

# Ajtai commitment expansion

Matthew Klein

July 11, 2024

# What we are trying to do

- ▶ We start off with a relation made hard to 'break' based on the MSIS problem
- ▶ We will show that this relation is equivalent to two other relations, that can be used for folding
- ▶ We then adapt this equivalence to the Customisable Constraint System (CCS)

# 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  $\mathbf{A}$

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

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

# 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  $\mathbf{f} \in \mathbb{R}_q^m$ .

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

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

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

Representing  $\|\vec{x}\|_\infty < B$  as an hadamard product

$$\mathcal{R}_{\text{MSISProd}}^B := \left\{ (pp, \overline{cm} \in \mathbb{Z}^{\kappa d}; \vec{x} \in \mathbb{Z}^{md} \mid \begin{array}{l} \overline{cm} = \overline{\mathbf{A}} \cdot \vec{x} \\ \wedge \|\vec{x}\| \circ \left[ \bigcirc_{i=1}^{B-1} (\vec{x} - \vec{i}) \circ (\vec{x} + \vec{i}) \right] = \vec{0} \end{array} \right\}$$

- To see this see that the biggest coefficient in any of the  $x$  matrices is less than  $B$



$$\mathcal{R}_{cm}^B$$

- ▶ We can look at  $\vec{x}$  in two ways
- ▶  $\vec{x}$  is a NTT representation of a  $\hat{f} \in \mathcal{R}_q^m$
- ▶  $\vec{x}$  is coefficient embedding of a  $\vec{f} \in \mathcal{R}_q^m$
- ▶ The Hadamard product of two NTT representation is equivalent to the multiplication of the two elements
- ▶ i.e  $\vec{x} \circ \vec{x} \cong \hat{f} \circ \hat{f}$

$$\mathcal{R}_{cm}^B := \left\{ (pp, \overline{cm} \in \mathcal{R}_q^\kappa; \vec{f} \in \mathcal{R}_q^m \mid \overline{cm} = \overline{\mathbf{A}} \cdot \vec{f} \wedge \|\hat{f}\| \circ \left[ \bigcirc_{i=1}^{B-1} (\hat{f} - \hat{i}) \circ (\hat{f} + \hat{i}) \right] = \hat{0} \right\}$$

$$\mathcal{R}_{eval}^B$$

- ▶ Essentially the same as before, with an added evaluation statement
- ▶ We supply the relation with variables and an evaluation of the  $\vec{f}$  at those variable

$$\mathcal{R}_{eval}^B = \left\{ (pp; (r, v, cm) \in \mathcal{R}_q^{\log m} \times \mathcal{R}_q \times \mathcal{R}_q^\kappa; \vec{f} \in \mathcal{R}_q^m) \mid \begin{array}{l} (pp; cm; \vec{f}) \in \mathcal{R}_{cm}^B \\ \wedge \text{mle}[\hat{f}](\vec{r}) = v \end{array} \right\}$$

## Let's take this to CCS

- ▶ We introduce an insane amount of notation
- ▶
  - ▶ Public Paramers ( $\mathbf{pp}$ )  $:= (n_r, n_c, t, n_s, \deg, l_{in})$
  - ▶  $\overline{\mathcal{R}}$  is an arbitrary ring
  - ▶  $\mathfrak{i}$  consists of
    1.  $t$  matrices  $M_1..M_t \in \overline{\mathcal{R}}^{n_r \times n_c}$  with  $\mathcal{O}(n_r + n_c)$  non-zero entries
    2.  $n_s$  multisets  $S_1..S_{n_s} \subseteq [t]$  with  $|S_i| < \deg$  for all  $i \in [n_s]$
    3.  $n_s$  scalars  $cn_1, \dots, cn_s \in \overline{\mathcal{R}}$
- ▶ We then introduce the relation  $\mathcal{R}_{\text{CCS}}$
- ▶
  1.  $\mathbf{pp}_{\text{CCS}} := (\mathbf{pp}, \mathfrak{i})$
  2.  $(\mathbf{pp}_{\text{CCS}}, \mathbb{X} \in \overline{\mathcal{R}}^{l_{in}}, \mathbb{W} \in \overline{\mathcal{R}}^{n_c - l_{in} - 1})$
  3.  $\vec{\mathbb{Z}} := (\mathbb{X}, 1, \mathbb{W}) \in \mathcal{R}^{n_c}$
  4. The condition for the relation is  $\sum_{i=1}^{n_s} c_i \cdot \bigcirc_{j \in S_i} (M_j \cdot \vec{\mathbb{Z}}) = 0^{n_r}$

$$\mathcal{R}_{\text{CCS}} := \left\{ (\mathbf{pp}_{\text{CCS}}, \mathbb{X} \in \overline{\mathcal{R}}^{l_{in}}, \mathbb{W} \in \overline{\mathcal{R}}^{n_c - l_{in} - 1}) \text{ such that } \sum_{i=1}^{n_s} c_i \cdot \bigcirc_{j \in S_i} (M_j \cdot \vec{\mathbb{Z}}) = 0^{n_r} \right\}$$

Let's bind  $\mathcal{R}_{\text{cm}}$  and  $\mathcal{R}_{\text{ccs}}$  together!

- ▶ We introduce the gadget matrix
- ▶  $l := \frac{m}{n_c}$
- ▶  $\mathbf{G} := \mathbf{I}_{n_c} \otimes [1, B, \dots B^{l-1}] \in \mathbb{Z}_q^{n_c \times m}$
- ▶ We then define  $\mathcal{R}_{\text{cmcss}}^B$

We then define

$$\mathcal{R}_{\text{cmcss}}^B := \left\{ (\text{pp}, \mathbb{X} := (\text{cm} \in \mathcal{R}_q^{\kappa}, \mathbb{X}_{\text{ccs}} \in \mathcal{R}_q^{l_{\text{in}}})) ; \mathbb{W} := (\vec{\mathbf{f}} \in \mathcal{R}_q^m, \mathbb{W}_{\text{ccs}} \in \mathcal{R}^{n-l_{\text{in}}-1}) \text{ s.t. } \right. \\ \left. (\text{pp}, \text{cm}, \vec{\mathbf{f}} \in \mathcal{R}_{\text{cm}}^B) \wedge (\text{pp}_{\text{ccs}}, \mathbb{X}_{\text{ccs}}; \mathbb{W}_{\text{ccs}}) \in \mathcal{R}_{\text{ccs}} \wedge (\mathbf{z}_{\text{ccs}} = \mathbf{G} \vec{\mathbf{f}}) \right\}$$

$$\bar{\mathbf{z}}_{\text{ccs}} := (\mathbb{X}_{\text{ccs}}, \mathbf{1}, \mathbb{W}_{\text{ccs}}) \in \mathcal{R}^{n_c}$$

$$\mathcal{R}_{\text{lccs}}^B$$

- ▶  $\vec{\mathbf{r}} \in \mathcal{R}_q^{\log m}$
- ▶  $[\mathbf{u}_i]_{i=1}^t$
- ▶  $\mathcal{R}_{\text{lccs}} := (\text{pp}_{\text{ccs}}, (\vec{\mathbf{r}}, [\mathbf{u}_i]_{i=1}^t, \mathbb{X}_{\text{ccs}}, \mathbf{h}))$
- ▶ For all  $i \in [t]$  it holds that  $\mathbf{u}_i = \sum_{\vec{\mathbf{b}} \in \{0,1\}^{\log n_c}} \text{mle}[M_i](\vec{\mathbf{r}}, \vec{\mathbf{b}}) \cdot \text{mle}[\mathbf{z}_{\text{ccs}}](\vec{\mathbf{b}})$