LATTICE-BASED CRYPTOGRAPHY

A.P. Komorowski[1,2]

[1]Faculty of Mathematics and Information Sciences, Warsaw University of Technology, 00-661 Warsaw, Poland
[2]National Cyber Security Centre (NCSC) Rakowiecka 2 00-909 Warszawa tel. 261865705 fax. 261865710 sekretariat.ncbc@mon.gov.pl

The Future of Standards in Cybersecurity, 2020

Who am I?

Who am I?

- Faculty of Mathematics and Information Sciences, Warsaw University of Technology

Who am I?

- Faculty of Mathematics and Information Sciences, Warsaw University of Technology
- National Cyber Security Centre

Why Lattice-based cryptography?

Why Lattice-based cryptography?

At July 22, 2020, the list of Post-Quantum Cryptography Standardization Competition Finalists were announced. There were 4 finalists in the category Public-key Encryption and Key-establishment Algorithms:

- CRYSTALS-KYBER (lattice-based),
- NTRU (lattice-based),
- SABER (lattice-based),
- Classic McEliece (code-based).

https://csrc.nist.gov/Projects/post-quantum-cryptography/round-3-submissions

Definition

Let $n, m \in \mathbb{Z}_+$, and $b_1, b_2, \ldots, b_m \in \mathbb{R}^n$- linearly independent. Then the (additive) subgroup

$$\mathcal{L}(b_1, b_2, \ldots, b_n) = \left\{ \sum_{i=0}^{n} a_i b_i \mid a_i \in \mathbb{Z} \right\}$$

of $\mathbb{R}^n$ generated by $b_1, b_2, \ldots, b_m$ is called the *lattice generated by the basis* $B = (b_1, b_2, \ldots, b_m)$.

LITERATURE:

 Raghunathan, M. S.: Discrete Subgroups of Lie Groups, Springer-Verlag Berlin Heidelberg, 1972.

 Witte-Morris, D.: Introduction to Arithmetic Groups , Deductive Press, 2015.

Norms and distances

Assume that there is a norm $\| \cdot \| \colon \mathbb{R}^n \to [0, \infty)$ defined on vector space $\mathbb{R}^n$.
A norm induces the distance $d : \mathbb{R}^n \times \mathbb{R}^n \to [0, \infty)$ by

$$d(x, y) = \| x - y \| .$$

Norms and distances

Assume that there is a norm $\| \cdot \|: \mathbb{R}^n \to [0, \infty)$ defined on vector space $\mathbb{R}^n$.
A norm induces the distance $d : \mathbb{R}^n \times \mathbb{R}^n \to [0, \infty)$ by

$$d(x, y) = \| x - y \| .$$

In general, to construct a lattice based-cryptosystem we can take any norm. In practice, most cryptosystems use the Euclidean norm $\| \cdot \|_2$.

Lattice problems - SVP/CVP

Shortest Vector Problem, SVP

Let $\mathcal{L}$ be a lattice. Find a nonzero vector $y \in \mathcal{L}$, such that $\| y \| \leq \| x \|$ for $x \in \mathcal{L} \setminus \{\mathbf{0}\}$.

Closest Vector Problem, CVP

Let $\mathcal{L}$ be a lattice and $t \in \mathcal{L}$. Find a vector $y \in \mathcal{L}$, such that $\| y - t \| \leq \| x - t \|$ for $x \in \mathcal{L} \setminus \{t\}$ and $y \neq t$.

Lattice problems - Decision SVP/CVP

Let $r \in \mathbb{R}$ with $r > 0$ be given.

Decision SVP

Let $\mathcal{L}$ be a lattice. Decide whether there exists a nonzero vector $y \in \mathcal{L}$, such that $\| y \| \leq r$.

Decision CVP

Let $\mathcal{L}$ be a lattice and $t \in \mathcal{L}$. Decide whether there exists a vector $y \in \mathcal{L}$ different than t, such that $\| y - t \| \leq r$.

