

Ajtai commitment expansion

Matthew Klein

July 10, 2024

Ajtai Commitments

- ▶ Ajtai commitments allow us to commit to a vector of polynomials
- ▶ We commit to an a vector $\vec{x} \in \mathcal{R}^m$ by multiplying it with a random matrix $\mathbf{A} \in \mathcal{R}_q^{\kappa \times m}$
- ▶ $\|\vec{x}\|_\infty < B$ where B is the norm bound
- ▶ Output of commitment is $cm := \mathbf{A} \cdot \vec{x} \bmod \mathbf{q} \in \mathcal{R}_q^\kappa$
- ▶ This commitment is considered binding because of the assumed hardness of MSIS

Ajtai commitments as a relation

- ▶ We define relation $\mathcal{R}_{MSIS\infty}^B$ between an ajtati commitment and the \vec{x}
- ▶ $\mathcal{R}_{MSIS\infty}^B := (pp, cm \in \mathcal{R}_q^\kappa; \vec{x} \in \mathcal{R}^m : (cm = \mathbf{A} \cdot \vec{x} \bmod \mathbf{q}) \wedge \|\vec{x}\|_\infty < \mathbf{B})$
- ▶ $pp := (\kappa, m, B, \mathbf{A})$ are the public parameters of the relation
- ▶ Public parameters define the 'meta' information of the relation:
 1. The size of the vectors and matrices
 2. The norm limit of \vec{x}
 3. The random matrix \mathbf{A}

$$\vec{x} \in \mathcal{R}_q^m$$

- ▶
 - ▶ $\|\vec{x}\|_{\text{infty}} < B$ and $B < \frac{q}{2}$
 - ▶ $\vec{x} \in \mathcal{R}^m$ can be uniquely represented in \mathcal{R}_q^m
 - ▶ We define $\|\vec{x}\|_{\text{infty}} < B$ as the norm after lifting $\vec{x} \in \mathcal{R}_q^m$ to \mathcal{R}
- ▶ We can rewrite our commitment as

$$\mathcal{R}_{\text{MSIS}\infty}^B := (pp, cm \in \mathcal{R}_q^\kappa; \vec{x} \in \mathcal{R}_q^m : (cm = \mathbf{A} \cdot \vec{x} \bmod \mathbf{q}) \wedge \|\vec{x}\|_\infty < \mathbf{B})$$

Coefficient Embeddings and Rotational Matrices

- ▶ For $a \in \mathcal{R}_q$, $\text{vec}(a)$ represents the vectors of coefficients
- ▶ For a vector $\vec{a} \in \mathcal{R}_q^m$, $\text{vec}(\vec{a}) \in \mathbb{Z}^{m \times d}$ represents the coefficient vectors in \vec{a}
- ▶ $\text{fvec}(\vec{a}) \in \mathbb{Z}^{md}$ is the vector that concatenates the rows of \vec{a}
- ▶ $\text{Rot}(\mathbf{a}) := (\text{vec}(\mathbf{a}), \text{vec}(\mathbf{X} \cdot \mathbf{a}), \dots, \text{vec}(\mathbf{X}^{d-1} \cdot \mathbf{a})) \in \mathbb{Z}_q^{d \times d}$.
- ▶ For a matrix $\mathbf{A} \in \mathbb{R}_q^{\kappa \times m}$, we define the rotation matrix $\text{Rot}(\mathbf{A}) \in \mathbb{Z}_q^{\kappa d \times md}$ as

$$\text{Rot}(\mathbf{A}) := \begin{bmatrix} \text{Rot}(\mathbf{A}_{1,1}) & \cdots & \text{Rot}(\mathbf{A}_{1,m}) \\ \vdots & \ddots & \vdots \\ \text{Rot}(\mathbf{A}_{\kappa,1}) & \cdots & \text{Rot}(\mathbf{A}_{\kappa,m}) \end{bmatrix}$$

- ▶ $\text{fvec}(\mathbf{A}\mathbf{f}) = \text{Rot}(\mathbf{A})\text{fvec}(\mathbf{f})$ for any $\mathbf{A} \in \mathbb{R}_q^{\kappa \times m}$ and $\mathbf{f} \in \mathbb{R}_q^m$.