**# of Calculations analysis:**

**Toeplitz by Vector**

This function performs expand Toeplitz + matrix by vector

Since it’s packed in words, there are only 256X4 multiplications

256x4:

OR + 2 \* shift + AND + XOR

256:

2\* Shift + 2\* AND

1 neg

**toeplitzMatrix (Expansion**):

256X4:

2 shifts + 1 if

1 OR

256:

Shift + AND

**matByVec**:

256x4:

AND

256:

2 shifts + 2 ANDS + minus + XOR

**Add**: TO ADD

**Toeplitz\_party1**:

256:

XOR

toeplitzByVec,

2\*Add

**Toeplitz\_party 2**: TO ADD, both part 1 and 2

To add:

Third phase functions

SC functions

**Communication analysis**:

**topelitz\_Party1**:

Receive 256 uint64\_t bits

Send 2 x 256 uint64\_t bits

: