Faster Fully Homomorphic Encryption

Damien Stehlé
Joint work with Ron Steinfeld

CNRS – ENS de Lyon / Macquarie University

Singapore, December 2010

Main result

Improved bit-complexity bound for homomorphically evaluating a binary gate with Gentry's fully homomorphic scheme:

$\widetilde{\mathcal{O}}(t^6) \longrightarrow \widetilde{\mathcal{O}}(t^{3.5})$ bit operations, with t =security parameter.

To compare with: standard RSA Enc/Dec costs $\widetilde{\mathcal{O}}(t^3)$ per bit.

Two ingredients:

- A less pessimistic analysis of one of the hardness assumptions.
- An improved decryption algorithm.

Main result

Improved bit-complexity bound for homomorphically evaluating a binary gate with Gentry's fully homomorphic scheme:

$\widetilde{\mathcal{O}}(t^6) \longrightarrow \widetilde{\mathcal{O}}(t^{3.5})$ bit operations, with t =security parameter.

To compare with: standard RSA Enc/Dec costs $\widetilde{\mathcal{O}}(t^3)$ per bit.

Two ingredients:

- A less pessimistic analysis of one of the hardness assumptions.
- An improved decryption algorithm.

Main result

Improved bit-complexity bound for homomorphically evaluating a binary gate with Gentry's fully homomorphic scheme:

$$\widetilde{\mathcal{O}}(t^6) \longrightarrow \widetilde{\mathcal{O}}(t^{3.5}) \text{ bit operations, with } t = \text{security parameter.}$$

To compare with: standard RSA Enc/Dec costs $\widetilde{\mathcal{O}}(t^3)$ per bit.

Two ingredients:

- A less pessimistic analysis of one of the hardness assumptions.
- An improved decryption algorithm.

1. **Reminders on homomorphic encryption.**
2. Ingredient 1: a less pessimistic analysis of S(V)SSP.
3. Ingredient 2: a shallower decryption algorithm.

Ideal lattices

Let n be a power of 2 and $R = \mathbb{Z}[x]/(x^n + 1)$.

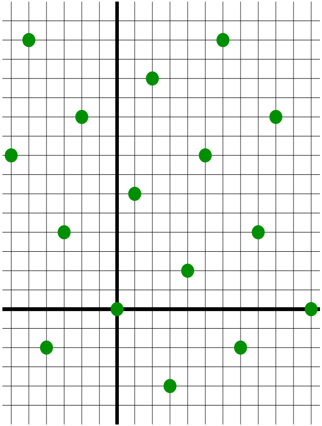
- $J \subseteq R$ is an ideal if $\forall a, b \in J, \forall r \in R : \quad a + b \cdot r \in J$.
- Any ideal is a lattice, i.e., an additive subgroup of $\mathbb{Z}^n$.

Basis: $(\mathbf{b}_i)_{i \leq n}$ linearly independent s.t.

$$L = \{\sum_{i \leq n} x_i \mathbf{b}_i : x_i \in \mathbb{Z}\}$$

Minimum: $\lambda = \min(\|\mathbf{b}\| : \mathbf{b} \in L \setminus \mathbf{0})$.

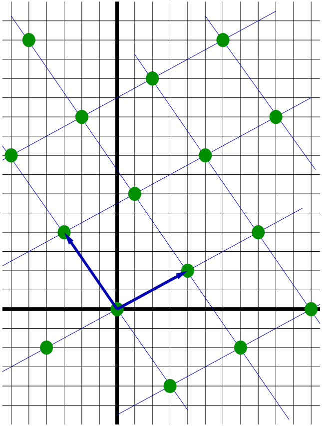
Determinant: $\det = |\det((\mathbf{b}_i)_i)|$, for any basis.
$= \text{volume of } \mathbb{R}^n / L$.



Ideal lattices

Let n be a power of 2 and $R = \mathbb{Z}[x]/(x^n + 1)$.

- $J \subseteq R$ is an ideal if $\quad \forall a, b \in J, \forall r \in R : \quad a + b \cdot r \in J$.
- Any ideal is a lattice, i.e., an additive subgroup of $\mathbb{Z}^n$.



Basis: $(\mathbf{b}_i)_{i \leq n}$ linearly independent s.t.

$$L = \{\sum_{i \leq n} x_i \mathbf{b}_i : x_i \in \mathbb{Z}\}$$

Minimum: $\lambda = \min(\|\mathbf{b}\| : \mathbf{b} \in L \setminus \mathbf{0})$.

Determinant: $\det = |\det((\mathbf{b}_i)_i)|$, for any basis.
$= \text{volume of } \mathbb{R}^n/L$.

Ideal lattices

Let n be a power of 2 and $R = \mathbb{Z}[x]/(x^n + 1)$.

