Shake指令

1. **absorb**:

参数：源数据首地址，数据长度，轮数，是否重置，安全等级

这个指令是一段数送进去后满了直接吸收（数据长度会大于一次吸收的长度）

2. **absorbload**:

参数：源数据首地址，数据长度，是否重置

这个指令只将数据送入shake模块准备吸收，但不进行吸收，用于需要几个数据拼起来的情况。

3. **absorbex**:

与2结合使用，进行一次吸收

4. **extrusion:**

参数：目标数据首地址，轮数，是否采样，矩阵是否转置，地址是否清0

这个指令和absorb对应，它会挤出全部数据并进行存储，S^T的问题不太好解决，预计使用一个地址控制模块去生成地址。

5. **extrusionex**:

执行一次挤压但不进行输出，为了那种在一轮出来的数据被拆分成了几个数据

6. **extrusionstore**:

参数：目标数据首地址，数据长度，是否转置，地址是否清0

与extrusionex结合使用，将结果的一定长度的数据进行存储，地址如果不清0，就直接沿用地址生成模块的地址，否则对其更新

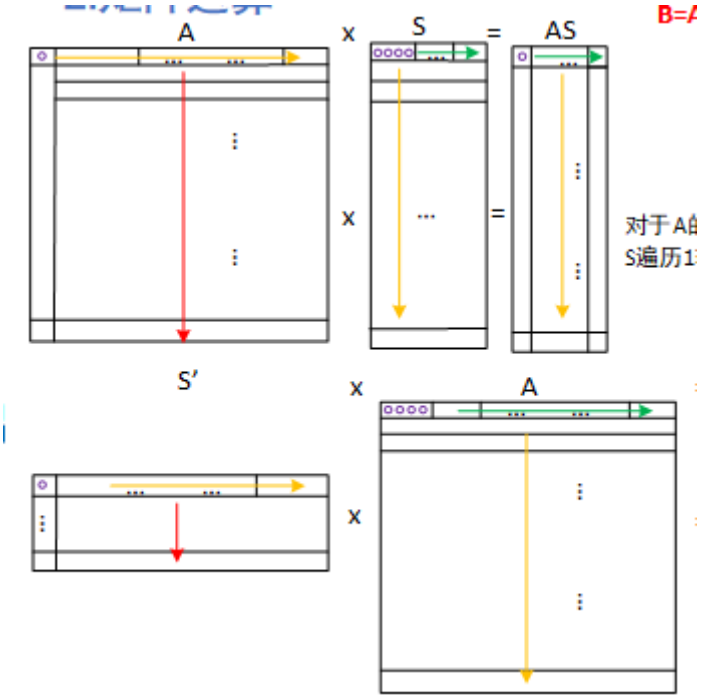
Mat指令

1. **matmul**:

参数：目标矩阵首地址，源矩阵1首地址，源矩阵2首地址，矩阵大小，是否取反

目前的设计上，执行的是C=A*B+C，所有的矩阵乘法都用这个循环顺序（所以S^T必须按正常顺序存）

取反是为了那个-BS



2. **matadd**:

参数：目标矩阵首地址，源矩阵首地址，矩阵大小

保留单独的加法是因为那个+encode(u)

几个算法的流程也写了，参数有所更新，可能对应不上，但是大致意思

Key generation

```
absorb z 128 1 true
extrusion z 128 1 false // shake产生seedA
shake_for_keygen // 这个是之前没想到SAT怎么搞，为这步单独搞的，但是想来想去还是觉得不优雅，可以向下面那样拆成几个指令
matmul A,S,E,1344,1344,8
absorbload seed_A 128
absorbload B xxx
absorbex
absorb B xxx 158 false
extrusionex
extrusionstore pkh 256
```

Encapsulation

```
absorb pk xxx 159 true
extrusionex
extrusionstore pkh 256
absorbload pkh 256
absorbload u 256
absorbload salt 512
```

```
absorbex
extrusionex
extrusionstore seed_SE 512  // 生成seed_SE
extrusionstore k 256

absorb seed_SE 512
// 拆分出S',E',E''
extrusion S' xxx xx true
extrusionex
extrusionstore S' xxx
extrusionstore E' xxx
extrusion E' xxx xx true
extrusionex
extrusionstore E' xxx
extrusionstore E'' xxx

matmul S' A E'
matmul S' B E''
matadd V u
absorb B' xxx xx true
absorbload C false
absorbload salt false
absorbload k false
extrusionex
extrusionstore ss 256
```

Decapsulation

```
matmul  -B' S C // decode 就不用了吧
absorbload pkh 256 true
absorbload u 256 false
absorbload salt 512 false
extrusionex
extrusionstore seed'_SE 512
extrusionstore k'

absorb B' xxx xx true
absorbload C false
absorbload salt false
absorbload k false
extrusionex
extrusionstore ss 256

absorb seed_SE 512
// 拆分出S',E',E''
extrusion S' xxx xx true
extrusionex
extrusionstore S' xxx
extrusionstore E' xxx
extrusion E' xxx xx true
extrusionex
extrusionstore E' xxx
extrusionstore E'' xxx
```

```
matmul S' A E'
matmul S' B E''
matadd V u
absorb B' xxx xx true
absorbload C false
absorbload salt false
absorbload k false
extrusionex
extrusionstore ss 256
```