Mastermath, Spring 2018
Intro to Lattice Algs & Crypto

Lecture 9

Lecturers: D. Dadush, L. Ducas
Scribe: K. de Boer

03/04/18

1 Introduction

In this lecture we cover basic cryptographic notions (Collision-resistante function, One-way function), and show how to construct such functions from a lattice problem, namely from the Short-Integer-Solution problem (SIS), which is a instantiation of the Approx-SVP problem on a specific class of random lattices.

2 Lattices used in cryptography

In these notes, we settle the following notation. We denote by q a number in $\mathbb{N}$. This number q is often required to be a prime or a prime power. We denote by $\mathbb{Z}_q = \mathbb{Z}/q\mathbb{Z}$, the integers modulo q. The variables $m, n \in \mathbb{N}$ will denote dimensions of matrices; in this lecture notes, m is associated with the number of variables and n is associated with the number of equations. In the subsequent sections, we assume $m \geq n \geq 0$.

Definition 1 (q-ary lattices) *A q-ary lattice Λ of dimension m is a lattice satisfying*

$$q\mathbb{Z}^m \subseteq \Lambda \subseteq \mathbb{Z}^m.$$

Algebraically and computationnally, one can think of a q-ary lattice as a subgroup of $\mathbb{Z}_q^m$: the inclusion of a point $\mathbf{x} \in \mathbb{Z}^m$ in a q-ary lattice only depends on $\mathbf{x}$ mod q. Yet, and in constract with q-ary codes, it is important to also consider the non-reduced value of $\mathbf{x} \in \mathbb{Z}^m$ to have a notion of Euclidean length.

Exercise 1 Show that there is a one-to-one correspondence between q-ary lattices Λ of dimension m and subgroups of $\mathbb{Z}_q^m$.

The following (q-ary) lattice bears the name 'parity check lattice', a name descending from coding-theory.

Definition 2 (Parity check lattice) *Let $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ be a matrix with coefficients in $\mathbb{Z}_q$. Define*

$$\Lambda_q^\perp(\mathbf{A}) = \{\mathbf{x} \in \mathbb{Z}^m \mid \mathbf{A}\mathbf{x} = 0 \textit{ mod } q\} \quad (= \ker(\mathbf{A} : \mathbb{Z}_q \to \mathbb{Z}_q^n)).$$

Technically, explicting the "mod q" is not required in the above definition, but is included as a helpful reminder to the reader: $\mathbb{Z}_q$ is $\mathbb{Z}$-module, so the product $\mathbf{A}\mathbf{x}$ is well defined, and belong to $\mathbb{Z}_q^n$.

Definition 3 (Row-generated lattice) *Let $\mathbf{A} \in \mathbb{Z}_q^{m\times n}$. Define*

$$\Lambda_q(\mathbf{A}) = \{\mathbf{y} \in \mathbb{Z}^m \mid y = \mathbf{A}\mathbf{s} \textit{ mod } q, \textit{ for some } \mathbf{s} \in \mathbb{Z}^n\} = \mathbf{A}\mathbb{Z}^n + q\mathbb{Z}^m.$$

Lemma 4 *For $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ and $\mathbf{A}' \in \mathbb{Z}_q^{m\times n}$, we have*

- $\dim \Lambda_q^\perp(\mathbf{A}) = m$ *and* $\dim \Lambda_q(\mathbf{A}') = m$.

- $\det(\Lambda_q^\perp(\mathbf{A})) \leq q^n$ *and* $\det(\Lambda_q(\mathbf{A}')) \geq q^{m-n}$
- *If q is prime, and $\mathbf{A}, \mathbf{A}'$ are non-singular in the finite field $\mathbb{Z}_q$, the above inequalities are equalities.*

