Computational problems in lattice-based cryptography

Steven Galbraith



University of Auckland, New Zealand

Plan

- LWE/(I)SIS and modulus switching
- Approximate GCD
- Homomorphic encryption
- Lattices
- Multi-linear maps

Please ask questions at any time.

AsiaCrypt 2015

November 29-December 3, 2015

Auckland, New Zealand

Lattice-based cryptography

Lattice-based cryptography refers to any system whose security depends on computational assumptions based on lattices (in contrast to factoring-based cryptography, discrete-logarithm based cryptography, etc).

Some achievements:

- Fully homomorphic encryption
- Multilinear maps and iO
- Attribute-based encryption for general circuits
- Cryptography based on worst-case assumptions
- Security against quantum computers (hopefully)

LWE and (I)SIS

- Let $m, n \in \mathbb{N}$ with $m > n$.
- Fix a distribution $\mathcal{D} \subseteq \mathbb{Z}^m$.
  Maybe uniform distribution on $\{0, 1\}^n$, or discrete Gaussian distribution.
- Let q be some modulus (often a prime).
- LWE (Regev): Given $(\mathbf{A}, \mathbf{b})$ where $\mathbf{A}$ is an $m \times n$ matrix to find $(\mathbf{s}, \mathbf{e}) \in \mathbb{Z}^n \times \mathbb{Z}^m$, if they exist, such that $\mathbf{e}$ is a likely sample from $\mathcal{D}$ and $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} \pmod{q}$.
- (I)SIS (Ajtai): Given $(\mathbf{A}, \mathbf{b})$ where $\mathbf{A}$ is an $n \times m$ matrix to find $\mathbf{x}$ (if it exists) that is a likely sample from $\mathcal{D}$ such that $\mathbf{b} = \mathbf{A}\mathbf{x} \pmod{q}$.
  This is the "inhomogeneous SIS problem" ISIS.
  SIS is the case $\mathbf{b} = \mathbf{0}, \mathbf{x} \neq \mathbf{0}$.

LWE and (I)SIS

- There are also decisional variants of these problems: Given $(\mathbf{A}, \mathbf{b})$ to decide whether or not a solution exists.
- LWE is usually considered in the "low density" case when there is a unique solution $(\mathbf{s}, \mathbf{e})$.
- (I)SIS is usually considered in the "high density" case, when there is more than one solution.
- LWE can be converted to the case where the vector $\mathbf{s}$ is also chosen from $\mathcal{D}$.
- Once $\mathbf{s}$ is a "small vector" one can re-write LWE as (low density) ISIS by writing

$$\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} = (\mathbf{A}|\mathbf{I}_m)\begin{pmatrix} \mathbf{s} \\ \mathbf{e} \end{pmatrix}.$$

LWE and (I)SIS

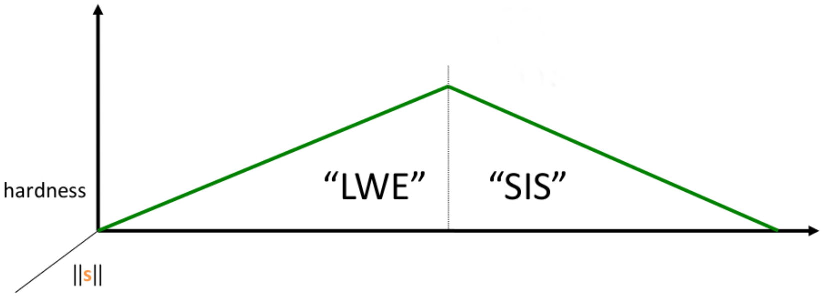

Image by Vadim Lyubashevsky

Modulus switching

- Suppose $\mathbf{b} = \mathbf{A}\mathbf{s} + \mathbf{e} + q\mathbf{k}$ with $\mathbf{s}$ short.
- Let q' be another modulus and set $\mathbf{b}' = [\frac{q'}{q}\mathbf{b}]$, $\mathbf{A}' = [\frac{q'}{q}\mathbf{A}]$. Then
$$\mathbf{b}' = \mathbf{A}'\mathbf{s} + \mathbf{e}' + q'\mathbf{k}$$
for some "short" vector $\mathbf{e}'$.
- Hence modulus switching turns LWE modulo q into LWE modulo q'.
- One can do a similar thing for ISIS by converting ISIS to LWE, doing modulus switching, and converting back. But it does not necessarily preserve binary vectors.
- Modulus switching tends to make LWE harder.

