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 $\mathbf{A} \in \mathcal{R}_{\boldsymbol{q}}^{\kappa \times \mathbf{m}}$
- $||\overrightarrow{x}||_\infty < B$ where B is the norm bound
- Output of commitment is $cm := \mathbf{A} \cdot \overrightarrow{x} \, \mathbf{mod\ q} \in \mathcal{R}_{\boldsymbol{q}}^{\kappa}$
- 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
  $\mathcal{R}^B_{MSIS\infty} := (pp,\ cm \in \mathcal{R}_q^\kappa;\ \overrightarrow{x} \in \mathcal{R}_q^m : (cm\ =\ \mathbf{A} \cdot \overrightarrow{x}\ \mathbf{mod\ q}) \wedge ||\overrightarrow{x}||_\infty < \mathbf{B})$