PROOF: For the dimension, note that $q\mathbb{Z}^m \subset \Lambda \subset \mathbb{Z}^m$. We only provide a proof for the inequality $\det(\Lambda_q^\perp(\mathbf{A})) \leq q^n$ and leave the other cases to the reader. Since $\Lambda_q^\perp(\mathbf{A}) \subset \mathbb{Z}^m$, $\det(\Lambda) = |\mathbb{Z}^m/\Lambda_q^\perp(\mathbf{A})|$. We therefore have $|\mathbb{Z}^m/\Lambda| = \mathrm{im}(\mathbf{A} : \mathbb{Z}_q \to \mathbb{Z}_q^n)$, and we conclude since $\mathrm{im}(\mathbf{A}) \subset \mathbb{Z}_q^n$. □

As we will see soon, the lattice $\Lambda_q^\perp(\mathbf{A})$ is often used as underlying lattice in cryptosystems. Therefore it is useful to know in what range the shortest vector of this lattice could be.

LEMMA 5 *Let q be prime, and let $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ be a matrix.*

- $\lambda_1^\infty(\Lambda_q^\perp(\mathbf{A})) \leq q^{n/m}$
- $\lambda_1^\infty(\Lambda_q^\perp(\mathbf{A})) > \frac{(q/2)^{n/m}-1}{2}$ *except with probability at most 2^{-n} over the choice of a uniform random matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$.*

PROOF: The first inequality is an application of Minkowski theorem, using

$$(2 \cdot \lambda_1^\infty(\Lambda_q^\perp(\mathbf{A})))^m \leq 2^m \cdot \det(\Lambda_q^\perp(\mathbf{A})) \leq 2^m \cdot q^{n/m}.$$

Here we just use the fact that any convex symmetric body with volume larger than $2^m \cdot \det(\Lambda_q^\perp(\mathbf{A}))$ must contain a non-zero lattice point.

For the second inequality, note that, we claim that for any $x \neq 0$ modulo q,

$$\mathbb{P}_{\mathbf{A}}[\mathbf{A}\mathbf{x} = 0 \bmod q] = q^{-n}.$$

Indeed, because $\mathbb{Z}_q$ is a finite field, one can verify that $\mathbf{A}\mathbf{x}$ is uniform in $\mathbb{Z}_q$ over the uniform choice of $\mathbf{A}$. Let us denote $\beta = \frac{(q/2)^{n/m}-1}{2}$, and count the number of vectors of ℓ_∞ norm less than β:

$$|\{\mathbf{x} \in \mathbb{Z}^m \mid \|x\|_\infty \leq \beta\}| = (2\beta+1)^m.$$

Using the union bound, we have

$$\mathbb{P}_{\mathbf{A}}[\exists \mathbf{x} \text{ with } \|\mathbf{x}\|_\infty \leq \beta \text{ and } \mathbf{A}\mathbf{x} = 0 \text{ modulo } q] \leq (2\beta+1)^m q^{-n} = (q/2)^n q^{-n} = 2^{-n}.$$

So, the probability that $\lambda_1^\infty(\Lambda_q^\perp((A))) \leq \beta$ is less than or equal to 2^{-n}, yielding the second bullet in the lemma. □

3 The SIS-problem

The abbreviation SIS stands for 'Short Integer Solution'. This name has the following clear explanation. Given a random matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, the problem is to find a short integer vector $\mathbf{x}$ that satisfies $\mathbf{A}\mathbf{x} = 0 \bmod q$.

DEFINITION 6 (SIS-PROBLEM) *The $\mathtt{SIS}_{m,n,q,\beta}$ problem is defined as follows:*
Given a uniform random matrix $\mathbf{A} \in \mathbb{Z}_q^{m\times n}$. Find $x \in [-\beta,\beta]^m \backslash \{\mathbf{0}\}$ such that $\mathbf{A}\mathbf{x} = 0$ mod q.

Remark 7 An instance $\mathbf{A}$ of the SIS problem is equivalent to finding a short non-zero vector in the lattice $\Lambda_q^{\perp}(\mathbf{A})$

Depending on the parameters, the hardness of the SIS-problem can range from 'vacuously hard' to having a polynomial time algorithm giving a solution.