Lattice problems - Approximate SVP/CVP

Let $\gamma \in \mathbb{R}$ with $\gamma \geq 1$.

γ-Approximate SVP

Let $\mathcal{L}$ be a lattice. Find a nonzero vector $y \in \mathcal{L}$, such that $\| y \| \leq \gamma \| x \|$ for $x \in \mathcal{L} \setminus \{\mathbf{0}\}$.

γ-Approximate CVP

Let $\mathcal{L}$ be a lattice and $t \in \mathcal{L}$. Find a nonzero vector $y \in \mathcal{L}$, such that $\| y - t \| \leq \gamma \| x - t \|$ for $x \in \mathcal{L} \setminus \{\mathbf{0}\}$.

Lattice problems - LWE

Learning With Errors, LWE

Let $A \in \mathbb{R}^{m \times n}$, $b \in \mathbb{R}^m$ and a distribution χ over $\mathbb{R}^m$ be known. Find $s \in \mathbb{Z}^n$ such that

$$A \cdot s + e = b,$$

where $e \sim \chi$.

Lattice problems - LWE

Learning With Errors, LWE

Let $A \in \mathbb{R}^{m \times n}$, $b \in \mathbb{R}^m$ and a distribution χ over $\mathbb{R}^m$ be known. Find $s \in \mathbb{Z}^n$ such that

$$A \cdot s + e = b,$$

where $e \sim \chi$.

Usually in cryptography, $A \in \mathbb{Z}_p^{m \times n}$, $b \in \mathbb{Z}_p^m$, $s \in \mathbb{Z}^n$ and χ is a "normal" distribution over $\mathbb{Z}_p^m$.

LITERATURE:


Blum, A., Kalai, A. and Wasserman, H.: Noise-tolerant learning, the parity problem, and the statistical query model, Journal of the ACM, 50(4), 2003, 506–519


Regev, O.: On lattices, learning with errors, random linear codes, and cryptography, In Proc. 37th ACM Symp. on Theory of Computing (STOC), 2005, 84–93


Angluin, D. and Laird, P.: Learning from noisy examples, Machine Learning, 2(4), 1988, 343–370

Lattice problems - LWR

Learning With Rounding, LWR

Let $A \in \mathbb{R}^{m \times n}$, $b \in \mathbb{Z}^m$ be known. Find $s \in \mathbb{Z}^n$ such that

$$\lfloor A \cdot s \rceil_p = b,$$

where $\lfloor [a_{ij}] \rceil_p \equiv [(\lfloor a_{ij} \rceil \mod p)]$.

Usually in cryptography, $A \in \mathbb{Z}_q^{m \times n}$, $b \in \mathbb{Z}_q^m$ and $s \in \mathbb{Z}_q^n$.
Note that LWR problem is a special case of LWE problem.
LITERATURE:

Banerjee, A., Peikert, C., and Rosen, A.: Pseudorandom Functions and Lattices, In: Advances in Cryptology EUROCRYPT 2012, 2012, 719737

NTRU

NTRU is a Public Key Cryptosystem connected with the SVP-problem on lattices.
Let $N, p, q \in \mathbb{Z}$ with $\gcd(p, q) = 1$ and $q > p$.
Let $R = \mathbb{Z}[X]/(X^N - 1)$. Let $\star$ denote the multiplining in R. Note that if

$$(\sum_{i=0}^{N-1} F_i x^i) \star (\sum_{i=0}^{N-1} G_i x^i) = \sum_{i=0}^{N-1} H_i x^i,$$

then

$$H_k = \sum_{(i,j):i+j \equiv k \mod N} F_i G_j.$$

LITERATURE:

Banerjee, A., Peikert, C., and Rosen, A.: NTRU: A Ring-Based Public Key Cryptosystem, In: Algorithmic Number Theory. Vol. 1423, 1998, 267–288

NTRU - Parameters, Public/Private key

Par N, p, q.

