Ajtai commitment and its proof of opening

Recall SIS

Definition 4.1.1 (Short Integer Solution ($\mathrm{SIS}_{n,q,\beta,m}$)). Given m uniformly random vectors $\mathbf{a}_i \in \mathbb{Z}_q^n$, forming the columns of a matrix $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$, find a nonzero integer vector $\mathbf{z} \in \mathbb{Z}^m$ of norm $\|\mathbf{z}\| \le \beta$ such that

$$f_{\mathbf{A}}(\mathbf{z}) := \mathbf{A}\mathbf{z} = \sum_i \mathbf{a}_i \cdot z_i = \mathbf{0} \in \mathbb{Z}_q^n. \tag{4.1.1}$$

CRHF

DEFINITION 2 *A family of collision resistant hash functions (CRHF) is a sequence $\{\mathcal{F}_n\}_{n=1}^{\infty}$, where each $\mathcal{F}_n$ is a family of functions $f : \{0,1\}^{m(n)} \to \{0,1\}^{k(n)}$, with the following properties.*

1. *There exists an algorithm that given any $n \ge 1$ outputs a random element of $\mathcal{F}_n$ in time polynomial in n.*
2. *Every function $f \in \mathcal{F}_n$ is efficiently computable.*
3. *For any $c > 0$, there is no polynomial-time algorithm that with probability at least $\frac{1}{n^c}$, given a random $f \in \mathcal{F}_n$ outputs x, y such that $x \ne y$ and $f(x) = f(y)$ (i.e., there is no polynomial-time algorithm that with non-negligible probability finds a collision).*

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 $\mathtt{SIS}_{m,n,q,1}$ 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 $\mathbf{m}_1 \ne \mathbf{m}_2 \in \mathcal{M}$ 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 $\|\mathbf{x}\|_\infty \le 1$. So any algorithm that finds a collision of $f_\cdot$, solves SIS. □

4.3 Construction of a commitment scheme from SIS

An example of a lattice-based commitment scheme can be obtained by considering SIS-related function $f_{\mathbf{A}} = \mathbf{A}\mathbf{x} \bmod q$. One obtains such a scheme by putting the triple of functions `Keygen`, `Commit` and `Verif` as follows.

The key generating function `KeyGen` takes as input 1^n and outputs a matrix (that serves as public key) $\mathbf{A} =: pk$ uniformly random from $\mathbb{Z}_q^{n\times m}$, where m is a parameter whose value will be decided later. For the random set R and its distribution D, put $R = \mathbb{Z}^{m-1}$ and $D = D_{\mathbb{Z}^{m-1},\sigma}$ the discrete Gaussian distribution on $\mathbb{Z}^{m-1}$, where $\sigma \in \mathrm{poly}(n)$.

The commitment function is defined as follows: $\mathtt{Commit}(pk = \mathbf{A}, \mu, r) := \mathbf{A} \cdot \begin{pmatrix} \mu \\ \mathbf{r} \end{pmatrix} \bmod q$, where $\mu \in \{0,1\}$. Here, $\begin{pmatrix} \mu \\ \mathbf{r} \end{pmatrix}$ is the vector that is obtained by concatenating; $(\mu|\mathbf{r})$.

To verify the commitment on input (pk, μ, r, c), check whether $\mathbf{A} \cdot \begin{pmatrix} \mu \\ \mathbf{r} \end{pmatrix} = c \bmod q$ and $\|\begin{pmatrix} \mu \\ \mathbf{r} \end{pmatrix}\| \leq \beta$. If this is both true, set $\mathtt{Verif}(pk, \mu, r, c) = 1$, otherwise 0.

LEMMA 7 *For appropriate parameters, above scheme is correct, statistically hiding and computationally binding, assuming that the $\mathtt{SIS}_{n,m,q,2\beta}$ is hard.*

- (Computationally binding) Suppose a probabilistic polynomial time algorithm is able to find (on input $\mathbf{A}$) a triple $(\mathbf{r}_0, \mathbf{r}_1, c)$ such that $\mathbf{A}\begin{pmatrix} 0 \\ \mathbf{r}_0 \end{pmatrix} = c = \mathbf{A}\begin{pmatrix} 1 \\ \mathbf{r}_1 \end{pmatrix} \bmod q$ with non-negligible probability. Then the vector $\mathbf{v} = \begin{pmatrix} 1 \\ \mathbf{r}_0 - \mathbf{r}_1 \end{pmatrix}$ is a $\mathtt{SIS}_{n,m,q,2\beta}$ solution. Therefore, this adversary solves SIS with these parameters, which is a contradiction, as we assumed that this was hard.