- If $\beta \ll q^{n/m}$, the problem is vacuously hard: Lemma 5 showed that, most likely, such solutions do not exists.
- If $\beta \gg \gamma_2^m \cdot q^{n/m}$, this is an instance of approx-SVP with exponential approximation factor γ_2^m, which can be solved by LLL.
- Somewhere in between these bounds is where cryptography takes place, typically for $\beta = q^{n/m} \cdot \mathrm{poly}(n)$.

Beware though that the second bullet point is rather naive: it suggest that the problems gets harder as $m \to \infty$. This is not the case, as one can just ignore columns of the SIS instance $\mathbf{A}$, forcing the corresponding coordinates of $\mathbf{x}$ to 0.

Exercise 2 For very large m, improve the bound $\beta \geq \gamma_2^m \cdot \lambda(\Lambda_q^{\perp}(\mathbf{A}))$ for which you can one find a polynomial-time algorithm for SIS by considering $\Lambda_q^{\perp}(\mathbf{A}')$ where $\mathbf{A} = [\mathbf{A}'|\mathbf{A}'']$.

4 Collision resistance

An important notion in cryptography is *collision resistance*. Informally, a function f is collision resistant whenever it is computationally hard to find two different inputs x_1, x_2 such that $f(x_1) = f(x_2)$. To make this notion formal, we need some explanation and notation.

First, we would like to settle what it means to be 'computationally hard'. In computer science, this is often formalized using asymptotics and (probabilistic) polynomial-time Turing machines. In order to be able to properly talk about asymptotics, it makes no sense to talk about computational hardness of one function alone. Instead, one observes a function *family*, which is parametrized by a variable λ. Mathematically, one would denote that as follows:

$$\mathcal{F} = \{f_\lambda : \mathcal{K}_\lambda \times \mathcal{M}_\lambda \to \mathcal{H}_\lambda \mid \lambda \in \mathbb{N}\}.$$

The parametrization variable λ is often called the *security parameter*, since it indicates how 'hard' the collision problem is (which will be defined properly very soon). The letters for the domain and codomain of the functions f_λ come from their cryptographic interpretation. Namely, $\mathcal{K}$ stands for *key space*, $\mathcal{M}$ for *message space* and $\mathcal{H}$ for *hashing space*. In cryptography, collision resistant functions are often called hash functions, and inputs to such functions are viewed as messages. For fixed λ, the key space allows to use many different hash functions from $\mathcal{M}$ to $\mathcal{H}$, instead of just one.

Now, computational hardness of finding a collision can be defined as follows.

Definition 8 (Collision resistance) *A function family $\mathcal{F} = \{f_\lambda : \mathcal{K}_\lambda \times \mathcal{M}_\lambda \to \mathcal{H}_\lambda \mid \lambda \in \mathbb{N}\}$ is said to be collision resistant if, for all λ, and all probabilistic-polynomial time algorithms $\mathcal{A}$, holds that*

$$\mathop{\mathbb{P}}_{\substack{k \in \mathcal{K} \\ \mathcal{A}}}[f_\lambda(k, m_0) = f_\lambda(k, m_1) \textit{ and } m_0 \neq m_1 \mid (m_0, m_1) \leftarrow \mathcal{A}(k)] \leq \textit{negl}(\lambda).$$

Here, $\mathrm{negl}(\lambda)$ is any function in $\lambda^{-\omega(1)}$. Note that randomness is taken uniformly over the key space $\mathcal{K}$, as well as over the randomness of the algorithm $\mathcal{A}$.

In human language, above definition says that a function family $\mathcal{F}$ is collision resistant whenever no algorithm (that runs in reasonable time) is able to find a collision in f_λ with some significant probability. Note that the notion of collision resistance is only interesting whenever the functions $f_\lambda(k, \cdot)$ are not injective. In real life, one therefore almost only looks at the case when the hashing space $\mathcal{H}$ is (much) smaller than $\mathcal{M}$.

