Public-Key Encryption Based on LWE

Li Chen
lichen.xd at gmail.com
Xidian University
November 9, 2013
Outline

1 Basic LWE cryptosystem
2 Homomorphic LWE cryptosystem
3 Discussion
References


Claim: Our slides are based on reference [1], [2], [3]
1 Basic LWE cryptosystem

Notations

- $\mathcal{N}(\mu, \sigma^2)$ denotes the normal (or Gaussian) distribution with mean $\mu$ and standard deviation $\sigma$ (variance $\sigma^2$).

- $\chi$ denotes the distribution on $\mathbb{Z}_q$.

- $\Psi_{\mu,\sigma^2}$ denotes the normal distribution $\mathcal{N}(\mu, \sigma^2)$ rounded up to the nearest integer and modulo $q$.

- We use a bold lower case character $\mathbf{z}$ to denote a column vector, use a bold upper case character $\mathbf{Z}$ to denote a matrix.
Definition 1.1 (Search LWE Problem I)  Take parameters \( n \in \mathbb{N} \), a modulus \( q \geq 2 \), and a ’error’ probability distribution \( \chi \) on \( \mathbb{Z}_q \). Let \( \mathcal{A}_{s, \chi} = \{(a, \langle a, s \rangle + e)\} \) be the probability distribution on \( \mathbb{Z}_q^n \times \mathbb{Z}_q \), where \( a \leftarrow \mathbb{Z}_q \), \( e \leftarrow \chi \), and all operations are performed in \( \mathbb{Z}_q \). An algorithm \( \mathcal{A} \) is said to solve the search LWE\(_{n,q,\chi} \) problem if, for any \( \mathbf{s} \in \mathbb{Z}_q \), given arbitrary number of independent samples from \( \mathcal{A}_{s, \chi} \), it output \( s \) (with high probability).

Definition 1.2 (Search LWE Problem II)  Take parameters \( n \in \mathbb{N} \), a modulus \( q \geq 2 \), and a ’error’ probability distribution \( \chi \) on \( \mathbb{Z}_q \). An algorithm \( \mathcal{A} \) is said to \((l, t, \varepsilon)\)-solve the search LWE\(_{n,q,\chi} \) problem if 

\[
\Pr_{\mathcal{A}, \mathbf{s}, \mathbf{e}} \left[ \mathbf{s} \leftarrow \mathcal{A}(\mathbf{A}, \mathbf{A}s + \mathbf{e}) \right] \geq \varepsilon
\]

where \( \mathbf{A} \leftarrow \mathbb{Z}_q^{l \times n}, \mathbf{s} \leftarrow \mathbb{Z}_q^n, \mathbf{e} \leftarrow \chi^n \), and the distinguisher runs in time at most \( t \).
Definition 1.3 (Decisional LWE Problem II) Take parameters $n \in \mathbb{N}$. An algorithm $\mathcal{D}$ is said to $(l, t, \varepsilon)$-solve the decisional LWE$_{n}$ problem if

$$\left| \Pr_{\mathcal{A}, \mathcal{M}, \mathcal{B}, \mathcal{F}, e} [\mathcal{D}(A, As + e) = 1] - \Pr_{\mathcal{A}, r} [\mathcal{D}(A, r) = 1] \right| \geq \varepsilon$$

where $A \leftarrow \mathbb{Z}_q^{l \times n}$, $s \leftarrow \mathbb{Z}_q^n$, $e \leftarrow \chi^n$, $r \leftarrow \mathbb{Z}_q^l$, and the distinguisher runs in time at most $t$. 
Lemma 1.4 (Decision to Search (Lemma 3.1 from [1])) Let \( n \geq 1 \) be some integer, \( 2 \leq q \leq \text{poly}(n) \) be a prime, and...

Lemma 1.5 (Average-case to Worst-case (Lemma 3.2 from [1])) Let \( n \geq 1 \) be some integer, \( 2 \leq q \leq \text{poly}(n) \) be a prime, and...
**Parameter** The error distribution is chosen from $\Psi_{0,\alpha^2}$, where $\alpha > 0$, and is typically taken to be $1/poly(n)$. The modulus $q$ is typically taken to be $poly(n)$ (taking an exponential modulus $q$ will increase the size of the input, but make the hardness problem somewhat better understood). The number of the samples $l$ seems to be insignificant.
Basic LWE

**Definition 1.6 (Basic LWE Cryptosystem)** The basic LWE cryptosystem is a 3-tuple (BasicLWEKenGen, BasicLWEEnc, BasicLWEDec), with the parameters $n \in \mathbb{N}$, the length of the secret key, $m$, the length of ciphertext, and $\alpha \in \mathbb{R}$, the error parameter (noise parameter). All operations are performed in $\mathbb{Z}_q$. One recommended parameter choice [1] is the following. Choose $q$ to be a prime, $n^2 < q < 2n^2$, $m = 1.1 \cdot n \log q$, and $\alpha = 1/(\sqrt{n} \log^2 n)$.