Algorithms for LWE/(I)SIS

- Lattice reduction/CVP algorithms are best in practice. See: Lindner-Peikert, Chen-Nguyen, Liu-Nguyen, Albrecht-Fitzpatrick-Göpfert.
  For case when secret is a binary vector, Bai-Galbraith gives improved lattice algorithm (ACISP 2014).
- Blum-Kalai-Wasserman is best in theory: subexponential but needs many samples.
  It can be viewed as a variant of the Goldreich-Levin/ Kushilevitz-Mansour Fourier learning algorithm.
  Lyubashevsky shows number of samples can be $O(n^{1+\epsilon})$.
- For (I)SIS when m very large and and $\mathcal{D} = \{0, 1\}^n$, can use combinatorial algorithms (Wagner's algorithm or Becker-Coron-Joux).
  See Bai-Galbraith-Li-Sheffield (eprint 2014/593).

Symmetric encryption from approximate GCD

(van Dijk, Gentry, Halevi and Vaikuntanathan, 2010)

- Let p be large prime, known to Alice and Bob.
- To encrypt $\mathfrak{m} \in \{0, 1\}$ to Bob, Alice does:
  - Choose $q, e \in \mathbb{Z}$ with $|e| \ll p$ and q large.
  - Compute $\mathsf{c} = pq + 2e + \mathfrak{m}$, and send to Bob.
- To decrypt c Bob does
  - $\mathfrak{m} = [[\mathsf{c}]_p]_2$.
- Here $[\mathsf{c}]_p$ denotes the integer in $(-p/2, p/2]$ congruent modulo p to c.

The approximate GCD problem

- Suppose Eve sees many communications between Alice and Bob.
- She sees $\mathsf{c}_i = pq_i + (2e_i + \mathfrak{m}_i)$ for $1 \leq i \leq k$.
- One of her goals might be to compute p, and hence read all messages.
- Approx-GCD problem: Given many samples $pq_i + e_i$ where e_i is "small" relative to p, to compute p.

Homomorphic encryption

- A nice feature of this system is that it is homomorphic.
- Let $\mathsf{c}_1 = pq_1 + 2e_1 + \mathfrak{m}_1$ and $\mathsf{c}_2 = pq_2 + 2e_2 + \mathfrak{m}_2$.
- Then $\mathsf{c}_1 + \mathsf{c}_2 = p(q_1 + q_2) + 2(e_1 + e_2) + (\mathfrak{m}_1 + \mathfrak{m}_2)$ is an encryption of $\mathfrak{m}_1 + \mathfrak{m}_2 \pmod{2}$.
- Also, $\mathsf{c}_1\mathsf{c}_2 = p(\star) + 2(e_1e_2 + e_1\mathfrak{m}_2 + e_2\mathfrak{m}_1) + (\mathfrak{m}_1\mathfrak{m}_2)$ is an encryption of $\mathfrak{m}_1\mathfrak{m}_2 \pmod{2}$.

Can turn into a public key encryption scheme

- Bob publishes many encryptions of zero $X_i = pq_i + 2e_i$, $1 \leq i \leq k$.
- To encrypt to Bob, Alice chooses $I \subseteq \{1, 2, \ldots, k\}$ and computes
$$\mathsf{c} = \sum_{i \in I} X_i \quad + 2e + \mathfrak{m}$$
and sends c to Bob.
- Full security analysis given by van Dijk, Gentry, Halevi and Vaikuntanathan.
- Variant where $X_0 = pq_0$ is also given in public key, and computations are modulo X_0.
- (ρ, η, γ)-Approximate GCD problem: Given $X_1, \ldots,$ $X_k \in \mathbb{Z} \cap [0, 2^\gamma]$ find an integer $2^{\eta-1} < p < 2^\eta$ such that $[X_i]_p < 2^\rho$ for all $1 \leq i \leq k$.
In what sense is this well-defined?

Euclid algorithm on approx-GCD

- Given $X_1 = pq_1 + e_1, X_2 = pq_2 + e_2$ one can run Euclid's algorithm.
- Since Euclid considers most-significant bits first, the algorithm will begin the same as if one was computing $\gcd(pq_1, pq_2)$.
- Euclid on (a, b) computes a sequence (r_i, s_i, t_i) such that $r_i = as_i + bt_i$ and $|r_i s_i| \approx |b|, |r_i t_i| \approx |a|$.
- Run Euclid on (pq_1, pq_2) we expect to get $r_i = p$ and $q_1 s_i + q_2 t_i = 1$.
- This means $s_i, t_i \approx q_2, q_1$ and so

  $$X_1 s_i + X_2 t_i = p(q_1 s_i + q_2 t_i) + (e_1 s_i + e_2 t_i).$$

  As long as $|e_1 s_i - e_2 t_i| \gg p$ then Euclid does not find p.
  Hence, if $\gamma - \eta + \rho \gg \eta$ then Euclid is not useful.
  Another way to write this condition: $q_i e_i \gg p$.
- Howgrave-Graham has also worked on this problem.