5 Cryptography and reductions

In cryptography, one often relies on certain 'hardness assumptions'. For example, people tend to say that the security of the famous cryptosystem RSA relies on the hardness of factoring[1]. In lattice based cryptosystems, something similar is happening; for example, we would like to show that breaking a specific cryptographic protocols is at least as hard as some lattice problem (that is believed to be hard).

For example, suppose we want to prove the following statement:

$$X \text{ is hard } \Rightarrow Y \text{ is hard.}$$

This means that problem Y is at least as hard as X. In computer science, this is proved as follows. Assume that there exists a so-called 'oracle' for Y. That is a miraculous (probably non-existing) algorithm that solves Y instantaneously. Now construct an algorithm $\mathcal{A}^Y$, that has access to the 'oracle' of Y and that solves X. If this algorithm is poly-time, one has proven that Y is at least as hard as X.

An hopefully clarifying example is the following so-called Merkle-Damgård domain extension of hash functions. Let $f : \mathcal{K} \times \{0,1\}^m \to \{0,1\}^n$ with $m > n$ be any function. Let $b = m - n > 0$. Set

$$f_{MD}^{(\ell)} : \mathcal{K} \times \{0,1\}^{\ell \cdot b} \to \{0,1\}^n, f_{MD}^{(\ell)}(\mu_1 \cdots \mu_\ell) = f_k(\cdots f_k(f_k(f_k(\mu_1|0)|\mu_2)|\mu_3)\cdots)|\mu_\ell),$$

where $\mu_i \in \{0,1\}^b$.

Theorem 9 *If f is collision resistant, then so is $f_{MD}^{(\ell)}$*

Proof: Suppose the latter is not collision resistant, meaning that there is an algorithm $\mathcal{A}$ that outputs a right pair $(\mu_1 \cdots \mu_\ell, \mu_1' \cdots \mu_\ell')$ with $f_{MD}^{(\ell)}(k, \mu_1 \cdots \mu_\ell) = f_{MD}^{(\ell)}(k, \mu_1' \cdots \mu_\ell')$ with probability $\frac{1}{p(\lambda)}$. Assume, that you found a collision for the Merkle-Darmgård construction of f.

Take the largest $i < \ell$ such that $f_{MD}^{(i)}(\mu_1 \cdots \mu_i) \neq f_{MD}^{(i)}(\mu_1' \cdots \mu_i')$. Then, taking $m_1 = f_{MD}^{(i)}(\mu_1 \cdots \mu_i)|\mu_{i+1}$ and $m_2 = f_{MD}^{(i)}(\mu_1' \cdots \mu_i')|\mu_{i+1}'$ yields a collision for f.

Then the same algorithm also finds an collision for f with polynomial probability, and f is therefore not collision resistant, too. By contraposition, we obtain the claim. □

Exercise 3 Make a Merkel-Damgård construction for arbitrary length input.

[1] In reality, this hardness assumption is slightly more complicated.

Collision resistant functions from the SIS problem The key space $\mathcal{K} = \mathbb{Z}_q^{n\times m}$, is the set of all $n \times m$ matrices with coefficients in $\mathbb{Z}_q$. Set $\mathcal{M} = \{0,1\}^m$ and $\mathcal{H} = \mathbb{Z}_q^n \approx \{0,1\}^{n \log_2 q}$. For key $\mathbf{A}$ and input message $x \in \mathcal{M}$, set

$$f_{\mathbf{A}}(\mathbf{x}) := \mathbf{A}\mathbf{x} \bmod q.$$

Lemma 10 *Is $\texttt{SIS}_{m,n,q,1}$ is hard, then $f_\cdot : \mathcal{K} \times \mathcal{M} \to \mathcal{H}$ is hard.*

Proof: Let $\mathbf{A} \in \mathcal{K}$. Suppose we are able to find two $\mathbf{m}_1 \neq \mathbf{m}_2 \in \mathcal{M}$ such that $f_{\mathbf{A}}(\mathbf{m}_1) = f_{\mathbf{A}}(\mathbf{m}_2)$. Let $\mathbf{x} = \mathbf{m}_1 - \mathbf{m}_2$. Then $\mathbf{A}\mathbf{x} = 0$, with $\|\mathbf{x}\|_\infty \leq 1$. So any algorithm that finds a collision of $f_\cdot$, solves SIS. □

6 One way functions

In this section, we will introduce a notion that is very similar to collision resistance, and, in fact, is mathematically related to it.

