

# Meeting with Jason

Friday, October 21, 2022 11:23

Things we'd like to know more about:

- The structure and semantics of your data
- Initial layout of the screen
- Which features we'd want to prioritize to build first
- Preferred visual encodings for your data

Data: response matrix,  $\delta_i^{(c)}$  (related to PUF)  
new  $\Delta_n$  matrix  $C$  (related to challenge)  
 $\downarrow$  real value

n-stage

APUF

$A$  function

Challenges

$c \in \mathbb{Z}_2^n$   
 $\downarrow$  input

$c_1 c_2 \dots c_n$   
 $[0 1 \dots 101]$

Response

$R(c) \in \mathbb{Z}_2 = \{0, 1\} = \text{sign}(\Delta_n(c))$   
 $\downarrow$  output  
 $\downarrow$  we use  $\{\pm 1\}$  instead

$c \rightarrow A \rightarrow R(c)$

$$\begin{aligned}\Delta_n(c) &= \sum_{i=1}^n \alpha_i \delta_i^{(c)} \\ &= \sum_{i=1}^n \alpha_i \delta_i^{(c_i)} + \delta_n\end{aligned}$$

Consider a set of challenges of size  $N$

$$[c_1, c_2, \dots, c_N] \rightarrow [A] \rightarrow [R(c_1), R(c_2), \dots, R(c_N)]$$

