OOKAMI PROJECT APPLICATION

Date: 10/04/22

Project Title: Exploiting parallelism to accelerate fully homomorhic encryption

Usage:

☒ Testbed

☐ Production

Principal Investigator: Prof. Alex Veidenbaum

University/Company/Institute: UC Irvine

Mailing address including country:
3056 Bren Hall
University of California
Irvine, CA 92697-3435

Phone number: 949-824-6188

Email: alexv@ics.uci.edu

Names & Email of initial project users: Sam Pyankov, spyankov@uci.edu
Titus Trifan, mtrifan@uci.edu

Usage Description:
The goal of this project is to explore using parallelism in Fully Homorphic Encryption (FHE) applications and its effect on performance. Performance is a major hurdle in the adoption of FHE schemes which promise secure and private computation over encrypted data. There are multiple opportunities for parallel execution in the critical bootstrapping function of FHE - two levels of nested OPENMP parallelism as well as SIMD parallelism. At the next level, we want to explore application parallelism via MPI when using parallelised FHE Our preliminary experience is that results vary widely depending on processors and compilers used. We would like to evaluate our approach with the recent processors available at the Stony Brook Center to better understand the issues.

Computational Resources:

Total node hours per year: 15,000

Size (nodes) and duration (hours) for a typical batch job: 1-4, initially 15min duration

Disk space (home, project, scratch): 16GB home, scratch initially negligible

Personnel Resources (assistance in porting/tuning, or training for your users**):**

Required software:

Compilers, TFHE library.

If your research is supported by US federal agencies:

Agency:

Grant number(s):

Production projects:

Production projects should provide an additional 1-2 pages of documentation about how
(a) the code has been tuned to perform well on A64FX (ideally including benchmark data comparing performance with other architectures such as x86 or GPUs)
(b) it can make effective use of the key A64FX architectural features (notably SVE, the high-bandwidth memory, and NUMA characteristics)
(c) it can accomplish the scientific objectives within the available 32 Gbyte memory per node