Efficient Inner-Product Encryption over NTRU Lattices

Shantian Cheng, Ivan Tjuawinata

Division of Mathematical Sciences
School of Physical and Mathematical Sciences
Nanyang Technological University

June 13, 2015 at CCCS, Guangzhou

Outline

Identity-Based Encryption (IBE)

Definition: (Shamir-Crypto 1984)

- $\mathsf{Setup}(N, q, \ell) \rightarrow \mathsf{msk}, \mathsf{pp}$
- $\mathsf{Extract}(\mathsf{pp}, \mathsf{msk}, \mathsf{id} \in I^{\ell}) \rightarrow \mathsf{sk}_{\mathsf{id}}$
- $\mathsf{Enc}(\mathsf{pp}, \mathsf{id}' \in I^{\ell}, m) \rightarrow \mathsf{ct}$
- $\mathsf{Dec}(\mathsf{pp}, \mathsf{sk}_{\mathsf{id}}, \mathsf{ct}) \rightarrow \begin{cases} m, & \mathsf{id} = \mathsf{id}' \\ \perp, & \mathsf{id} \neq \mathsf{id}' \end{cases}$

Properties:

- Point-to-point communication. (Email)
- Access to the encrypted data is all or nothing.

New Challenge from Cloud Storage

In Cloud storage, data owners may share their outsourced data with a large number of users.

- The owner specifies a decryption policy that only individuals who satisfy the policy can decrypt. (attribute-based encryption)
- Or, the authorized users want to only retrieve specific data files they are interested in. (searchable keyword-based encryption)
  - Boolean combinations of keywords queries help enhance the efficiency of retrieving files from cloud. (conjunction and disjunction)

Predicate Encryption (PE)

Definition: (Boneh and Waters-TCC 2007)

- $\text{Setup}(N, q, \ell) \rightarrow \text{msk}, \text{pp}$
- $\text{Extract}(\text{pp}, \text{msk}, \phi \in \Phi) \rightarrow \text{sk}_\phi$
- $\text{Enc}(\text{pp}, \sigma \in \Sigma, m) \rightarrow \text{ct}$
- $\text{Dec}(\text{pp}, \text{sk}_\phi, \text{ct}) \rightarrow \begin{cases} m, & \mathcal{P}(\phi, \sigma) = 1 \\ \perp, & \mathcal{P}(\phi, \sigma) \neq 1 \end{cases}$

Properties:

- Fine-grained access control over access to encrypted data.
- Expressive for different requirement. (IBE, ABE, etc.)

Inner-Product Encryption (IPE)

Definition: (Katz et al.-Eurocrypt 2008)

- $\text{Setup}(N, q, \ell) \rightarrow \text{msk}, \text{pp}$
- $\text{Extract}(\text{pp}, \text{msk}, \vec{v} \in F^{\ell}) \rightarrow \text{sk}_{\vec{v}}$
- $\text{Enc}(\text{pp}, \vec{w} \in F^{\ell}, m) \rightarrow \text{ct}$
- $\text{Dec}(\text{pp}, \text{sk}_{\vec{v}}, \text{ct}) \rightarrow \begin{cases} m, & \langle \vec{v}, \vec{w} \rangle = 0 \\ \approx \text{uniformly random}, & \langle \vec{v}, \vec{w} \rangle \neq 0 \end{cases}$

Security:

- (Weakly) attribute hiding: Indistinguishable between $\text{Enc}(\text{pp}, \vec{w_1}, m_1)$ and $\text{Enc}(\text{pp}, \vec{w_2}, m_2)$.

