COSIC WEB

COSIC
CRYPTOGRAPHY & CYBER SECURITY

PAPER

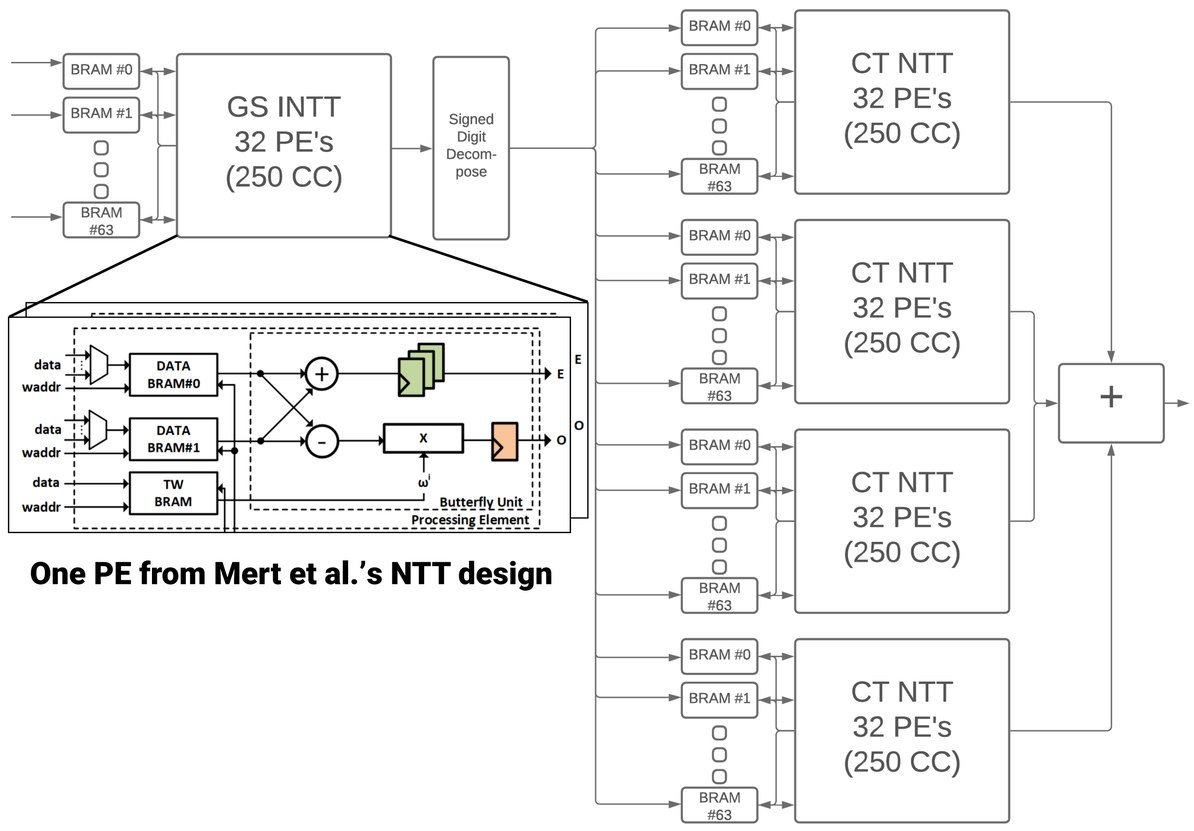
FHEW Hardware Accelerator

FHEW Algorithm From A Hardware Perspective

- **ACC:** made up of 2 vectors of size N=1024
- **Secret Key:** an array of *512*1024*2*23*2*2*4* values
- **a:** vector of *512* values
- **Result:** ACC, updated with $a_i * s_i$ for i=0...*512*−1