Definition 11 (One-way function) *A function family $\mathcal{F} = \{f_\cdot^{(\lambda)} : \mathcal{K}_\lambda \times \mathcal{M}_\lambda \to \mathcal{H}_\lambda \mid \lambda \in \mathbb{N}\}$ is one-way if for all probabilistic polynomial time algorithms $\mathcal{A}$ holds*

$$\mathop{\mathbb{P}}_{\substack{k\in\mathcal{K}\\ m\in\mathcal{M}\\ \mathcal{A}}} [f_k^{(\lambda)}(\mathcal{A}(1^\lambda, f_k^{(\lambda)}(m))) = f_k^{(\lambda)}(m)] \leq negl(\lambda)$$

Lemma 12 *If a family $\mathcal{F}$ has the following properties:*

- *$\mathcal{F}$ is collision resistant*
- *For almost all $k \in \mathcal{K}$, and for almost all $m \in \mathcal{M}$ there exists an $m' \neq m$ such that $f(m) = f(m')$.*

then it is a one-way function.

Remark 13 Above lemma is can be called the 'two-to-one property'; any collision resistant function that is almost always two-to-one, is a one way function as well.

Proof: By contradiction, we assume that the function is not one-way and that for almost $k \in \mathcal{K}$ and for almost all $m \in \mathcal{M}$ there exists an $m' \neq m$ such that $f(m) = f(m')$.

The function is not one-way, meaning that there is an algorithm $\mathcal{A}$ that finds a pre-image of $h = f_k^{(\lambda)}(m)$ with non-negligible probability $\frac{1}{p(\lambda)}$. The reduction algorithm can be described as follows.

- Sample a random $m \in \mathcal{M}$, and compute $h = f_k^{(\lambda)}(m)$.
- Output a possible pre-image $\mathcal{A}(1^\lambda, h)$ of h.

To analyze this algorithm, we partition the message space into blocks that have the same image.

$$\mathcal{M} = \bigcup_{h\in\mathcal{H}} \mathcal{M}_h$$

Here, $\mathcal{M}_h = \{m \in \mathcal{M} \mid f_k^{(\lambda)}(m) = h\}$, which can be empty as well. The second assumption in the lemma implies that $\#\{\mathcal{M}_h \mid \#\mathcal{M}_h = 1\} \leq \text{negl}(\lambda)$. So, with large probability (proportional to $(1 - \mathrm{negl}(\lambda)))$ we have that sampling an $m \in \mathcal{M}$ yields one from a block $\mathcal{M}_h$ of size ≥ 2. Since the algorithm $\mathcal{A}$ only depends on the function value $h \in \mathcal{H}$, it outputs an $m' \in \mathcal{M}_h$ with probability $p_{m'}/p(\lambda)$, because $1/p(\lambda)$ is the success probability of $\mathcal{A}$. Therefore, the probability over $\mathcal{M}$ of the above reduction algorithm to succeed equals

$$\min_{h\in\mathcal{H},\#M_h>1} \frac{1}{\#\mathcal{M}_h} \sum_{m\in\mathcal{M}_h} (1-p_m)\frac{1}{p(\lambda)} = \min_{h\in\mathcal{H},\#\mathcal{M}_h>1} \left(1 - \frac{1}{\#\mathcal{M}_h}\right) \cdot \frac{1}{p(\lambda)} \geq \frac{1}{2p(\lambda)}.$$

This last probability is clearly inverse-polynomial, therefore $\mathcal{F}$ is not collision resistant as well. By contraposition, the claim holds. □

In the next lecture, we choose parameters for the SIS-alike collision resistant function f_A such that this function has the two-to-one property (except with negligible probability). This function must then be one-way, instead of only collision resistant.