- **BasicLWEKenGen()**: Choose a secret key $sk = s \in \mathbb{Z}_q^n$. The public key is $pk = (A, b)$, where $A \leftarrow \mathbb{Z}_q^{m \times n}$, $b = As + e$, $e \leftarrow \chi^l$.

- **BasicLWEEnc(pk = (A, b), d)**: To encrypt a message bit $d \in \mathbb{Z}_2$, choose $f \leftarrow \mathbb{Z}_2^m$ and output ciphertext $(u, v)$, where $u = A^T f$ and $v = \langle b, f \rangle + d \lfloor \frac{q}{2} \rfloor$.

- **BasicLPNDec(sk = s, (u, v))**: The decryption is

\[
  d' = \begin{cases} 
    0 & \text{if } v - \langle u, s \rangle \text{ is closer } 0 \text{ than to } \lfloor \frac{q}{2} \rfloor \text{ modulu } q. \\
    1 & \text{otherwise.}
  \end{cases}
\]
Note:

\[ v - \langle u, s \rangle = \langle b, f \rangle + d \lfloor \frac{q}{2} \rfloor + \langle u, s \rangle = b^T f + s^T u + d \lfloor \frac{q}{2} \rfloor = (s^T A^T + e^T) f + s^T A^T f + d \lfloor \frac{q}{2} \rfloor = e^T f + d \lfloor \frac{q}{2} \rfloor. \]

Correctness: Only need to show \( |e^T f| < \lfloor \frac{q}{4} \rfloor \) (with a high probability)...
Proof
Let $e_i$ and $f_i$ denote the entries of $e$ and $f$ respectively. Set $|f| = \sum_i f_i$, i.e. the $L^1$-norm. Then $e^T f$ is the sum of $|f|$ normal errors, since each $e_i \sim \Psi(0, \alpha q)$, then $e^T f \sim \Psi(0, \sqrt{|f|\alpha q})$.

Or, we can say $e^T f$ follows normal distribution with the standard deviation is at most $\sqrt{|f|\alpha q} < q/\log n$, a standard calculation shows that the probability that such a normal variable is greater than $q/4$ is negligible.

By Chebyshev’s inequality,

$$\Pr[|e^T f - 0| \geq \frac{q}{4}] \leq \frac{|f|\alpha^2 q^2}{\frac{q}{4}^2} \leq 4m\alpha^2$$

$\square$
2 Homomorphic LWE cryptosystem

Definition 2.1 (Homomorphic LWE Cryptosystem) The homomorphic LWE cryptosystem is a 3-tuple \((\text{HomoLWEKenGen}, \text{HomoLWEEnc}, \text{HomoLWEDec})\), with the parameters \(n \in \mathbb{N}\), the length of the secret key, \(m\), the length of ciphertext, and \(\alpha \in \mathbb{R}\), the error parameter (noise parameter). All operations are performed in \(\mathbb{Z}_q\). One recommended parameter choice [1] is the following. Choose \(q\) to be a prime, \(n^2 < q < 2n^2\), \(m = 1.1 \cdot n \log q\), and \(\alpha = 1/(\sqrt{n} \log^2 n)\).

- **HomoLWEKenGen()**: Choose a secret key \(sk = s \in \mathbb{Z}_q^n\). The public key is \(pk = (A, b)\), where \(A \leftarrow \mathbb{Z}^{m \times n}_q\), \(b = As + e\), \(e \leftarrow \chi_\alpha^l\).

- **HomoLWEEnc(pk = (A, b), d)**: To encrypt a message bit \(d \in \mathbb{Z}_2\), choose \(f \leftarrow (2\mathbb{Z})^m_4\) and output ciphertext \((u, v)\), where \(u = A^Tf\) and \(v = \langle b, f \rangle + d\).

- **HomoLPNDec(sk = s, (u, v))**: The decryption is \(d' = (v - \langle u, s \rangle) \mod 2\). 
Note:
\[ d' = v - \langle u, s \rangle = \langle b, f \rangle + d + \langle u, s \rangle = (s^T A^T + e^T)f + s^T A^T f + d = e^T f + d. \]

**Correctness**: Only need to show \( |e^T f| < q \) (with a high probability)...
3 Discussion

To be continued :)

Basic LWE
Thanks! & Questions?