Inner-Product Encryption

- IPE supports disjunctive, conjunctive keyword searches.
- Search for keyword $x = 7$ or $x = 9$ $\iff$ $\mathrm{OR}_{7,9}(x) = 1$
  $\iff$ $p(x) = (x-7)(x-9) = x^2 - 16x + 63 = 0$
  $\iff$ inner product of $\vec{v} = (1, -16, 63), \vec{w} = (x^2, x, 1)$ is 0
- Search for keywords $x_1 = 7$ and $x_2 = 9$
  $\iff$ $\mathrm{AND}_{7,9}(x_1, x_2) = 1$
  $\rightsquigarrow$ $p'(x) = c \cdot (x_1 - 7) + (x_2 - 9) = cx_1 + x_2 - (7c + 9) = 0$
  $\iff$ inner product of $\vec{v} = (c, 1, -(7c+9)), \vec{w} = (x_1, x_2, 1)$ is 0

Constructions

Pairing on composite-number or prime order groups.

- Katz et al.-Eurocrypt 2008
- Okamoto and Takashima-Asiacrypt 2009

Lattice based on learning with errors (LWE) assumptions.

- Agrawal et al-Asiacrypt 2011
- Xagawa-PKC 2013

Definition

- Hoffstein et al.-ANTS 1998.
- $N = 2^m$, $q \in \mathbb{Z}_+$.
- $\mathcal{R} = \mathbb{Z}[x]/(x^N + 1)$, $\mathcal{R}_q = \mathcal{R} \bmod q$.

Definition

The NTRU lattice associated to $h \in \mathcal{R}_q$ and q is

$$\Lambda_{h,q} = \left\{(u, v) \in \mathcal{R}^2 : u + v * h = 0 \bmod q\right\}.$$

$\Lambda_{h,q}$ is a full-rank lattice in $\mathbb{Z}^{2N}$.

Assumptions

- **Decisional Small Polynomial Ratio (DSPR) Assumption.**
  $h = g * f^{-1} \sim U(\mathcal{R}_q)$ given $f, g \leftarrow$ discrete Gaussian distribution over $\mathcal{R}_q$.
- **Decisional Ring-LWE Assumption.**
  $(d_i, d_i * r + e_i) \sim U(\mathcal{R}_q \times \mathcal{R}_q)$ given $d_i \leftarrow U(\mathcal{R}_q)$ and r, e_i are small polynomials.

NANYANG TECHNOLOGICAL UNIVERSITY

Trapdoor Generation and Gaussian Sampling

Comparison between Ducas et al.-Asiacrypt 2014 and Gentry et al.-STOC 2008.

- Master_Keygen$(N, q) \rightarrow h \sim U(\mathcal{R}_q), \mathbf{B} \in \mathbb{Z}^{2N \times 2N}$ (basis of $\Lambda_{h,q}$)
  - TrapGen(n, m, q) $\rightarrow A \sim U(\mathbb{Z}_q^{n \times m}), \mathbf{B} \in \mathbb{Z}^{m \times m}$ (basis of $\Lambda_q^{\perp}(\mathbf{A})$).
- Gaussian_Sampler$(\mathbf{B}, \sigma, \mathbf{c}) \rightarrow \mathbf{v} \sim D_{\Lambda(\mathbf{B}),\sigma,\mathbf{c}}$
  - SampleD$(\mathbf{B}, \sigma, \mathbf{c}) \rightarrow \mathbf{v} \sim D_{\Lambda(\mathbf{B}),\sigma,\mathbf{c}}$

NANYANG TECHNOLOGICAL UNIVERSITY

Anticirculant Matrix

- Let $f = f_0 + f_1 x + \cdots + f_{N-1} x^{N-1} \in \mathcal{R}$. The anticirculant matrix of f is

$$\mathcal{A}(f) = \begin{bmatrix} f_0 & -f_{N-1} & \cdots & -f_1 \\ f_1 & f_0 & \cdots & -f_2 \\ \vdots & \vdots & \ddots & \vdots \\ f_{N-1} & f_{N-2} & \cdots & f_0 \end{bmatrix}.$$

- $\mathcal{A}(f) + \mathcal{A}(g) = \mathcal{A}(f + g)$ and $\mathcal{A}(f) \times \mathcal{A}(g) = \mathcal{A}(f \times g)$.

