PARALLELIZATION OF FULLY HOMOMORPHIC DATA ENCODING

JESS WOODS

COMPUTER SCIENCE RESEARCH
$f(d)$
\[ d_1 + d_2 = d_1 + d_2 \]
\[ d_1 \cdot d_2 = d_1 \cdot d_2 \]
THE SCHEME

Size & Security Parameters

Key Generation

Public
Private

Encode

d

Decode

d

d
\((a + b) \times (c + d)\)
$d$

$D$e$c$ode

$D$e$c$ode$

$d$
PROBLEMS
THEORY SOLUTION: BATCHING
IMPLEMENTATION SOLUTION: CPU
IMPLEMENTATION SOLUTION: GPU
IMPLEMENTATION SOLUTION: FPGA
MY RESEARCH