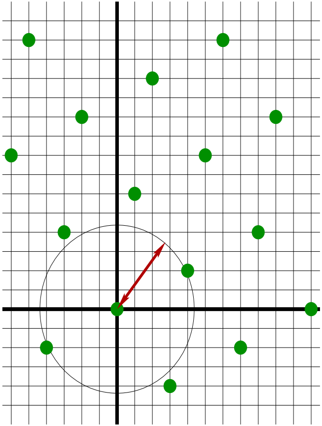
- $J \subseteq R$ is an ideal if $\forall a, b \in J, \forall r \in R: \quad a + b \cdot r \in J$.
- Any ideal is a lattice, i.e., an additive subgroup of $\mathbb{Z}^n$.

Basis: $(\mathbf{b}_i)_{i \leq n}$ linearly independent s.t.

$$L = \{\sum_{i \leq n} x_i \mathbf{b}_i : x_i \in \mathbb{Z}\}$$

Minimum: $\lambda = \min(\|\mathbf{b}\| : \mathbf{b} \in L \setminus \mathbf{0})$.

Determinant: $\det = |\det((\mathbf{b}_i)_i)|$, for any basis.
$= \text{volume of } \mathbb{R}^n/L$.



Ideal lattices

Let n be a power of 2 and $R = \mathbb{Z}[x]/(x^n + 1)$.

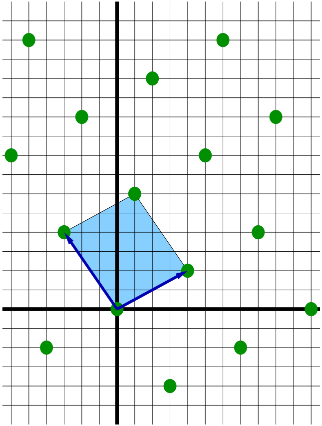
- $J \subseteq R$ is an ideal if $\forall a, b \in J, \forall r \in R : \quad a + b \cdot r \in J$.
- Any ideal is a lattice, i.e., an additive subgroup of $\mathbb{Z}^n$.

Basis: $(\mathbf{b}_i)_{i \leq n}$ linearly independent s.t.

$$L = \{\sum_{i \leq n} x_i \mathbf{b}_i : x_i \in \mathbb{Z}\}$$

Minimum: $\lambda = \min(\|\mathbf{b}\| : \mathbf{b} \in L \setminus \mathbf{0})$.

Determinant: $\det = |\det((\mathbf{b}_i)_i)|$, for any basis.
$= \text{volume of } \mathbb{R}^n/L$.



Gentry's somewhat homomorphic scheme: SomHom

- Public key: B_J a basis of an ideal J, with rather large $\det(J)$.
- Secret key: $\mathbf{v}_J^{sk}$.
- Plaintext domain: $\mathcal{P} = \{0, 1\}$. Ciphertext domain: $\mathcal{C} = R/B_J$.
- Encryption:

$$\pi \mapsto \psi = (\pi + 2\rho) \bmod B_J, \quad \text{with } \rho \text{ random and small.}$$

- Decryption:

$$\psi \mapsto (\psi - \lfloor \mathbf{v}_J^{sk} \cdot \psi \rceil) \bmod 2.$$

Gentry's somewhat homomorphic scheme: SomHom

- Public key: B_J a basis of an ideal J, with rather large $\det(J)$.
- Secret key: $\mathbf{v}_J^{sk}$.
- Plaintext domain: $\mathcal{P} = \{0,1\}$. Ciphertext domain: $\mathcal{C} = R/B_J$.

- Encryption:

$$\pi \mapsto \psi = (\pi + 2\rho) \bmod B_J, \quad \text{with } \rho \text{ random and small.}$$

- Decryption:

$$\psi \mapsto (\psi - \lfloor \mathbf{v}_J^{sk} \cdot \psi \rceil) \bmod 2.$$

Gentry's somewhat homomorphic scheme: SomHom

- Public key: B_J a basis of an ideal J, with rather large $\det(J)$.
- Secret key: $\mathbf{v}_J^{sk}$.
- Plaintext domain: $\mathcal{P} = \{0, 1\}$. Ciphertext domain: $\mathcal{C} = R/B_J$.

- Encryption:

$$\pi \mapsto \psi = (\pi + 2\rho) \bmod B_J, \text{ with } \rho \text{ random and small.}$$

- Decryption:

$$\psi \mapsto (\psi - \lfloor \mathbf{v}_J^{sk} \cdot \psi \rceil) \bmod 2.$$

Properties of Gentry's scheme

- "$\mathtt{Enc}(\pi_1) \binom{+}{\times} \mathtt{Enc}(\pi_2) \bmod B_J$" decrypts to $\pi_1 \binom{+}{\times} \pi_2$.
- "$\pi + 2\rho \bmod B_J$" decrypts to π, if $\rho \lesssim \det(J)^{1/n} \approx \lambda(J)$.
- An addition doubles ρ, a multiplication squares ρ.

