Kotaro MATSUOKA

matsuoka.kotaro.85m@st.kyoto-u.ac.jp (Primary)
matsuoka.kotaro@gmail.com (Secondary)
@nimdanaoto
https://www.nindanaoto.dev/
https://nindanaoto.github.io/ (Some slides)
https://github.com/nindanaoto
Integrated Systems Engineering Laboratory, Course of Communications and Computer Engineering, Graduate School of Informatics, Kyoto University, Yoshida-honmachi, Sakyo-ku, Kyoto, 606-8501, Japan

Summary

I am intensely interested in Privacy-Preserving Computing, particularly secure logic circuit evaluations using homomorphic encryption (HE) with fully homomorphic encryption over the torus (TFHE). At USENIX Security 2019 [4], I presented as the first author about a CPU circuit emulation over TFHE. In this work, the CPU ran at the maximum frequency of 1.25 Hz using eight V100 GPUs. The surprisingly slow evaluation speed of FHE prompted me to research further on FHE and hardware acceleration for FHE to make secure function evaluations faster from an implementation perspective.

Education

2023 – present — **PhD. student & Japan Society for the Promotion of Science Research Fellowship for Young Scientists, Kyoto University**

2021 – 2023 — **M.Sc. Informatics, Kyoto University**, Development of FPGA-based TFHE accelerator.
Thesis title: *HOGE: A Fast FPGA Implementation Using Radix-32 Four-Step NTT for a Homomorphic Logic Gate of TFHE*.

2017 – 2021 — **B.Eng. Electric and Electrical Engineering, Kyoto University**, Numerical Electromagnetic Simulation.
Thesis title: *Time varying electromagnetic field simulation of superconducting wires containing magnetic materials based on $H - \varphi - \Psi$ method*.

Publications

[1] **K. Matsuoka**, S. Bian, and T. Sato, "HOGE: Homomorphic gate on an FPGA," in *29th Asia and South Pacific Design Automation Conference (ASP-DAC)*, 2024, pp. 325–332.

[2] K. Suemitsu, **K. Matsuoka**, T. Sato, and M. Hashimoto, "Logic locking over TFHE for securing user data and algorithms," in *29th Asia and South Pacific Design Automation Conference (ASP-DAC)*, 2024, pp. 600–605.

[3] R. Banno, **K. Matsuoka**, N. Matsumoto, S. Bian, M. Waga, and K. Suenaga, "Oblivious online monitoring for safety LTL specification via fully homomorphic encryption," in *Computer Aided Verification*, S. Shoham and Y. Vizel, Eds., Cham: Springer International Publishing, 2022, pp. 447–468, ISBN: 978-3-031-13185-1. URL: https://link.springer.com/chapter/10.1007/978-3-031-13185-1_22.

[4] **K. Matsuoka**, R. Banno, N. Matsumoto, T. Sato, and S. Bian, "Virtual secure platform: A Five-Stage pipeline processor over TFHE," in *30th USENIX Security Symposium (USENIX Security 21)*, USENIX Association, Aug. 2021, pp. 4007–4024, ISBN: 978-1-939133-24-3. URL: https://www.usenix.org/conference/usenixsecurity21/presentation/matsuoka.

[5]**K. Matsuoka**, Y. Hoshizuki, T. Sato, and S. Bian, "Towards better standard cell library: Optimizing compound logic gates for TFHE," in *Proceedings of the 9th on Workshop on Encrypted Computing & Applied Homomorphic Cryptography*, ser. WAHC '21, Virtual Event, Republic of Korea: Association for Computing Machinery, 2021, pp. 63–68, ISBN: 9781450386562. DOI: 10.1145/3474366.3486927.

[6]**K. Matsuoka**, Y. Yushima, R. Hayakawa, R. Kawasaki, K. Hayashi, and M. Kaneko, "An RFID tag identification protocol via boolean compressed sensing," *IEICE Communications Express*, vol. 5, no. 5, pp. 118–123, 2016. DOI: 10.1587/comex.2016XBL0012.

