Public-Key Encryption Based on LWE

Li Chen

lichen.xd at gmail.com

Xidian University

November 9, 2013

Outline

References

[1] Oded Regev. The learning with errors problem (invited survey). In *2010 25th Annual IEEE Conference on Computational Complexity*, pages 191–204. IEEE, 2010.

[2] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. In *Proceedings of the thirty-seventh annual ACM symposium on Theory of computing*, pages 84–93. ACM, 2005.

[3] Zvika Brakerski and Vinod Vaikuntanathan. Efficient fully homomorphic encryption from (standard) lwe. In *Foundations of Computer Science (FOCS), 2011 IEEE 52nd Annual Symposium on*, pages 97–106. IEEE, 2011.

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 μ and standard deviation σ (variance σ^2).
- χ denotes the distribution on $\mathbb{Z}_q$.
- Ψ_{μ,σ^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 χ on $\mathbb{Z}_q$. Let $A_{\mathbf{s},\chi} = \{(\mathbf{a}, \langle \mathbf{a}, \mathbf{s} \rangle + e)\}$ be the probability distribution on $\mathbb{Z}_q^n \times \mathbb{Z}_q$, where $\mathbf{a} \xleftarrow{\$} \mathbb{Z}_q$, $e \leftarrow \chi$, and all operations are performed in $\mathbb{Z}_q$. An algorithm $\mathcal{A}$ is saidto solve the search $\mathsf{LWE}_{n,q,\chi}$ problem if , for any $mathbfs \in \mathbb{Z}_q$, given arbitrary number of independent samples from $A_{\mathbf{s},\chi}$, it output $\mathbf{s}$ (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 χ on $\mathbb{Z}_q$. An algorithm $\mathcal{A}$ is said to (l, t, ε)-solve the search $\mathsf{LWE}_{n,q,\chi}$ problem if

$$\Pr_{\mathbf{A},\mathbf{s},\mathbf{e}}[\mathbf{s} \xleftarrow{\$} \mathcal{A}(\mathbf{A}, \mathbf{A}\mathbf{s} + \mathbf{e})] \geq \varepsilon$$

where $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{l \times n}$, $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^n$, $\mathbf{e} \leftarrow \chi^n$, 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, ε)-solve the decisional LWE$_n$ problem if

$$\left| \Pr_{\mathbf{A}, mathbfs, \mathbf{e}}[\mathcal{D}(\mathbf{A}, \mathbf{A}\mathbf{s} + \mathbf{e}) = 1] - \Pr_{\mathbf{A}, \mathbf{r}}[\mathcal{D}(\mathbf{A}, \mathbf{r}) = 1] \right| \geq \varepsilon$$

where $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{l \times n}$, $\mathbf{s} \xleftarrow{\$} \mathbb{Z}_q^n$, $\mathbf{e} \leftarrow \chi^n$, $\mathbf{r} \xleftarrow{\$} \mathbb{Z}_q^l$, 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, $2 \leq q \leq poly(n)$ be a prime, and...

Lemma 1.5 (Average-case to Worst-case (Lemma 3.2 from [1])) Let $n \geq 1$ be some integer, $2 \leq q \leq poly(n)$ be a prime, and...

Parameter The error distribution is chosen from Ψ_{0,α^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.

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 $sk = \mathbf{s} \in \mathbb{Z}_q^n$. The public key is $pk = (\mathbf{A}, \mathbf{b})$, where $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{m \times n}$, $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e}$, $\mathbf{e} \leftarrow \chi_\alpha^l$.
- BasicLWEEnc($pk = (\mathbf{A}, \mathbf{b}), d$): To encrypt a message bit $d \in \mathbb{Z}_2$, choose $\mathbf{f} \xleftarrow{\$} \mathbb{Z}_2^m$ and output cipertext $(\mathbf{u}, v)$, where $\mathbf{u} = \mathbf{A}^T \mathbf{f}$ and $v = \langle \mathbf{b}, \mathbf{f} \rangle + d \lfloor \frac{q}{2} \rfloor$.
- BasicLPNDec($sk = \mathbf{s}, (\mathbf{u}, v)$): The decryption is