Prkey $(f, g) \in R^2$, such that there exist $F_p, F_q \in R$, such that

$$F_p \star f \equiv 1 \mod p \text{ and } F_q \star f \equiv 1 \mod q.$$

Pubkey

$$h :\equiv F_q \star g \mod q$$

LITERATURE:


Banerjee, A., Peikert, C., and Rosen, A.: NTRU: A new high-speed public key cryptosystem, Manuscript circulated at CRYPTO 1996 rump session, 1996


Banerjee, A., Peikert, C., and Rosen, A.: NTRU: A Ring-Based Public Key Cryptosystem, In: Algorithmic Number Theory. Vol. 1423, 1998, 267–288

NTRU - Encryption/Decryption

Mes $m \in R$ with coefficients $a_i < p$.

Enc Let $r \in R$ be randomly chosen. The ciphertext is defined as

$$c :\equiv (pr) \star h + m \mod q$$

Dec Compute

$$a \equiv f \star c \mod q,$$

to decrypt the message compute

$$m \equiv F_p \star a \mod p.$$

LITERATURE:


Banerjee, A., Peikert, C., and Rosen, A.: NTRU: A new high-speed public key cryptosystem, Manuscript circulated at CRYPTO 1996 rump session, 1996


Banerjee, A., Peikert, C., and Rosen, A.: NTRU: A Ring-Based Public Key Cryptosystem, In: Algorithmic Number Theory. Vol. 1423, 1998, 267–288

NTRU - Why NTRU works?

- $\star$ is associative, commutative and distributive over addition $+$.

NTRU - Why NTRU works?

$\star$ is associative, commutative and distributive over addition $+$.

$$\begin{aligned} a &\equiv f \star c \pmod q \equiv f \star (pr) \star h + f \star m \pmod q \\ &\equiv f \star (pr) \star F_q \star g + f \star m \pmod q \\ &\equiv (pr) \star g + f \star m \pmod q \end{aligned}$$

NTRU - Why NTRU works?

$\star$ is associative, commutative and distributive over addition $+$.

$$\begin{aligned} a &\equiv f \star c \pmod q \equiv f \star (pr) \star h + f \star m \pmod q \\ &\equiv f \star (pr) \star F_q \star g + f \star m \pmod q \\ &\equiv (pr) \star g + f \star m \pmod q \end{aligned}$$

If we choose proper p and q, then we can assume that $|(pr) \star g + f \star m| \leq q$.

NTRU - Why NTRU works?

$\star$ is associative, commutative and distributive over addition $+$.

$$\begin{aligned} a &\equiv f \star c(\mod q) \equiv f \star (pr) \star h + f \star m \mod q \\ &\equiv f \star (pr) \star F_q \star g + f \star m \mod q \\ &\equiv (pr) \star g + f \star m \mod q \end{aligned}$$

If we choose proper p and q, then we can assume that $|(pr) \star g + f \star m| \leq q$.

$$F_p \star a(\mod p) \equiv F_p \star (pr) \star g + F_p \star f \star m(\mod p) \equiv m$$

LITERATURE:


Banerjee, A., Peikert, C., and Rosen, A.: NTRU: A new high-speed public key cryptosystem, Manuscript circulated at CRYPTO 1996 rump session, 1996


Banerjee, A., Peikert, C., and Rosen, A.: NTRU: A Ring-Based Public Key Cryptosystem, In: Algorithmic Number Theory. Vol. 1423, 1998, 267–288

LWE-based general cryptosystems

Par $n, m, l, t, r, q \in \mathbb{Z}$, an distribution χ over $\mathbb{Z}^{m \times l}$.
Let

$$f : \mathbb{Z}_t^l \to \mathbb{Z}_t^q, (v_1, v_2, \ldots, v_t) \mapsto (\lfloor qv_1/l \rceil, \lfloor qv_2/l \rceil, \ldots, \lfloor qv_t/l \rceil)$$

$$f^{-1} : \mathbb{Z}_t^q \to \mathbb{Z}_t^l, (v_1, v_2, \ldots, v_t) \mapsto (\lfloor lv_1/q \rceil, \lfloor lv_2/q \rceil, \ldots, \lfloor lv_t/q \rceil)$$