Best known attack: Finding π from "$\pi + 2\rho \bmod B_J$" is an instance of the Bounded Distance Decoding problem.

See [Gentry-CRYPTO'10] for a security proof of $\mathtt{SomHom}$.

Properties of Gentry's scheme

- "$\mathtt{Enc}(\pi_1) \binom{+}{\times} \mathtt{Enc}(\pi_2) \bmod B_J$" decrypts to $\pi_1 \binom{+}{\times} \pi_2$.
- "$\pi + 2\rho \bmod B_J$" decrypts to π, if $\rho \lesssim \det(J)^{1/n} \approx \lambda(J)$.
- An addition doubles ρ, a multiplication squares ρ.

Best known attack: Finding π from "$\pi + 2\rho \bmod B_J$" is an instance of the Bounded Distance Decoding problem.

See [Gentry-CRYPTO'10] for a security proof of SomHom.

Properties of Gentry's scheme

- "$\mathtt{Enc}(\pi_1) \binom{+}{\times} \mathtt{Enc}(\pi_2)$ mod B_J" decrypts to $\pi_1 \binom{+}{\times} \pi_2$.
- "$\pi + 2\rho$ mod B_J" decrypts to π, if $\rho \lesssim \det(J)^{1/n} \approx \lambda(J)$.
- An addition doubles ρ, a multiplication squares ρ.

Best known attack: Finding π from "$\pi + 2\rho$ mod B_J" is an instance of the Bounded Distance Decoding problem.

See [Gentry-CRYPTO'10] for a security proof of $\mathtt{SomHom}$.

Properties of Gentry's scheme

- "$\mathtt{Enc}(\pi_1) \binom{+}{\times} \mathtt{Enc}(\pi_2) \bmod B_J$" decrypts to $\pi_1 \binom{+}{\times} \pi_2$.
- "$\pi + 2\rho \bmod B_J$" decrypts to π, if $\rho \lesssim \det(J)^{1/n} \approx \lambda(J)$.
- An addition doubles ρ, a multiplication squares ρ.

Best known attack: Finding π from "$\pi + 2\rho \bmod B_J$" is an instance of the Bounded Distance Decoding problem.

See [Gentry-CRYPTO'10] for a security proof of SomHom.

Properties of Gentry's scheme

- "$\texttt{Enc}(\pi_1) \binom{+}{\times} \texttt{Enc}(\pi_2) \bmod B_J$" decrypts to $\pi_1 \binom{+}{\times} \pi_2$.
- "$\pi + 2\rho \bmod B_J$" decrypts to π, if $\rho \lesssim \det(J)^{1/n} \approx \lambda(J)$.
- An addition doubles ρ, a multiplication squares ρ.

Best known attack: Finding π from "$\pi + 2\rho \bmod B_J$" is an instance of the Bounded Distance Decoding problem.

See [Gentry-CRYPTO'10] for a security proof of $\texttt{SomHom}$.

Lattice reduction 'Rule of Thumb' conjecture

BDD_γ

Given $(\mathbf{b}_i)_i$ basis of L and $\mathbf{t} \in \mathbb{Q}^n$ such that $\mathrm{dist}(\mathbf{t}, L) \leq \gamma^{-1} \cdot \lambda(L)$, find $\mathbf{b} \in L$ closest to $\mathbf{t}$.

SVP_γ

Given $(\mathbf{b}_i)_i$ basis of L, find $\mathbf{b} \in L$ such that $0 < \|\mathbf{b}\| \leq \gamma \cdot \lambda(L)$.

Lattice reduction 'rule of thumb' conjecture

There exists a constant c s.t. the following holds. Assuming there is nothing "special" with the lattice:
with time $\leq 2^t$, one cannot solve $\mathrm{SVP}_\gamma/\mathrm{BDD}_\gamma$ for $\gamma < c^{n/t}$.

This conjecture is consistent with the current algorithmic knowledge. Essentially unchanged since [Schnorr'87].

Lattice reduction 'Rule of Thumb' conjecture

BDD_γ

Given $(\mathbf{b}_i)_i$ basis of L and $\mathbf{t} \in \mathbb{Q}^n$ such that $\text{dist}(\mathbf{t}, L) \leq \gamma^{-1} \cdot \lambda(L)$, find $\mathbf{b} \in L$ closest to $\mathbf{t}$.

SVP_γ

Given $(\mathbf{b}_i)_i$ basis of L, find $\mathbf{b} \in L$ such that $0 < \|\mathbf{b}\| \leq \gamma \cdot \lambda(L)$.

Lattice reduction 'rule of thumb' conjecture

There exists a constant c s.t. the following holds. Assuming there is nothing "special" with the lattice:
with time $\leq 2^t$, one cannot solve $\text{SVP}_\gamma/\text{BDD}_\gamma$ for $\gamma < c^{n/t}$.