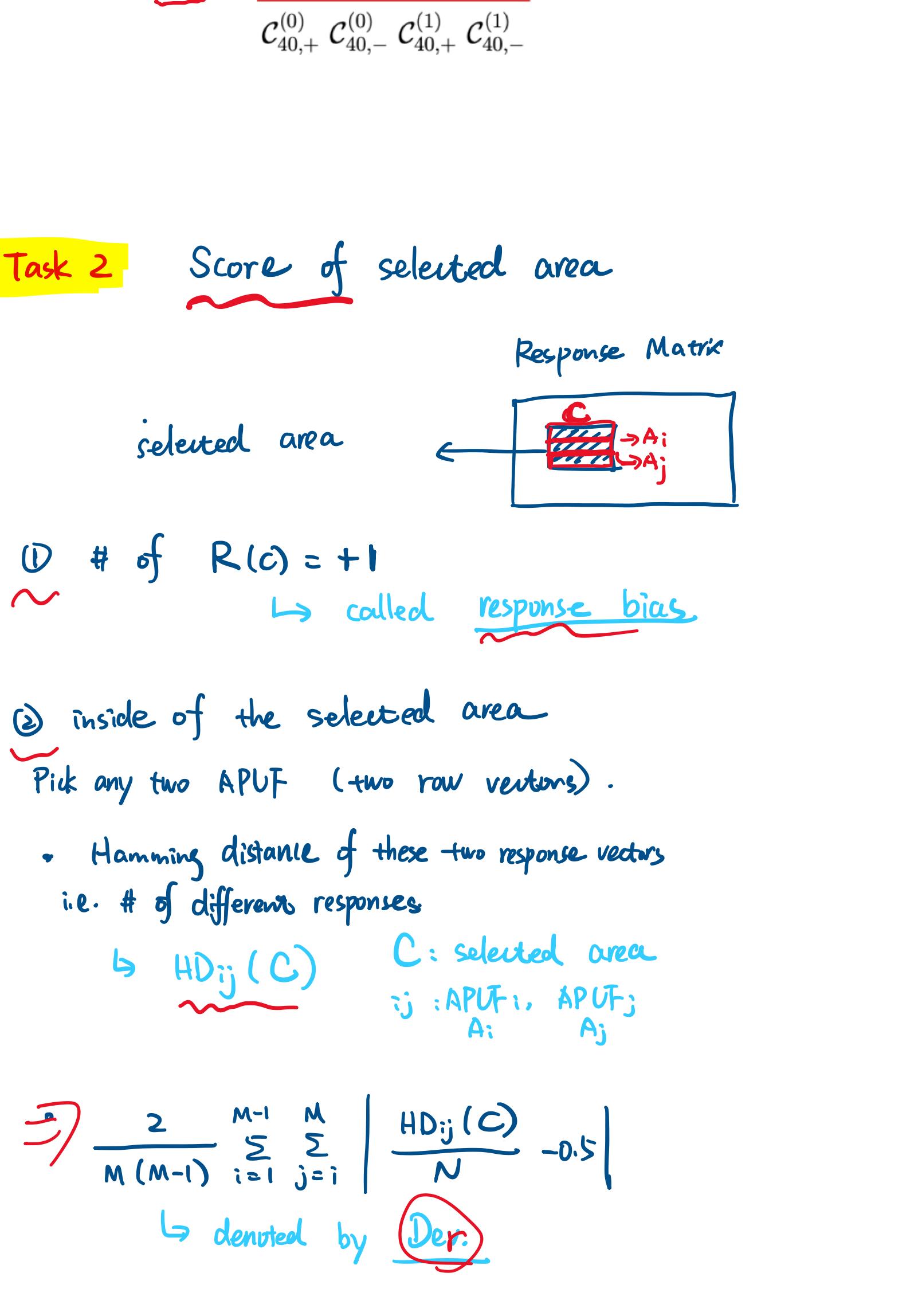
row vector

Consider a set of APUFs of size  $M$

$$c \rightarrow \begin{bmatrix} A_1 \\ A_2 \\ \vdots \\ A_M \end{bmatrix} \rightarrow \begin{bmatrix} R_1(c) \\ R_2(c) \\ \vdots \\ R_M(c) \end{bmatrix}$$

$\Rightarrow$  Response matrix of  $M$  APUFs  
 $N$  challenges

$$R(A, C) = \begin{bmatrix} R_1(c_1) & \dots & R_1(c_N) \\ \vdots & \ddots & \vdots \\ R_M(c_1) & \dots & R_M(c_N) \end{bmatrix}_{M \times N}$$



Reordering  $\left\{ \begin{array}{l} \delta_i^{(c)} \text{ values} \\ \text{challenges} \end{array} \right\}$  Task 1

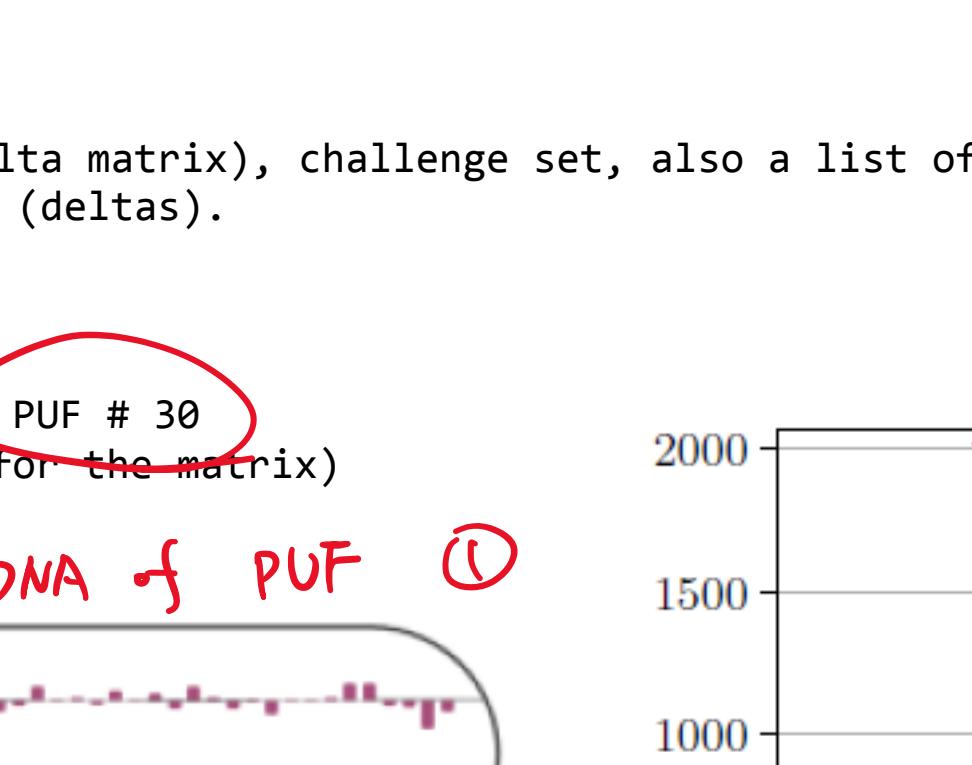
① challenges - vertical

$$c = [c_1, c_2, c_3, c_4] \in C$$

Partition the  $C$  according to  $\left\{ \begin{array}{l} c_2 \\ \text{sign} \end{array} \right\}$

$$\text{sign} = \begin{cases} +, & \text{if } c_3 + c_4 \text{ is even} \\ -, & \text{if } c_3 + c_4 \text{ is odd} \end{cases}$$

$$\Rightarrow c = C_{2,+}^{(0)} \cup C_{2,-}^{(0)} \cup C_{2,+}^{(1)} \cup C_{2,-}^{(1)}$$



②  $\delta_i^{(x)}$  value - horizontal

An APUF is characterized by  $\delta_i^{(x)}$ .