- (Statistically hiding) The goal is to prove that $\tilde{\forall} \mathbf{A} = pk \leftarrow \mathtt{KeyGen}(1^n)$ holds $\mathtt{Commit}(pk, 0, r) \approx_s \mathtt{Commit}(pk, 1, r)$, i.e., that the statistical distance is negligible. Decompose A into a first column $\mathbf{a}_0$ and the rest of the matrix $\mathbf{A}'$: $\mathbf{A} = (\mathbf{a}_0|\mathbf{A}')$. Our aim is to prove that

$$\Delta = \frac{1}{2}\sum_{c\in C} |\mathbb{P}[\mathbf{A}'r = c] - \mathbb{P}[\mathbf{A}'r + a_0 = c]| \leq \mathrm{negl}(n).$$

Define $\Lambda_q^{\perp c} = \{\mathbf{x} \in \mathbb{Z}^m \mid \mathbf{A}\mathbf{x} \equiv c \bmod q\}$. Then, by construction

$$\mathbb{P}_{r\leftarrow D_{\mathbb{Z}^{m-1},\sigma}}[\mathbf{A}r = c] = \frac{\rho_\sigma(\Lambda_q^{\perp c}(\mathbf{A}'))}{\rho_\sigma(\mathbb{Z}^{m-1})}$$

If $\sigma \geq \eta_\varepsilon(\Lambda_q^{\perp c}(\mathbf{A}))$, the smoothing parameter of $\Lambda_q^{\perp c}(\mathbf{A}')$, then we know that (informally) the cumulative weight of the Gaussians of any coset of $\Lambda_q^{\perp c}(\mathbf{A}')$ is the same, up to a factor $(1 \pm \varepsilon)$ [Lecture 8, Lemma 5]. In particular, $\rho_\sigma(\Lambda_q^{\perp(c-a_0)}(\mathbf{A}')) \in [1-\varepsilon, 1+\varepsilon] \cdot \rho_\sigma(\Lambda_q^{\perp c}(\mathbf{A}'))$. Therefore

$$\Delta = \frac{1}{2}\sum_{c\in C} |\mathbb{P}[\mathbf{A}'r = c] - \mathbb{P}[\mathbf{A}'r + a_0 = c]| = \frac{1}{2\rho_\sigma(\mathbb{Z}^{m-1})}\sum_{c\in C} |\rho_\sigma(\Lambda_q^{\perp(c-a_0)}(\mathbf{A}')) - \rho_\sigma(\Lambda_q^{\perp c}(\mathbf{A}'))|$$

$$\leq \frac{1}{2\rho_\sigma(\mathbb{Z}^{m-1})}\sum_{c\in C} \varepsilon \cdot \rho_\sigma(\Lambda_q^{\perp c}(\mathbf{A}')) \leq \varepsilon/2$$

In order to know the parameter choice for σ, we need to estimate $\eta_\varepsilon(\Lambda_q^{\perp c}(\mathbf{A}))$ with $\varepsilon \in \mathrm{negl}(n)$. This is because σ needs to be larger than the smoothing parameter.

□

LYU SIGNATURE

Prove the knowledge of a SIS secret

Signing Key: $\mathbf{S} \xleftarrow{\$} \{-d, \ldots, 0, \ldots, d\}^{m \times k}$
Verification Key: $\mathbf{A} \xleftarrow{\$} \mathbb{Z}_q^{n \times m}, \mathbf{T} \leftarrow \mathbf{AS}$
Random Oracle: $\mathrm{H} : \{0,1\}^* \to \{\mathbf{v} : \mathbf{v} \in \{-1,0,1\}^k, \|\mathbf{v}\|_1 \leq \kappa\}$

Sign$(\mu, \mathbf{A}, \mathbf{S})$
1: $\mathbf{y} \xleftarrow{\$} D_\sigma^m$
2: $\mathbf{c} \leftarrow \mathrm{H}(\mathbf{Ay}, \mu)$
3: $\mathbf{z} \leftarrow \mathbf{Sc} + \mathbf{y}$
4: output $(\mathbf{z}, \mathbf{c})$ with probability $\min\left(\frac{D_\sigma^m(\mathbf{z})}{M D_{\mathbf{Sc},\sigma}^m(\mathbf{z})}, 1\right)$

Verify$(\mu, \mathbf{z}, \mathbf{c}, \mathbf{A}, \mathbf{T})$
1: Accept iff
$\|\mathbf{z}\| \leq \eta\sigma\sqrt{m}$ and $\mathbf{c} = \mathrm{H}(\mathbf{Az} - \mathbf{Tc}, \mu)$

Fig. 1. Signature Scheme.