This conjecture is consistent with the current algorithmic knowledge. Essentially unchanged since [Schnorr'87].

Lattice reduction 'Rule of Thumb' conjecture

BDD_γ

Given $(\mathbf{b}_i)_i$ basis of L and $\mathbf{t} \in \mathbb{Q}^n$ such that $\mathrm{dist}(\mathbf{t}, L) \leq \gamma^{-1} \cdot \lambda(L)$, find $\mathbf{b} \in L$ closest to $\mathbf{t}$.

SVP_γ

Given $(\mathbf{b}_i)_i$ basis of L, find $\mathbf{b} \in L$ such that $0 < \|\mathbf{b}\| \leq \gamma \cdot \lambda(L)$.

Lattice reduction 'rule of thumb' conjecture

There exists a constant c s.t. the following holds. Assuming there is nothing "special" with the lattice:
with time $\leq 2^t$, one cannot solve $\mathrm{SVP}_\gamma/\mathrm{BDD}_\gamma$ for $\gamma < c^{n/t}$.

This conjecture is consistent with the current algorithmic knowledge. Essentially unchanged since [Schnorr'87].

From SomHom to FullHom, via bootstrapping

- An encryption scheme is bootstrappable if it can homomorphically evaluate its own decryption circuit.
- Decryption/security constraints
  $\Rightarrow$ SomHom is not bootstrappable.

To squash the decryption, some effort is shifted from $\mathcal{P}$ to $\mathcal{C}$:

- Splitting the secret key $\mathbf{v}_J^{sk}$:

$$\mathbf{v}_J^{sk} = \sum_{i \leq n_{set}} s_i \mathbf{v}_i, \text{ for } \mathbf{s} \in \{0,1\}^n \text{ of Hamming weight } n_{sub}.$$

- New secret key: $(s_i)_i$; New public key: B_J, $(\mathbf{v}_i)_i$.
- Ciphertext expansion: $\psi \mapsto (\psi \times \mathbf{v}_i)_i$.
- Decryption: $\psi, (\psi \times \mathbf{v}_i)_i \mapsto (\psi - \lfloor \sum_i s_i(\psi \times \mathbf{v}_i) \rceil) \bmod 2$.

From SomHom to FullHom, via bootstrapping

- An encryption scheme is bootstrappable if it can homomorphically evaluate its own decryption circuit.
- Decryption/security constraints
  $\Rightarrow$ SomHom is not bootstrappable.

To squash the decryption, some effort is shifted from $\mathcal{P}$ to $\mathcal{C}$:

- Splitting the secret key $\mathbf{v}_J^{sk}$:

$$\mathbf{v}_J^{sk} = \sum_{i \leq n_{set}} s_i \mathbf{v}_i, \text{ for } \mathbf{s} \in \{0,1\}^n \text{ of Hamming weight } n_{sub}.$$

- New secret key: $(s_i)_i$; New public key: B_J, $(\mathbf{v}_i)_i$.
- Ciphertext expansion: $\psi \mapsto (\psi \times \mathbf{v}_i)_i$.
- Decryption: $\psi, (\psi \times \mathbf{v}_i)_i \mapsto (\psi - \lfloor \sum_i s_i(\psi \times \mathbf{v}_i) \rceil) \bmod 2$.

From SomHom to FullHom, via bootstrapping

- An encryption scheme is bootstrappable if it can homomorphically evaluate its own decryption circuit.
- Decryption/security constraints
  $\Rightarrow$ SomHom is not bootstrappable.

To squash the decryption, some effort is shifted from $\mathcal{P}$ to $\mathcal{C}$:

- Splitting the secret key $\mathbf{v}_J^{sk}$:

$$\mathbf{v}_J^{sk} = \sum_{i \leq n_{set}} s_i \mathbf{v}_i, \text{ for } \mathbf{s} \in \{0,1\}^n \text{ of Hamming weight } n_{sub}.$$

- New secret key: $(s_i)_i$; New public key: B_J, $(\mathbf{v}_i)_i$.
- Ciphertext expansion: $\psi \mapsto (\psi \times \mathbf{v}_i)_i$.
- Decryption: $\psi, (\psi \times \mathbf{v}_i)_i \mapsto (\psi - \lfloor \sum_i s_i(\psi \times \mathbf{v}_i) \rceil) \bmod 2$.

1. Reminders on homomorphic encryption.
2. **Ingredient 1: a less pessimistic analysis of S(V)SSP.**
3. Ingredient 2: a shallower decryption algorithm.

Using the lattice 'rule of thumb' for both BDD and S(V)SSP.