Adaptive attacks

- It is standard (and realistic) in crypto to consider the setting where an attacker has access to a decryption oracle.
- Recall that decryption of ciphertext c computes $\mathfrak{m} = [[\mathrm{c}]_p]_2$.
  Query decryption oracle on even integers $c \approx p/2$.
  If c is even then $c < p/2 \implies [[c]_p]_2 = 0$, while $p/2 < c < p \implies [[c]_p]_2 = 1$.
  Hence determine secret key p by binary search.
- The security notion we would like is called "IND-CCA1".
- Problem: To design an IND-CCA1 variant of this scheme.
- Similar attacks on all homomorphic encryption schemes except Loftus, May, Smart and Vercauteren IND-CCA1 scheme.
- Micciancio and Peikert (EUROCRYPT 2012) have IND-CCA1 encryption from LWE, but not homomorphic.
- This conference has a talk on CCA-secure FHE.

Lattices

- Let $\mathbf{b}_1, \dots, \mathbf{b}_n$ be linearly independent vectors in $\mathbb{R}^n$.
- The set $L = \{\sum_{i=1}^{n} x_i \mathbf{b}_i : x_i \in \mathbb{Z}\}$ is a (full rank) lattice. Call its elements **points** or **vectors**.
- Alternative definition: A discrete subgroup of $\mathbb{R}^n$.
- Everyone working with lattices should declare whether their vectors are **rows** or **columns**.
  Today I am using **rows**.
- The **basis matrix** is the $n \times n$ matrix $\mathbf{B}$ whose rows are the vectors $\mathbf{b}_1, \dots, \mathbf{b}_n$.
- A lattice has many different bases.

Computational Problems (Informally)

- Shortest vector problem (SVP): Given a basis matrix $\mathbf{B}$ for a lattice L find a non-zero vector $\mathbf{v} \in L$ such that $\|\mathbf{v}\|$ is minimal. The norm here is usually the standard Euclidean norm in $\mathbb{R}^n$, but it can be any norm such as the ℓ_1 norm or ℓ_∞ norm.
- Closest vector problem (CVP): Given a basis matrix $\mathbf{B}$ for a full rank lattice $L \subseteq \mathbb{R}^n$ and an element $\mathbf{t} \in \mathbb{R}^n$ find $\mathbf{v} \in L$ such that $\|\mathbf{v} - \mathbf{t}\|$ is minimal.

Lattice attack on approx GCD

- Recall $X_i = pq_i + e_i$.
- Consider the lattice whose rows are spanned by

$$\mathbf{B} = \begin{pmatrix} 2^{\rho} & -X_2 & -X_3 & \cdots & -X_t \\ 0 & X_1 & 0 & \cdots & 0 \\ 0 & 0 & X_1 & & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & X_1 \end{pmatrix}.$$

- Note that

$$(q_1, q_2, \ldots, q_t)\mathbf{B} = (2^{\rho} q_1, e_1 q_2 - e_2 q_1, \ldots, e_1 q_t - e_t q_1)$$

is of length $\sqrt{t} 2^{\rho+\gamma-\eta}$.

Lattice attack on approx GCD

- The Gaussian heuristic suggests the lattice contains a vector of length

$$\sqrt{\frac{t}{2\pi e}}\det(\mathbf{B})^{1/t} \approx \sqrt{\frac{t}{2\pi e}} 2^{(\rho+(t-1)\gamma)/t}.$$

- So for large enough t then the target vector is especially short and might be found using lattice reduction.

Other research

- Also attacks by: Chen-Nguyen; Coron, Naccache and Tibouchi; Cohn-Heninger.
  These attacks show that the errors (hence, parameter ρ) cannot be too small.
- But mainly the security comes from the size of the q_i rather than the size of the errors.
- The suggested parameters make the scheme astronomically large: X_i has λ^5 bits while p has λ^2 bits.
- In the case $X_0 = pq_0$, elliptic curve factoring method finds p in $e^{(c+o(1))\lambda} = L_{X_0}(\frac{1}{5}, c + o(1))$ bit operations.
- Problem: Find an attack that works when q very large.

Multi-linear maps

- Coron, Lepoint and Tibouchi have given a multi-linear map based on somewhat similar ideas.
- It is too complicated to write down in this talk.
- Cheon, Han, Lee, Ryu and Stehlé (EUROCRYPT 2015; eprint 2014/906) have broken it.
  (As long as low-level encodings of zero are public.)
- There were two "fixes" that are already broken.
- Coron, Lepoint and Tibouchi have proposed a new "fix" (eprint 2015/162)
- Is the fix secure?
- Also some work by Lee and Seo (CRYPTO 2014).