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

Note:

$$\begin{aligned} v - \langle \mathbf{u}, \mathbf{s} \rangle &= \langle \mathbf{b}, \mathbf{f} \rangle + d\lfloor \tfrac{q}{2} \rfloor + \langle \mathbf{u}, \mathbf{s} \rangle \\ &= \mathbf{b}^T \mathbf{f} + \mathbf{s}^T \mathbf{u} + d\lfloor \tfrac{q}{2} \rfloor = (\mathbf{s}^T \mathbf{A}^T + \mathbf{e}^T)\mathbf{f} + \mathbf{s}^T \mathbf{A}^T \mathbf{f} + d\lfloor \tfrac{q}{2} \rfloor \\ &= \mathbf{e}^T \mathbf{f} + d\lfloor \tfrac{q}{2} \rfloor. \end{aligned}$$

Correctness: Only need to show $|\mathbf{e}^T \mathbf{f}| < \lfloor \frac{q}{4} \rfloor$ (with a high probability)...

Proof

Let e_i and f_i denote the entries of $\mathbf{e}$ and $\mathbf{f}$ respectively. Set $|f| = \sum_i f_i$, i.e. the L^1-norm. Then $\mathbf{e}^T\mathbf{f}$ is the sum of $|f|$ normal errors, since each $e_i \sim \Psi(0, \alpha q)$, then $\mathbf{e}^T\mathbf{f} \sim \Psi(0, \sqrt{|f|}\alpha q)$.

Or, we can say $\mathbf{e}^T\mathbf{f}$ 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,

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

□

2 Homomorphic LWE cryptosystem

Definition 2.1 (Homomorphic LWE Cryptosystem) The homomorphic LWE cryptosystem is a 3-tuple $(\mathsf{HomoLWEKenGen}, \mathsf{HomoLWEEnc}, \mathsf{HomoLWEDec})$, 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 $\alpha = 1/(\sqrt{n} \log^2 n)$.

- $\mathsf{HomoLWEKenGen}()$: Choose a secret key $sk = \mathbf{s} \in \mathbb{Z}_q^n$. The public key is $pk = (\mathbf{A}, \mathbf{b})$, where $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{m \times n}$, $\mathbf{b} = \mathbf{As} + \mathbf{e}$, $\mathbf{e} \leftarrow \chi_\alpha^l$.
- $\mathsf{HomoLWEEnc}(pk = (\mathbf{A}, \mathbf{b}), d)$: To encrypt a message bit $d \in \mathbb{Z}_2$, choose $\mathbf{f} \xleftarrow{\$} (2\mathbb{Z})_4^m$ and output cipertext $(\mathbf{u}, v)$, where $\mathbf{u} = \mathbf{A}^T \mathbf{f}$ and $v = \langle \mathbf{b}, \mathbf{f} \rangle + d$.
- $\mathsf{HomoLPNDec}(sk = \mathbf{s}, (\mathbf{u}, v))$: The decryption is $d' = (v - \langle \mathbf{u}, \mathbf{s} \rangle) \bmod 2$.

Note:

$$d' = v - \langle \mathbf{u}, \mathbf{s} \rangle = \langle \mathbf{b}, \mathbf{f} \rangle + d + \langle \mathbf{u}, \mathbf{s} \rangle = (\mathbf{s}^T \mathbf{A}^T + \mathbf{e}^T)\mathbf{f} + \mathbf{s}^T \mathbf{A}^T \mathbf{f} + d = \mathbf{e}^T \mathbf{f} + d.$$

Correctness: Only need to show $|\mathbf{e}^T \mathbf{f}| < q$ (with a high probability)...

3 Discussion

To be continued :)

Thanks! & Questions?