# 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 $\overrightarrow{x} \in \mathcal{R}^m$ by multiplying it with a random matrix $\mathbf{A} \in \mathcal{R}_q^{\kappa \times \mathbf{m}}$
- $||\overrightarrow{x}||_\infty < B$ where $B$ is the norm bound
- Output of commitment is $cm := \mathbf{A} \cdot \overrightarrow{x} \mathbf{mod\ q} \in \mathcal{R}_q^\kappa$
- This commitment is considered binding because of the assumed hardness of MSIS

# Ajtai commitments as a relation

- We define relation $\mathcal{R}^{B}_{MSIS^{\infty}}$ between an ajtati commitment and the $\overrightarrow{x}$
- $\mathcal{R}^{B}_{MSIS^{\infty}} := (pp,\ cm \in \mathcal{R}^{\kappa}_{q};\ \overrightarrow{x} \in \mathcal{R}^{m} : (cm = \mathbf{A} \cdot \overrightarrow{x} \ \mathbf{mod\ q}) \wedge ||\overrightarrow{x}||_{\infty} < \mathbf{B})$
- $pp := (\kappa, m, B, \mathbf{A})$ 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 $\overrightarrow{x}$
  3. The random matrix $\mathbf{A}$

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

- - $||\overrightarrow{x}||_\infty < B$ and $B < \frac{q}{2}$
  - $\overrightarrow{x} \in \mathcal{R}^m$ can be uniquely represented in $\mathcal{R}_q^m$
  - We define $||\overrightarrow{x}||_{|infty} < B$ as the norm after lifting $\overrightarrow{x} \in \mathcal{R}_q^m to \mathcal{R}$
- We can rewrite our commitment as
  $\mathcal{R}^B_{MSIS^\infty} := (pp, cm \in \mathcal{R}_q^\kappa; \overrightarrow{x} \in \mathcal{R}_q^m : (cm = \mathbf{A} \cdot \overrightarrow{x} \textbf{ mod q}) \wedge ||\overrightarrow{x}||_\infty < \mathbf{B})$

# Coefficient Embeddings and Rotational Matrices

- For $a \in \mathcal{R}_q$, $vec(a)$ reoresents the vectors of coefficients
- For a vector $\overrightarrow{a} \in \mathcal{R}_q^m$, $vec(\overrightarrow{a}) \in \mathbb{Z}^{m \times d}$ represents the coefficient vectors in $\overrightarrow{a}$
- $fvec(\overrightarrow{a}) \in \mathbb{Z}^{md}$ is the vector that concatonates the rows of $\overrightarrow{a}$
- $\text{Rot}(\mathbf{a}) := (\text{vec}(\mathbf{a}), \text{vec}(\mathbf{X} \cdot \mathbf{a}), \ldots, \text{vec}(\mathbf{X}^{d-1} \cdot \mathbf{a})) \in \mathbb{Z}_q^{d \times d}$.
- 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

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

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

$$\overrightarrow{x} \in \mathbb{Z}^{\kappa d}$$

- We can uniquely represent $\overrightarrow{x} \in \mathcal{R}_q^m$ as $\overrightarrow{x} \in \mathbb{Z}^{\kappa d}$ by taking $fvec(\overrightarrow{x})$
- $\overline{\mathbf{A}} = rot(\mathbf{A})$
- $\overline{cm}$ is the coefficient embedding of $cm$
- $\overline{cm} = \overline{\mathbf{A}} \cdot fvec(\overrightarrow{x})$

$\mathcal{R}^B_{MSIS^\infty} := (pp, \overline{cm} \in \mathbb{Z}^{\kappa d}; \overrightarrow{x} \in \mathbb{Z}^{md} : (\overline{cm} = \overline{\mathbf{A}} \cdot \overrightarrow{x} \ mod\ q) \wedge ||\overrightarrow{x}||_\infty < B)$