The Sparse Vector Subset Sum Problem

$\mathrm{SVSSP}_{n_{set}, n_{sub}}$

Distinguish between $(\mathbf{a}_i)_{i \leq n_{set}}$ uniform in $[R \bmod (2J)]^{n_{set}}$ and the same but conditioned on the existence of $\mathbf{s} \in \{0,1\}^{n_{set}}$ of Hamming weight n_{sub} s.t. $\sum_i s_i \mathbf{a_i} = 0 \bmod 2J$.

- Resembles Sparse Subset Sum Problem (with integers rather than ring elements), used for server-aided RSA.
- Gentry showed that `FullHom` is secure assuming the hardnesses of:
  - BDD_γ for ideal lattices, for a large γ.
  - $\mathrm{SVSSP}_{n_{set}, n_{sub}}$ for specific values of $n_{sub} \ll n_{set}$.

The Sparse Vector Subset Sum Problem

$\mathrm{SVSSP}_{n_{set},n_{sub}}$

Distinguish between $(\mathbf{a}_i)_{i \le n_{set}}$ uniform in $[R \bmod (2J)]^{n_{set}}$ and the same but conditioned on the existence of $\mathbf{s} \in \{0,1\}^{n_{set}}$ of Hamming weight n_{sub} s.t. $\sum_i s_i \mathbf{a_i} = 0 \bmod 2J$.

- Resembles Sparse Subset Sum Problem (with integers rather than ring elements), used for server-aided RSA.
- Gentry showed that `FullHom` is secure assuming the hardnesses of:
  - BDD_γ for ideal lattices, for a large γ.
  - $\mathrm{SVSSP}_{n_{set},n_{sub}}$ for specific values of $n_{sub} \ll n_{set}$.

Known attacks on SVSSP

$\mathrm{SVSSP}_{n_{set},n_{sub}}$

Distinguish between $(\mathbf{a}_i)_{i \leq n_{set}}$ uniform in $[R \bmod (2J)]^{n_{set}}$ and the same but conditioned on the existence of $\mathbf{s} \in \{0,1\}^{n_{set}}$ of Hamming weight n_{sub} s.t. $\sum_i s_i \mathbf{a_i} = 0 \bmod 2J$.

- Birthday paradox. Requires time $\binom{n_{set}}{n_{sub}}^{1/2}$.
- Lattice attack: $\mathbf{s}$ is likely to be a shortest non-zero vector in

$$L = \{\mathbf{x} \in \mathbb{Z}^{n_{set}} : \sum_i x_i \mathbf{a}_i = 0 \bmod 2J\}.$$

Known attacks on SVSSP

$\text{SVSSP}_{n_{set}, n_{sub}}$

Distinguish between $(\mathbf{a}_i)_{i \leq n_{set}}$ uniform in $[R \bmod (2J)]^{n_{set}}$ and the same but conditioned on the existence of $\mathbf{s} \in \{0,1\}^{n_{set}}$ of Hamming weight n_{sub} s.t. $\sum_i s_i \mathbf{a_i} = 0 \bmod 2J$.

- Birthday paradox. Requires time $\binom{n_{set}}{n_{sub}}^{1/2}$.
- Lattice attack: $\mathbf{s}$ is likely to be a shortest non-zero vector in

$$L = \{\mathbf{x} \in \mathbb{Z}^{n_{set}} : \sum_i x_i \mathbf{a}_i = 0 \bmod 2J\}.$$

Analysis of the lattice attack against SVSSP

$$L = \{\mathbf{x} \in \mathbb{Z}^{n_{set}} : \sum_i x_i \mathbf{a}_i = 0 \bmod 2J\}.$$

- $\dim(L) = n_{set}$.
- $\lambda(L) \in [1, \sqrt{n_{sub}}]$.
- $\det(L) \leq \det(2J) = 2^n \det(J)$.

Former analysis:

- $n_{set} \gg \log_2 \det(2J)$ implies the existence of too many short vectors (via Minkowski's theorem).
- Most are unlikely to give any insight for solving SVSSP.

Analysis of the lattice attack against SVSSP

$$L = \{\mathbf{x} \in \mathbb{Z}^{n_{set}} : \sum_i x_i \mathbf{a}_i = 0 \bmod 2J\}.$$

- $\dim(L) = n_{set}$.
- $\lambda(L) \in [1, \sqrt{n_{sub}}]$.
- $\det(L) \leq \det(2J) = 2^n \det(J)$.

Former analysis:

- $n_{set} \gg \log_2 \det(2J)$ implies the existence of too many short vectors (via Minkowski's theorem).
- Most are unlikely to give any insight for solving SVSSP.

A less pessimistic analysis of the lattice attack

$$L = \{\mathbf{x} \in \mathbb{Z}^{n_{set}} : \sum_i x_i \mathbf{a}_i = 0 \bmod 2J\}.$$

- The former analysis assumes being able to find extremely short vectors of L, i.e., essentially solve SVP.
- But for SomHom, we assumed BDD_γ hard for a large γ.