PrKey A matrix $S \in \mathbb{Z}_q^{n \times l}$,

PubKey Let $A \in \mathbb{Z}^{m \times n}$ and $E \in \mathbb{Z}^{m \times l}$ with $E \sim \chi$. The public key is the pair

$$(A, P = AS + E) \in \mathbb{Z}^{m \times n} \times \mathbb{Z}^{m \times l}.$$

Mes $m \in \mathbb{Z}_t^l$.

LITERATURE:


Regev, O.: On lattices, learning with errors, random linear codes, and cryptography, In Proc. 37th ACM Symp. on Theory of Computing (STOC), 2005, pages 84–93


Peikert, C., Vaikuntanathan V., and Waters B.: A framework for efficient and composable oblivious transfer, In Advances in Cryptology (CRYPTO), LNCS. Springer, 2008

LWE-based general cryptosystems

Enc Choose $a \in \{-r, -r+1, \ldots, r\}^m$ uniformly at random. The ciphertext is a pair

$$(u, c) = (A^T a, P^T a + f(m)) \in \mathbb{Z}_q^n \times \mathbb{Z}_q^l.$$

Dec Output

$$m' = f^{-1}(c - S^T u).$$

LWE-based general cryptosystems

Enc Choose $a \in \{-r, -r+1, \ldots, r\}^m$ uniformly at random. The ciphertext is a pair

$$(u, c) = (A^T a, P^T a + f(m)) \in \mathbb{Z}_q^n \times \mathbb{Z}_q^l.$$

Dec Output

$$m' = f^{-1}(c - S^T u).$$

Note that sometimes $m = Dec(Enc(m))$ does not hold. A probability of such situation should be low in good LWE-based cryptosystems.

LITERATURE:


Regev, O.: On lattices, learning with errors, random linear codes, and cryptography, In Proc. 37th ACM Symp. on Theory of Computing (STOC), 2005, pages 84–93


Peikert, C., Vaikuntanathan V., and Waters B.: A framework for efficient and composable oblivious transfer, In Advances in Cryptology (CRYPTO), LNCS. Springer, 2008

CRYSTALS Kyber, Parametrs and keys

Let $R = \mathbb{Z}[x]/(x^{256}+1)$, $R_q = \mathbb{Z}_q[x]/(x^{256}+1)$

$$Com : R \times \mathbb{Z}_+ \times \mathbb{Z}_+ \to R_d; (x, d, q) \mapsto \lfloor (d/q)x \rceil (\mod d)$$

$$DeCom : R \times \mathbb{Z}_+ \times \mathbb{Z}_+ \to R_q; (x, d, q) \mapsto \lfloor (q/d)x \rceil (\mod q)$$

Par k, q, d_t, d_U, d_v- positive integers, an binomial distribution χ on $\mathbb{Z}$.

PrKey Let $A \in R_q^{k \times k}$, Let $S, E \in R^k$ with each coefficient generated according to χ. The Private Key is S.

PubKey $(P = Com(AS + E, 2^{d_t}, q), A) \in R_{2^d} \times R_q^{k \times k}$.

Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J.M., Schwabe, P., Seiler, G., and Stehl, D.: CRYSTALS Kyber: a CCA-secure module-lattice-based KEM, 2018 IEEE European Symposium on Security and Privacy, EuroSP 2018, 2018

CRYSTALS Kyber, Encryption and Decryption

Mes $m \in R_q$, represented as an polynomial with coefficients in $\{0, 1\}$.