Outline

Setup(N, q, ℓ)

$k := \lceil \lg q \rceil$ and inner-product predicates space $\mathcal{R}_q^\ell$.

1. $\left(h, \mathbf{B} = \begin{bmatrix} \mathcal{A}(g) & \mathcal{A}(G) \\ \mathcal{A}(-f) & \mathcal{A}(-F) \end{bmatrix}\right) \leftarrow \text{Master\_Keygen}(N, q)$.
   - Requirement: $\|(f, g)\| \approx 1.17\sqrt{q}$, $h = g * f^{-1}$ and $f * G - g * F = q$;
   - Property: $\mathbf{B}$ is a basis of NTRU lattice $\Lambda_{h,q}$ with $\left\|\tilde{\mathbf{B}}\right\| \approx 1.17\sqrt{q}$.
2. $d_{i,\gamma} \xleftarrow{\$} \mathcal{R}_q$, where $i \in \{1, \cdots, \ell\}, \gamma \in \{0, \cdots, k-1\}$. $u \xleftarrow{\$} \mathcal{R}_q$.

Output $\text{pp} \leftarrow (h, \{d_{i,\gamma}\}, u)$ and $\text{msk} = \mathbf{B}$.

Extract(pp, msk, $\vec{v} \in \mathcal{R}_q^\ell$)

1. $\vec{v} = (v_1, \cdots, v_\ell)$. For each $v_i \in [0, q-1]^N$, compute the binary decomposition of v_i as $v_i = \sum_{\gamma=0}^{k-1} v_{i,\gamma} \cdot 2^\gamma$, where $v_{i,\gamma} \in \{0,1\}^N$.
2. $d_{\vec{v}} := \sum_{i=1}^{\ell} \sum_{\gamma=0}^{k-1} v_{i,\gamma} * d_{i,\gamma} \in \mathcal{R}_q$.
3. $(s_1, s_2, s_3) \leftarrow$

$$(u,0,0) - \text{Gaussian\_Sampler}\left(\begin{bmatrix} g & G & 0 \\ -f & -F & -h^{-1} * d_{\vec{v}} \\ 0 & 0 & 1 \end{bmatrix}, \sigma, (u,0,0)\right).$$

   - Requirement: $\sigma \geq \frac{1}{\sqrt{2}} \sqrt{\frac{\lambda \ln 2}{2\pi^2}} \cdot 1.17\sqrt{q}$.
   - Property: $s_1 + s_2 * h + s_3 * d_{\vec{v}} = u$, $\|(s_1, s_2, s_3)\| \leq \sigma\sqrt{3N}$.

Output $\text{sk}_{\vec{v}} \leftarrow (s_2, s_3)$.

$\mathsf{Enc}(\mathsf{pp}, \vec{w} \in \mathcal{R}_q^\ell, m)$

1. Choose $r, e_0, e_1, e_{i,\gamma} \xleftarrow{\$} \{-1, 0, 1\}^N$ and $g \xleftarrow{\$} \mathcal{R}_q$
2. $c_0 \leftarrow r * h + e_0$.
3. $c_1 \leftarrow r * u + e_1 + m \cdot \lfloor q/2 \rfloor$.
4. $c_{i,\gamma} \leftarrow r * (d_{i,\gamma} + 2^\gamma \cdot w_i * g) + e_{i,\gamma}$. (Here $\vec{w} = (w_1, \cdots, w_\ell)$)
   - $\langle \vec{v}, \vec{w} \rangle = \sum_{i=1}^{\ell} \sum_{\gamma=0}^{k-1} (v_{i,\gamma} \cdot 2^\gamma) * w_i = \sum_{i=1}^{\ell} \sum_{\gamma=0}^{k-1} v_{i,\gamma} * (2^\gamma \cdot w_i)$.
   - Requirement: $\ell \cdot k$ less than any polynomial of n. (Arora and Ge-ICALP 2011).
   - Property: Based on Ring-LWE, the distribution of $c_0, c_1, c_{i,\gamma}$ is indistinguishable from uniform. (Weakly attribute hiding)

Output $\mathsf{ct} \leftarrow \left(c_0, c_1, \{c_{i,\gamma}\}_{i \in \{1,\cdots,\ell\}, \gamma \in \{0,\cdots,k-1\}}\right)$.