We homogenize the hardness assumptions:

- 'Rule of thumb' $\Rightarrow$ in time $\leq 2^t$, one cannot find vectors shorter than $c^{n_{set}/t}$, for some constant c.
- Minkowski's theorem implies that there are many vectors of L within that norm bound.
- Most are unlikely to give any insight for solving SVSSP.

A less pessimistic analysis of the lattice attack

$$L = \{\mathbf{x} \in \mathbb{Z}^{n_{set}} : \sum_i x_i \mathbf{a}_i = 0 \bmod 2J\}.$$

- The former analysis assumes being able to find extremely short vectors of L, i.e., essentially solve SVP.
- But for SomHom, we assumed BDD_γ hard for a large γ.

We homogenize the hardness assumptions:

- 'Rule of thumb' $\Rightarrow$ in time $\leq 2^t$, one cannot find vectors shorter than $c^{n_{set}/t}$, for some constant c.
- Minkowski's theorem implies that there are many vectors of L within that norm bound.
- Most are unlikely to give any insight for solving SVSSP.

A less pessimistic analysis of the lattice attack

$$L = \{\mathbf{x} \in \mathbb{Z}^{n_{set}} : \sum_i x_i \mathbf{a}_i = 0 \bmod 2J\}.$$

- The former analysis assumes being able to find extremely short vectors of L, i.e., essentially solve SVP.
- But for SomHom, we assumed BDD_γ hard for a large γ.

We homogenize the hardness assumptions:

- 'Rule of thumb' $\Rightarrow$ in time $\leq 2^t$, one cannot find vectors shorter than $c^{n_{set}/t}$, for some constant c.
- Minkowski's theorem implies that there are many vectors of L within that norm bound.
- Most are unlikely to give any insight for solving SVSSP.

1. Reminders on homomorphic encryption.
2. Ingredient 1: a less pessimistic analysis of S(V)SSP.
3. **Ingredient 2: a shallower decryption algorithm.**

Using fewer multiplications to homomorphically decrypt.

Decryption

- For SomHom: $\psi \mapsto \psi - \lfloor \mathbf{v}_J^{sk} \cdot \psi \rceil \bmod 2$.
- Squashed decryption:
$$\psi, (\psi \times \mathbf{v}_i)_i \mapsto \psi - \lfloor \sum_i s_i (\psi \times \mathbf{v}_i) \rceil \bmod 2.$$
- The decryption circuit is to be evaluated homomorphically.
- What's important: not the time complexity, but the multiplicative degree of the algebraic decryption circuit.
- Because this fixes the homomorphic capacity of SomHom, and thus the size of J.

Decryption

- For SomHom: $\psi \mapsto \psi - \lfloor \mathbf{v}_J^{sk} \cdot \psi \rceil \bmod 2$.
- Squashed decryption:

$$\psi, (\psi \times \mathbf{v}_i)_i \mapsto \psi - \lfloor \sum_i s_i (\psi \times \mathbf{v}_i) \rceil \bmod 2.$$

- The decryption circuit is to be evaluated homomorphically.
- What's important: not the time complexity, but the multiplicative degree of the algebraic decryption circuit.
- Because this fixes the homomorphic capacity of SomHom, and thus the size of J.

Decryption

- For SomHom: $\psi \mapsto \psi - \lfloor \mathbf{v}_J^{sk} \cdot \psi \rceil \bmod 2$.
- Squashed decryption:

$$\psi, (\psi \times \mathbf{v}_i)_i \mapsto \psi - \lfloor \sum_i s_i (\psi \times \mathbf{v}_i) \rceil \bmod 2.$$

- The decryption circuit is to be evaluated homomorphically.
- What's important: not the time complexity, but the multiplicative degree of the algebraic decryption circuit.
- Because this fixes the homomorphic capacity of SomHom, and thus the size of J.

Decryption

- For $\textsc{SomHom}$: $\psi \mapsto \psi - \lfloor \mathbf{v}_J^{sk} \cdot \psi \rceil \bmod 2$.
- Squashed decryption:
$$\psi, (\psi \times \mathbf{v}_i)_i \mapsto \psi - \lfloor \sum_i s_i (\psi \times \mathbf{v}_i) \rceil \bmod 2.$$
- The decryption circuit is to be evaluated homomorphically.
- What's important: not the time complexity, but the multiplicative degree of the algebraic decryption circuit.
- Because this fixes the homomorphic capacity of $\textsc{SomHom}$, and thus the size of J.

Degree of the decryption

Dominating component: sum of n_{sub} reals $y_1, \ldots, y_{n_{sub}}$, modulo 2.

1. Choose a precision p for the inputs: $y_i = \sum_{j=0}^{p} y_{i,j} 2^{-j}$.
2. For each j, compute $S_j = \sum_{i \le n_{sub}} y_{i,j}$.
3. Compute $S = \left(\sum_j S_j 2^{-j}\right) \bmod 2$.

