha \cdot n^{O(d)}$
regardless of scale!

Full Homomorphism via Bootstrapping

Evaluating depth d circuit: $\boldsymbol{\alpha \to \alpha \cdot n^{O(d)}}$

For “bootstrapping”: $d = O(\log n) \Rightarrow$ $\boldsymbol{\alpha \to \alpha \cdot n^{O(\log n)}}$

$\Rightarrow$ dec. if $\boldsymbol{\alpha \approx n^{-O(\log n)}}$ regardless of q!

(in [BGV12] only for “small” odd q)

Using $q \approx 2^n \Rightarrow$ Hardness based on classical GapSVP.

Conclusion

- Scale-independence $\Rightarrow$ FHE without modulus switching.
- Homomorphic properties independent of q.
  - But q still matters for security.

- Properties of [BGV12] extend.
- Bonuses:
  - Our q can be even (e.g. power of 2).
  - Security based on classical GapSVP (as opposed to quantum).
- Simpler!

also see blog post with Boaz Barak:

tiny.cc/fheblog1 ; tiny.cc/fheblog2

Farewell CRYPTO '12…

blog post with Boaz Barak:

tiny.cc/fheblog1 ; tiny.cc/fheblog2