Invited Talk

[7]**K. Matsuoka**, R. Banno, N. Matsumoto, T. Sato, and S. Bian, *Virtual Secure Platform: A Five-Stage Pipeline Processor over TFHE*, (Japanese Web Page), 2022. URL: https://www.ipsj.or.jp/event/fit/fit2022/FIT2022_program/data/html/event/event_TCS5-2.html.

[8]**K. Matsuoka**, R. Banno, N. Matsumoto, T. Sato, and S. Bian, *Virtual Secure Platform: A Five-Stage Pipeline Processor over TFHE (from Usenix Security 2021)*, (Japanese Web Page), 2021. URL: https://www.ieice.org/~isec/wcis/wcis2021/Workshop%20on%20Cryptography%20and%20Information%20Security%202021.htm.

Skills

Languages	Japanese, English
Coding	C++, Chisel, Python, CUDA, Verilog, …
Misc.	Robotics, PCB design, Assembling desktop PC, Basic Linux operation skills…

Software Contributions

TFHEpp	C++ CPU implementation of TFHE from scratch (equipped with Circuit Bootstrapping) https://github.com/virtualsecureplatform/TFHEpp
kvsp	CPU emulation over TFHE (developed as a joint work with my friends [4]) https://github.com/virtualsecureplatform/kvsp
cuFHE	Forked CUDA implementation of TFHE (maintained and expanded functionality) https://github.com/virtualsecureplatform/cuFHE
HOGE	FPGA implementation of TFHE https://github.com/virtualsecureplatform/HOGE
Iyokan	Logic circuit execution engine for TFHEpp and cuFHE (developed as a joint work [4]) https://github.com/virtualsecureplatform/Iyokan
Sudachi	Logic circuit execution engine for TFHEpp using Taskflow https://github.com/virtualsecureplatform/Sudachi
Tangor	Logic circuit execution engine for HOGE using StarPU https://github.com/virtualsecureplatform/HOGE

Invented Patents (Not holding rights)

[9]Y. Hoshizuki and **K. Matsuoka**, "Encryption processing device and encryption processing method," Patent Application US 2024/0048353 A1, Feb. 2024.

[10]Y. Hoshizuki and **K. Matsuoka**, "Encryption processing device and encryption processing method," Patent Application US 2024/0039698 A1, Feb. 2024.

[11]Y. Hoshizuki and **K. Matsuoka**, "Encryption processing device and encryption processing method," Patent Application US 2024/0022395 A1, Jan. 2024.

Miscellaneous Experience

Awards and Achievements

2019 **NHK Student Robot Contest, First Place** https://official-robocon.com/history/gakusei/about/history/twentyeight/(Japanese Page, 京都大学／機械研究会 is our team, NHK is a Japanese public broadcaster)

ABU Asia-Pacific Robot Contest, Best Eight http://aburobocon2019.mnb.mn/en/news/show/74 (Japan is our team, ABU is short for Asia-Pacific Broadcasting Union)

2020 **Super Creators Certified under Exploratory IT Human Resources Project, METI** https://www.meti.go.jp/english/press/2020/0528_002.html (METI is short for The Ministry of Economy, Trade and Industry)

FY2019 President's Award, Kyoto University As Kyoto University Mechatronics Creators (Kikaiken) for results in NHK and ABU Robot Contests, https://www.kyoto-u.ac.jp/sites/default/files/inline-files/210317-presidents-award-fddb15c03a57f22385761b7cdbfd48ff.pdf

2021 **FY2020 President's Award, Kyoto University**, As Virtual Secure Platform development team for the academic result [4], https://www.kyoto-u.ac.jp/en/news/2021-03-19-0

Teaching

2020-2023 **Instructor about TFHE in Security Camp** Security Camp is a 5-day educational event co-hosted by IPA (Information-technology Promotion Agency), an affiliated organization to METI. https://www.ipa.go.jp/en/about/it-talents/security-camp.html