NTRU/Ring-LWE – History

- NTRU: Hoffstein, Pipher, Silverman (ANTS 1998).
- Rejuvinated by Stehlé and Steinfeld; Lopez-Alt, Tromer and Vaikuntanathan
- Ring-LWE: Lyubashevsky, Peikert and Regev

Some applications of Ring-LWE/NTRU

- Lopez-Alt, Tromer and Vaikuntanathan have given a homomorphic encryption scheme based on NTRU.
- Brakerski, Gentry and Vaikuntanathan have given homomorphic encryption based on LWE/Ring-LWE.
- Lyubashevsky has given efficient public key signatures based on Ring-LWE and NTRU.
  Efficient signatures: Güneysu-Lyubashevsky-Pöppelmann (CHES 2012); Ducas-Durmus-Lepoint-Lyubashevsky (CRYPTO 2013).

Multilinear maps (Garg, Gentry, Halevi 2013)

- A pairing is a non-degenerate, bilinear map $e : G_1 \times G_2 \to G_3$.
- Typically constructed out of the Weil or Tate-Lichtenbaum pairing on elliptic curves.
- It would be interesting to have a non-degenerate multilinear map $e : G_1 \times G_2 \times \cdots \times G_k \to G_{k+1}$.
- We can't really do that yet, but there is something slightly analogous.
- The one-way function $g \to g^x$ is replaced by "randomised encodings" a of random elements x.
- The "multilinear map" is essentially a homomorphic multiplication of these encodings, followed by an operation that "deterministically extracts some bits" from the product.

Multilinear maps (Garg, Gentry, Halevi 2013)

- Let g be a short vector, defining a principal ideal $I = (g)$ in $R_q = \mathbb{Z}_q[x]/(x^n + 1)$. Also need g invertible and g^{-1} short.
- $z \in R_q$ is random and invertible.
- Public key includes $y = (1 + gr)/z$, $x_i = gb_i/z$, and $p_{\mathrm{zt}} = hz^k/g$, where r, b_i are short and h is medium size.
- To generate "random exponent" one chooses a short vector d in R_q.
- To generate a "randomised (level one) encoding of x" one computes

$$\begin{aligned} u &= dy + \sum_i r_i x_i \\ &= (d + g(r + \sum_i r_i b_i))/z = (d \pmod{(g)} + g \cdot \mathrm{small})/z. \end{aligned}$$

- Idea: It is hard to determine d given u.

Multilinear maps (Garg, Gentry, Halevi 2013)

- Given randomized (level one) encodings $u_1, \dots, u_k$ all of the form $(d_i + g \cdot \text{small})/z$ one computes

$$u = u_1 \cdots u_k = (d_1 \cdots d_k + g \cdot \text{smallish})/z^k.$$

- We call this "level k".
- Now, recall $p_{\text{zt}} = hz^k/g$, so

$$up_{\text{zt}} = (d_1 \cdots d_k)(h/g) + h \cdot \text{smallish}.$$

- Since (h/g) is a constant and $h \cdot$ smallish is smallish too, the most significant bits of the representation of up_{zt} depend only on $d_1 \cdots d_k$.

Security of GGH multilinear maps

- Spectacular cryptanalysis by Yupu Hu and Huiwen Jia (eprint 2015/301).
- GGH may still be used safely(?) in applications like *iO* where encodings of zero are not made public.
- Is there a "fix" for GGH?
- Are there other attacks on GGH?
- Cramer-Ducas-Peikert-Regev (building on ideas of Bernstein and Campbell-Groves-Shepherd) show how to compute very short generator g of principal ideal I if it exists.

Differences with pairings

- For pairings, the "encoding" is $d \to g^d$, which is a one-way function (both phrases important here!)
- For GGH the encoding is $d \to dy$, which is not one-way, unless one adds extra randomisation in which case it is not a function.
- Pairings give a group homomorphism from one group to another, typically $E(\mathbb{F}_q) \to \mathbb{F}_{q^k}^*$.
- GGH gives an "algebraic map" (multiplication of ring elements) followed by a non-algebraic map (extraction of most significant bits).

Differences with pairings

- Boneh and Silverberg "explained" why cannot get multilinear maps from algebraic geometry.
- But their result is about "ideal" multilinear maps.
  It does not apply to randomised encodings and zero-testing.
- So is there a way to get randomised encodings and zero-testing from RSA or ECC?

Conclusions and advice

- Lattice-based crypto is a very hot topic.
- Young researchers must learn about lattice-based crypto.
- There are many open problems.
- For example, I expect further algorithmic improvements for: approx-GCD, Ring-LWE, homomorphic encryption, multilinear maps.
- There are very few experts in lattice cryptography. I recommend you to send your paper to the experts for their advice before submitting to a conference or journal.
- And put your papers on eprint.

Thank You