- Step 2 dominates.
- If $\sum_k S_{j,k} 2^k$ is the binary representation of S_j, then $S_{j,k}$ has algebraic degree 2^k.
- S_j can be as large as $n_{sub} \Rightarrow$ decryption degree $\approx n_{sub}$

Degree of the decryption

Dominating component: sum of n_{sub} reals $y_1, \ldots, y_{n_{sub}}$, modulo 2.

1. Choose a precision p for the inputs: $y_i = \sum_{j=0}^{p} y_{i,j} 2^{-j}$.
2. For each j, compute $S_j = \sum_{i \le n_{sub}} y_{i,j}$.
3. Compute $S = (\sum_j S_j 2^{-j}) \bmod 2$.

- Step 2 dominates.
- If $\sum_k S_{j,k} 2^k$ is the binary representation of S_j, then $S_{j,k}$ has algebraic degree 2^k.
- S_j can be as large as $n_{sub} \Rightarrow$ decryption degree $\approx n_{sub}$

Shallower decryption: first remark

Dominating component: sum of n_{sub} reals $y_1, \ldots y_{n_{sub}}$, modulo 2.

1. Choose a precision p for the inputs: $y_i = \sum_{j=0}^{p} y_{i,j} 2^{-j}$.
2. For each j, compute $S_j = \sum_{i \leq n_{sub}} y_{i,j}$.
3. Compute $S = (\sum_j S_j 2^{-j}) \bmod 2$.

- S_j needs only being evaluated mod 2^{j+1}.
- Since $j \leq p$, the decryption degree is $\leq \min(2^{p+1}, n_{sub})$.
- But which p do we need?

Shallower decryption: choice of p

$$y_i = y_i' + \varepsilon_i, \quad |\varepsilon_i| \leq 2^{-p} \quad i = 1..n_{sub}.$$

- Promise: $\sum y_i$ is at distance $\leq 1/4$ of an integer.
- Former strategy: $p = 4 + \log_2 n_{sub} \Rightarrow \left|\sum_i \varepsilon_i\right| \leq 1/8$.
- Worst-case scenario: the signs of the errors are equal.

The worst-case scenario is very unlikely to happen!

- If the ε_i's are iid with expectancy 0, Hoeffding's bound gives:

$$\Pr\left[\left|\sum_i \varepsilon_i\right| \geq \sqrt{n_{sub}} \cdot 2^{-p} \cdot \omega(\sqrt{\log t})\right] \leq n^{-\omega(1)}.$$

$\Rightarrow$ Choose $p \approx \frac{1}{2} \log_2 n_{sub}$.

Shallower decryption: choice of p

$$y_i = y_i' + \varepsilon_i, \quad |\varepsilon_i| \leq 2^{-p} \quad i = 1..n_{sub}.$$

- Promise: $\sum y_i$ is at distance $\leq 1/4$ of an integer.
- Former strategy: $p = 4 + \log_2 n_{sub} \Rightarrow \ |\sum_i \varepsilon_i| \leq 1/8$.
- Worst-case scenario: the signs of the errors are equal.

The worst-case scenario is very unlikely to happen!

- If the ε_i's are iid with expectancy 0, Hoeffding's bound gives:

$$\Pr\left[|\sum_i \varepsilon_i| \geq \sqrt{n_{sub}} \cdot 2^{-p} \cdot \omega(\sqrt{\log t}) \right] \leq n^{-\omega(1)}.$$

$\Rightarrow$ Choose $p \approx \frac{1}{2} \log_2 n_{sub}$.

Shallower decryption: choice of p

$$y_i = y_i' + \varepsilon_i, \quad |\varepsilon_i| \leq 2^{-p} \quad i = 1..n_{sub}.$$

- Promise: $\sum y_i$ is at distance $\leq 1/4$ of an integer.
- Former strategy: $p = 4 + \log_2 n_{sub} \Rightarrow |\sum_i \varepsilon_i| \leq 1/8$.
- Worst-case scenario: the signs of the errors are equal.

The worst-case scenario is very unlikely to happen!

- If the ε_i's are iid with expectancy 0, Hoeffding's bound gives:

$$\Pr\left[|\sum_i \varepsilon_i| \geq \sqrt{n_{sub}} \cdot 2^{-p} \cdot \omega(\sqrt{\log t}) \right] \leq n^{-\omega(1)}.$$

$\Rightarrow$ Choose $p \approx \frac{1}{2} \log_2 n_{sub}$.

Shallower decryption: choice of p

$$y_i = y'_i + \varepsilon_i, \quad |\varepsilon_i| \leq 2^{-p} \quad i = 1..n_{sub}.$$

- Promise: $\sum y_i$ is at distance $\leq 1/4$ of an integer.
- Former strategy: $p = 4 + \log_2 n_{sub} \Rightarrow |\sum_i \varepsilon_i| \leq 1/8$.
- Worst-case scenario: the signs of the errors are equal.