Enc Choose $r, e_1 \in R^k$ with each coefficient generated according to χ and $e_2 \in R$ chosen according to χ. Let

$$t = DeCom(P, d_t, q).$$

Then the ciphertext is a pair

$$(U = Com(A^T r + e_1, 2^{d_U}, q), v = Com(t^T r + e_2 + \lfloor q/2 \rceil m, 2^{d_v}, q))$$

Dec Output

$$m' = Com(DeCom(v, 2^{d_v}, q) - S \cdot DeCom(U, 2^{d_U}, q), 2, q)$$

Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J.M., Schwabe, P., Seiler, G., and Stehl, D.: CRYSTALS Kyber: a CCA-secure module-lattice-based KEM, 2018 IEEE European Symposium on Security and Privacy, EuroSP 2018, 2018

SABER

Let $R = \mathbb{Z}[x]/(x^{256}+1), R_q = \mathbb{Z}_q[x]/(x^{256}+1)$.

Par l, q, t- positive integers, an binomial distribution χ over R, constant vector $h \in R_q^l$, $h_1 \in R_q$.

PrKey A vector $S \in R_q^l$, with each coefficient generated according to χ,

PubKey Let $A \in R_q^{l \times l}$. The public key is the pair

$$(A, P = Com(AS + h, p, q)) \in R_q^{l \times l} \times R_p^k.$$

DAnvers, J-P., Sujoy Sinha Roy, A.K. and Vercauteren, F.: Saber: Module-LWR based key exchange, CPA-secure encryption and CCA-secure KEM, IACR Cryptol. ePrint Arch., 2018, pages 84–93

SABER

Mes $m \in R_q$, represented as an polynomial with coefficients in $\{0, 1\}$.

Enc Choose $S' \in R_q^k$ with each coefficient generated according to χ. Let

$$P' = Com(AS' + h, p, q) \in R_p^k$$

Then the ciphertext is a pair

$$(v = Com({P'}^T S' + h_1 + \frac{p}{2}m, 2t, p), P') \in R_{2t} \times R_p^k.$$

Dec Output

$$m' = Com({P'}^T S' + h_1 + \frac{p}{2}m, 2, p) \in R_2$$

DAnvers, J-P., Sujoy Sinha Roy, A.K. and Vercauteren, F.: Saber: Module-LWR based key exchange, CPA-secure encryption and CCA-secure KEM, IACR Cryptol. ePrint Arch., 2018, pages 84–93

LITERATURE


Angluin, D. and Laird, P.: Learning from noisy examples, Machine Learning, 2(4), 1988, 343–370


Banerjee, A., Peikert, C., and Rosen, A.: NTRU: A new high-speed public key cryptosystem, Manuscript circulated at CRYPTO 1996 rump session, 1996


Blum, A., Kalai, A. and Wasserman, H.: Noise-tolerant learning, the parity problem, and the statistical query model, Journal of the ACM, 50(4), 2003, 506–519


Bos, J., Ducas, L., Kiltz, E., Lepoint, T., Lyubashevsky, V., Schanck, J.M., Schwabe, P., Seiler, G., and Stehl, D.: CRYSTALS Kyber: a CCA-secure module-lattice-based KEM, 2018 IEEE European Symposium on Security and Privacy, EuroSP 2018, 2018


DAnvers, J-P., Sujoy Sinha Roy, A.K. and Vercauteren, F.: Saber: Module-LWR based key exchange, CPA-secure encryption and CCA-secure KEM, IACR Cryptol. ePrint Arch., 2018, pages 84–93


Micciancio D., Regev, O.: Lattice-based Cryptography, In Post-Quantum Cryptography, Springer, Berlin, Heidelberg 2009, pages 147–191


Peikert, C., Vaikuntanathan V., and Waters B.: A framework for efficient and composable oblivious transfer, In Advances in Cryptology (CRYPTO), LNCS. Springer, 2008


Raghunathan, M. S.: Discrete Subgroups of Lie Groups, Springer-Verlag Berlin Heidelberg, 1972.


Regev, O.: On lattices, learning with errors, random linear codes, and cryptography, In Proc. 37th ACM Symp. on Theory of Computing (STOC), 2005, pages 84–93


Witte-Morris, D.: Introduction to Arithmetic Groups , Deductive Press, 2015.

The End

Thank you!