Consider 4-stage APUF instance.

$$2 \times 4 \cdot \begin{bmatrix} S_1^{(0)} & S_2^{(0)} & S_3^{(0)} & S_4^{(0)} \\ S_1^{(1)} & S_2^{(1)} & S_3^{(1)} & S_4^{(1)} \end{bmatrix} \quad \delta_i^{(x)} \in \mathbb{R}$$

①



(c)

②

$\sigma$ -fault APUFs

(f)

larger  $\delta_{40}^{(0)}$

small  $\delta_{40}^{(1)}$

$C_{40,+}^{(0)}, C_{40,-}^{(0)}, C_{40,+}^{(1)}, C_{40,-}^{(1)}$

(e)

Like a list of setting and outputs (scores)

R matrix (Delta matrix), challenge set, also a list of the parameters for each PUF (deltas).

Now I want PUF # 30 (row # 30 for the matrix)

$\delta_{40}^{(0)} = 0.5$  DNA of PUF ①

$\delta_{40}^{(1)} = 0.5$

$\delta_{40}^{(0)} = 0.5$  DNA of PUF ②

$\delta_{40}^{(1)} = 0.5$

Histogram ( $\Delta_{30}$ )

0 500 1000 1500 2000

-50 -25 0 25 50

0 500 1000 1500 2000

-50 -25 0 25 50

0 500 1000 1500 2000

-50 -25 0 25 50

0 500 1000 1500 2000

-50 -25 0 25 50

0 500 1000 1500 2000

-50 -25 0 25 50

0 500 1000 1500 2000

-50 -25 0 25 50

0 500 1000 1500 2000

-50 -25 0 25 50

0 500 1000 1500 2000

-50 -25 0 25 50

0 500 1000 1500 2000

-50 -25 0 25 50

0 500 1000 1500 2000

-50 -25 0 25 50

0 500 1000 1500 2000

-50 -25 0 25 50

0 500 1000 1500 2000

-50 -25 0 25 50

0 500 1000 1500 2000

-50 -25 0 25 50

0 500 1000 1500 2000

-50 -25 0 25 50

0 500 1000 1500 2000

-50 -25 0 25 50

0 500 1000 1500 2000

-50 -25 0 25 50

0 500 1000 1500 2000

-50 -25 0 25 50

0 500 1000 1500 2000

-50 -25 0 25 50

0 500 1000 1500 2000

-50 -25 0 25 50

0 500 1000 1500 2000

-50 -25 0 25 50

0 500 1000 1500 2000

-50 -25 0 25 50

0 500 1000 1500 2000

-50 -25 0 25 50

0 500 1000 1500 2000

-50 -25 0 25 50

0 500 1000 1500 2000

-50 -25 0 25 50

0 500 1000 1500 2000

-50 -25 0 25 50

0 500 1000 1500 2000

-50 -25 0 25 50

0 500 1000 1500 2000

-50 -25 0 25 50

0 500 1000 1500 2000

-50 -25 0 25 50

0 500 1000 1500 2000

-50 -25 0 25 50

0 500 1000 1500 2000

-50 -25 0 25 50

0 500 1000 1500 2000

-50 -25 0 25 50

0 500 1000 1500 2000

-50 -25 0 25 50

0 500 1000 1500 2000

-50 -25 0 25 50

0 500 1000 1500 2000

-50 -25 0 25 50

0 500 1000 1500 2000

-50 -25 0 25 50

0 500 1000 1500 2000

-50 -25 0 25 50

0 500 1000 1500 2000

-50 -25 0 25 50

0 500 1000 1500 2000

-50 -25 0 25 50

0 500 1000 1500 2000

-50 -25 0 25 50

0 500 1000 1500 2000

-50 -25 0 25 50

0 500 1000 1500 2000

-50 -25 0 25 50

0 500 1000 1500 2000

-50 -25 0 25 50

0 500 1000 1500 2000

-50 -25 0 25 50

0 500 1000 1500 2000

-50 -25 0 25 50

0 500 1000 1500 2000

-50 -25 0 25 50

0 500 1000 1500 2000

-50 -25 0 25 50