Zero-Knowledge

Theorem 4.6. *Let V be a subset of $\mathbb{Z}^m$ in which all elements have norms less than T, σ be some element in $\mathbb{R}$ such that $\sigma = \omega(T\sqrt{\log m})$, and $h : V \to \mathbb{R}$ be a probability distribution. Then there exists a constant $M = O(1)$ such that the distribution of the following algorithm $\mathcal{A}$:*

1: $\mathbf{v} \xleftarrow{\$} h$
2: $\mathbf{z} \xleftarrow{\$} D_{\mathbf{v},\sigma}^m$
3: output $(\mathbf{z}, \mathbf{v})$ *with probability* $\min\left(\frac{D_\sigma^m(\mathbf{z})}{M D_{\mathbf{v},\sigma}^m(\mathbf{z})}, 1\right)$

is within statistical distance $\frac{2^{-\omega(\log m)}}{M}$ of the distribution of the following algorithm $\mathcal{F}$:

1: $\mathbf{v} \xleftarrow{\$} h$
2: $\mathbf{z} \xleftarrow{\$} D_\sigma^m$
3: output $(\mathbf{z}, \mathbf{v})$ *with probability* $1/M$

Moreover, the probability that $\mathcal{A}$ outputs something is at least $\frac{1-2^{-\omega(\log m)}}{M}$.

More concretely, if $\sigma = \alpha T$ for any positive α, then $M = e^{12/\alpha + 1/(2\alpha^2)}$, the output of algorithm $\mathcal{A}$ is within statistical distance $\frac{2^{-100}}{M}$ of the output of $\mathcal{F}$, and the probability that $\mathcal{A}$ outputs something is at least $\frac{1-2^{-100}}{M}$.

Soundness

Definition 2.3 (Relaxed Binding Commitment [ALS20; ACK21; Ajt96; PR06; LM06]). *Fix $q = q(\lambda)$,$\kappa = \kappa(\lambda)$, $m = m(\lambda)$, bound $b \in \mathbb{N}$ and a set $\mathcal{S} \subseteq R_q^*$ with invertible elements. We say that a randomly sampled linear function $\mathbf{A} \xleftarrow{R} R_q^{\kappa \times m}$ is $(b, \mathcal{S})$-relaxed binding if for all expected polynomial-time adversary $\mathcal{A}$,*

$$\Pr\left[\begin{array}{c} 0 < \|\mathbf{z}_1\|_\infty, \|\mathbf{z}_2\|_\infty < b \wedge s_1, s_2 \in \mathcal{S} \wedge \\ \mathbf{A}\mathbf{z}_1 s_1^{-1} = \mathbf{A}\mathbf{z}_2 s_2^{-1} \wedge \\ \mathbf{z}_1 s_1^{-1} \neq \mathbf{z}_2 s_2^{-1} \end{array} \middle| \begin{array}{c} \mathbf{A} \xleftarrow{R} R_q^{\kappa \times m} \\ (\mathbf{z}_1, \mathbf{z}_2 \in R_q^m, s_1, s_2) \leftarrow \mathcal{A}(\mathbf{A}) \end{array}\right] = \mathsf{negl}(\lambda).$$

It is clear that if the $(b, \mathcal{S})$-relaxed binding property doesn't hold, then we can find $\mathbf{x} := s_2\mathbf{z}_1 - s_1\mathbf{z}_2 \neq \mathbf{0} \in R^m$ such that $\mathbf{Ax} = 0 \bmod q$. Here $s_2\mathbf{z}_1 - s_1\mathbf{z}_2$ is computed over R by first lifting $s_1, s_2, \mathbf{z}_1, \mathbf{z}_2$ to R. Moreover, $\|\mathbf{x}\|_\infty < B := 2b\|\mathcal{S}\|_{\mathsf{op}}$, thus we can reduce the $(b, \mathcal{S})$-relaxed binding property to the MSIS assumption $\mathsf{MSIS}_{q,\kappa,m,B}^\infty$.

If we don't care ZK...