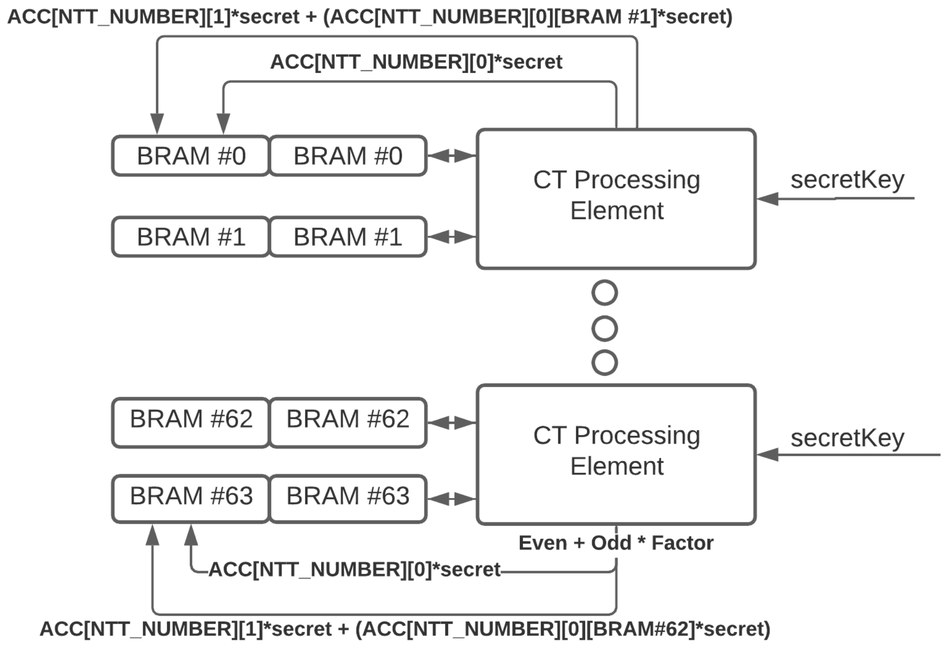
```
1  begin
2    for i = 0, 1, ...512 − 1 do
3      for j = 0, 2 − 1 do
4        c_j = ⌊a_i / B_r^j⌋ mod B;
5        if c_j > 0 then
6          for k = 0, 2 − 1 do
7            CoefACC[k] = INTT(ACC[k]);
             // 512*2*2=2048 INTTs
8            dcmp[k][3:0] = SignedDigitDecompose(CoefACC[k]);
9            for l = 0, 1, ...4 − 1 do
10             evalACC[k][l] = NTT(dcmp[k][l]);
               // 512*2*2*4=8192 NTTs
11           end
12         end
13         for k = 0, 2 − 1 do
14           ACC[k] = 0;
15           for l = 0, 1, ...4 − 1 do
16             for m = 0, 2 − 1 do
17               ACC[k] += evalACC[m][l] * SK[k][l][m];
                 // 512*2*2*4*2=16384 pointwise mult.
18             end
19           end
20         end
21       end
22     end
23   end
24   Return ACC;
25 end
```

Our FHEW Hardware Design



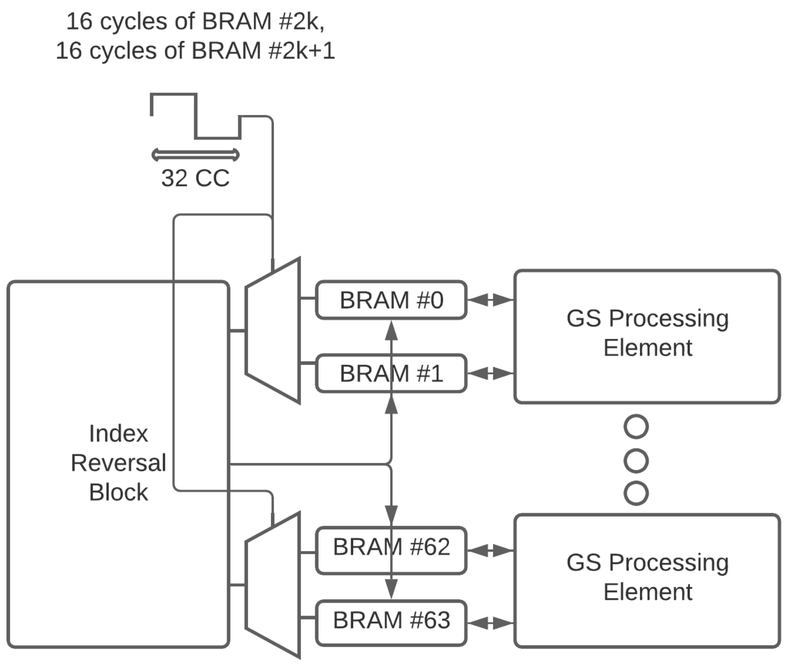
One PE from Mert et al.'s NTT design

Secret Key Multiplication integrated with CT NTT



Bitreversal modification of Mert et al.'s design

- **Significant Modification required for FHEW/External Product**



Results

Task	Input	Add $a_i * s_i$ to **ACC**	Output	1/16th Bootstrap
µs	20.52	36.16	20.49	1143.27

TABLE 4.1: Simulation run time

Frequency	WNS	LUT	FF	BRAM	DSP
100MHz	1.595 ns	133971	56565	146	768

TABLE 4.2: Implementation results for 1 INTT and 2 NTT run

RESEARCH TEAM

Jonas Bertels, Michiel Van Beirendonck, Furkan Turan
Ingrid Verbauwhede

FUNDING

European Commission | Horizon 2020 European Union funding for Research & Innovation

DPRIVE DATA PROTECTION IN VIRTUAL ENVIRONMENTS

erc

KU LEUVEN

https://www.esat.kuleuven.be/cosic/

@CosicBe

ESAT