$\mathsf{Dec}(\mathsf{pp}, \mathsf{sk}_{\vec{v}}, \mathsf{ct})$

1. Compute

$$c_{\vec{v}} := \sum_{i=1}^{\ell} \sum_{\gamma=0}^{k-1} v_{i,\gamma} * c_{i,\gamma}.$$

2. Let $c := c_1 - s_2 * c_0 - s_3 * c_{\vec{v}}$.

Output the vector $\left\lceil \frac{c}{q/2} \right\rfloor$.

Remark:

$$\begin{aligned} c &= m \cdot \lfloor q/2 \rfloor + \langle \vec{v}, \vec{w} \rangle * s_3 * r * g \\ &\quad \underbrace{+ e_1 + r * s_1 - s_2 * e_0 - s_3 * \sum_{i=1}^{\ell} \sum_{\gamma=0}^{k-1} v_{i,\gamma} * e_{i,\gamma}}_{\text{error term} < q/5} \end{aligned}$$

Parameters

Asymptotically:

- We require $q = O\left((\ell \cdot N^{1.5} \cdot \log N)^{2+\epsilon}\right)$. Public key size=ciphertext size= $O(\ell N \log^2 q)$.
- q and public parameter are N times smaller than Xagawa-PKC 2013.

Low dimensions:

Security parameter λ	80	192
Root Hermite factor γ	1.0055	1.0029
Polynomial degree N	2048	4096
Modulus q	2^{66}	2^{70}
Dimension ℓ	5	6
Public key size	8 MB	16 MB
Master key size	128 KB	256 KB
Private key size	64 KB	128 KB
Ciphertext size	8 MB	16 MB

Outline

Possible Ways to Improve

New trapdoor generation and preimage sampling algorithms.

- Ring-based analogue of *simpler, tighter, faster, smaller* new trapdoors from Micciancio and Peikert-Eurocrypt 2012.
- To our best knowledge, no ring-based or NTRU adaptation of SampleD.

Binary expansion to other number systems.

- Factorial number system ($n!$), primorial number system ($p!$). (tradeoff between q and size of pp, ct)

Implementation of Lattice-Based Cryptography

NTRU encryption bas been included in

- IEEE 1363.1-2008
- ASC (Accredited Standards Committee) ANSI X9.98-2010.

Generalize NTRU to support more functionalities (IBE, PE, etc.).

References

- Agrawal, S., Freeman, D., Vaikuntanathan, V.: Functional Encryption for Inner Product Predicates from Learning with Errors. In: ASIACRYPT 2011, LNCS, vol. 7073, pp. 21–40. Springer, Heidelberg (2011)
- Ducas, L., Lyubashevsky, V., Prest, T.: Efficient Identity-Based Encryption over NTRU Lattices. In: ASIACRYPT 2014, LNCS, vol. 8874, pp. 22–41. Springer, Heidelberg (2014)
- Gentry, C., Peikert, C., Vaikuntanathan, V.: Trapdoors for hard lattices and new cryptographic constructions. pp. 197–206. STOC '08, ACM, New York, NY, USA (2008)
- Katz, J., Sahai, A., Waters, B.: Predicate encryption supporting disjunctions, polynomial equations, and inner products. Journal of Cryptology 26(2), 191–224 (2013)

NANYANG TECHNOLOGICAL UNIVERSITY

THANK YOU

THANK YOU!