The worst-case scenario is very unlikely to happen!

- If the ε_i's are iid with expectancy 0, Hoeffding's bound gives:

$$\Pr\left[|\sum_i \varepsilon_i| \geq \sqrt{n_{sub}} \cdot 2^{-p} \cdot \omega(\sqrt{\log t})\right] \leq n^{-\omega(1)}.$$

$\Rightarrow$ Choose $p \approx \frac{1}{2} \log_2 n_{sub}$.

Shallower decryption: choice of p

$$y_i = y_i' + \varepsilon_i, \quad |\varepsilon_i| \leq 2^{-p} \quad i = 1..n_{sub}.$$

- Promise: $\sum y_i$ is at distance $\leq 1/4$ of an integer.
- Former strategy: $p = 4 + \log_2 n_{sub} \Rightarrow |\sum_i \varepsilon_i| \leq 1/8$.
- Worst-case scenario: the signs of the errors are equal.

The worst-case scenario is very unlikely to happen!

- If the ε_i's are iid with expectancy 0, Hoeffding's bound gives:

$$\Pr\left[|\sum_i \varepsilon_i| \geq \sqrt{n_{sub}} \cdot 2^{-p} \cdot \omega(\sqrt{\log t}) \right] \leq n^{-\omega(1)}.$$

$\Rightarrow$ Choose $p \approx \frac{1}{2} \log_2 n_{sub}$.

Shallower decryption: choice of p

$$y_i = y_i' + \varepsilon_i, \quad |\varepsilon_i| \leq 2^{-p} \quad i = 1..n_{sub}.$$

- Promise: $\sum y_i$ is at distance $\leq 1/4$ of an integer.
- Former strategy: $p = 4 + \log_2 n_{sub} \Rightarrow |\sum_i \varepsilon_i| \leq 1/8$.
- Worst-case scenario: the signs of the errors are equal.

The worst-case scenario is very unlikely to happen!

- If the ε_i's are iid with expectancy 0, Hoeffding's bound gives:

$$\Pr\left[|\sum_i \varepsilon_i| \geq \sqrt{n_{sub}} \cdot 2^{-p} \cdot \omega(\sqrt{\log t}) \right] \leq n^{-\omega(1)}.$$

$\Rightarrow$ Choose $p \approx \frac{1}{2} \log_2 n_{sub}$.

Remarks on the shallower decryption

- Making the ε_i's iid with expectancy 0 requires some care.
- Decryption is now probabilistic: it fails with negligible prob.
- Additional difficulty for the KDM-variant of Gentry's `FullHom` (to ensure independence).

Conclusion

Let $q = \det(2J)$, security goal $\geq 2^t$.

Condition	[Gentry'09]	Here
Ideal-BDD hard	$q^{1/n} \leq c^{n/t}$	
SVSSP-Combinatorial	$\binom{n_{set}}{n_{sub}} \geq 2^{2t}$	
SVSSP-Lattice	$n_{set} = \Omega(\log q)$	$\frac{n_{set}^2}{t} = \widetilde{\Omega}(\log q)$
Bootstrappability	$n_{sub} \leq \log q^{1/n}$	$\sqrt{n_{sub}} \lesssim \log q^{1/n}$

Complexity of homomorphically evaluating one gate:

$$\approx n_{set} \log q : \quad \widetilde{\mathcal{O}}(t^6) \longrightarrow \widetilde{\mathcal{O}}(t^{3.5}).$$

Conclusion

Let $q = \det(2J)$, security goal $\geq 2^t$.

Condition	[Gentry'09]	Here
Ideal-BDD hard	$q^{1/n} \leq c^{n/t}$	
SVSSP-Combinatorial	$\binom{n_{set}}{n_{sub}} \geq 2^{2t}$	
SVSSP-Lattice	$n_{set} = \Omega(\log q)$	$\frac{n_{set}^2}{t} = \widetilde{\Omega}(\log q)$
Bootstrappability	$n_{sub} \leq \log q^{1/n}$	$\sqrt{n_{sub}} \lesssim \log q^{1/n}$

Complexity of homomorphically evaluating one gate:

$$\approx n_{set} \log q : \quad \widetilde{\mathcal{O}}(t^6) \longrightarrow \widetilde{\mathcal{O}}(t^{3.5}).$$

Open problems

1. Faster scheme, e.g., using more bits in the plaintext (see work by Smart and Vercauteren).
2. Fewer security assumptions, e.g., no S(V)SSP.
3. Better understood security assumptions: can we rely on more classical assumptions? can we improve Gentry's CRYPTO'10 reduction?
4. What about practice? (see work by Gentry and Halevi).