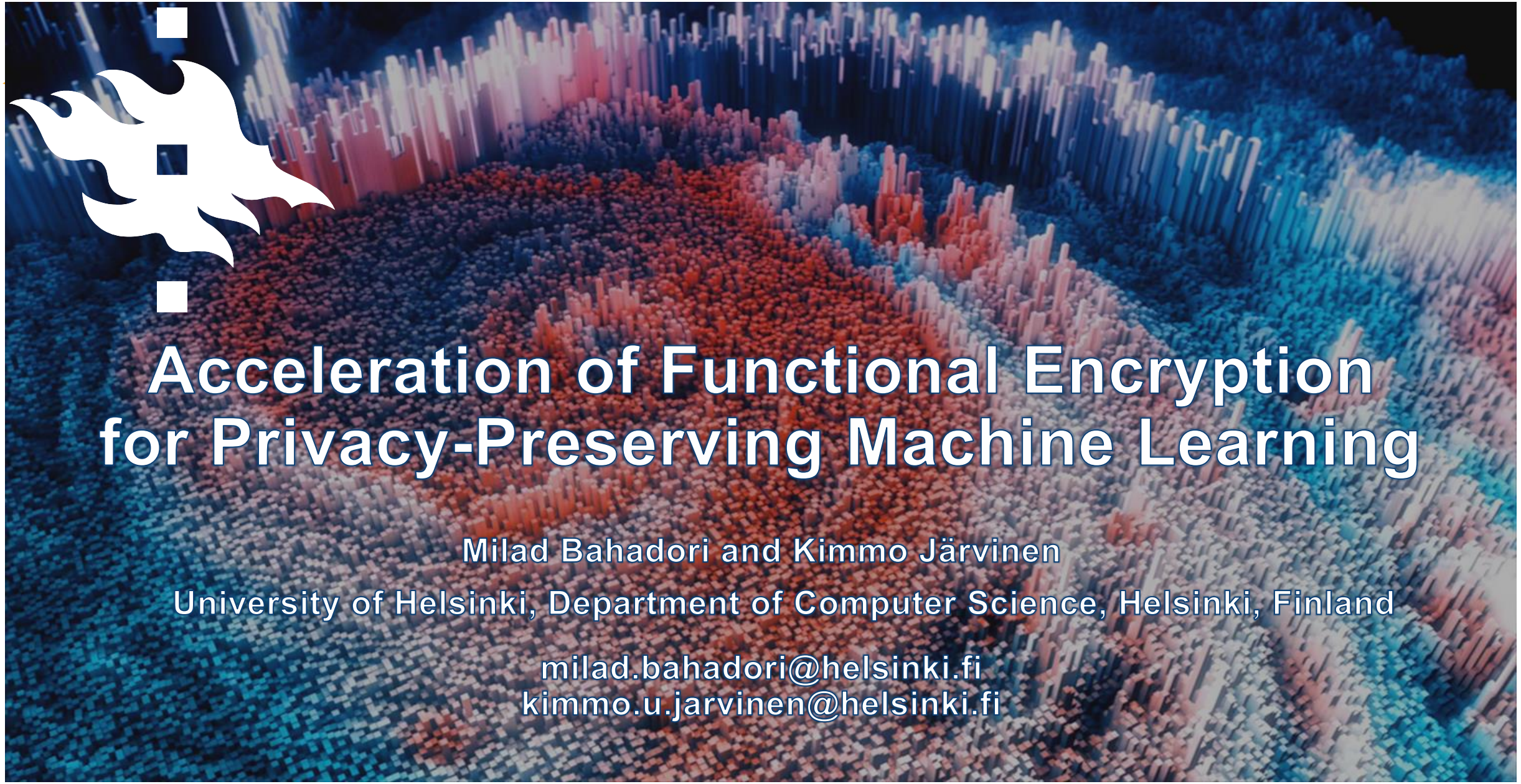


Acceleration of Functional Encryption for Privacy-Preserving Machine Learning

Milad Bahadori and Kimmo Järvinen

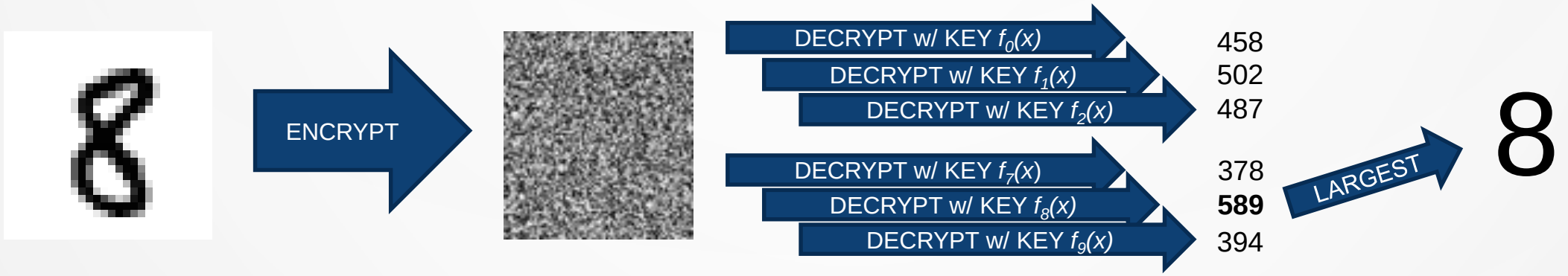
University of Helsinki, Department of Computer Science, Helsinki, Finland

milad.bahadori@helsinki.fi
kimmo.u.jarvinen@helsinki.fi

FUNCTIONAL ENCRYPTION (FE)

Cryptosystems where decryption does not give the plaintext x but $f(x)$

- Show great promise for privacy-enhancing technologies
- Different keys allow computing different functions
- In practice, very limited functions (linear or quadratic) are feasible
- Statistics, simple machine learning or pattern recognition applications are possible



FUNCTIONAL ENCRYPTION ACCELERATION

FE schemes are computationally heavy

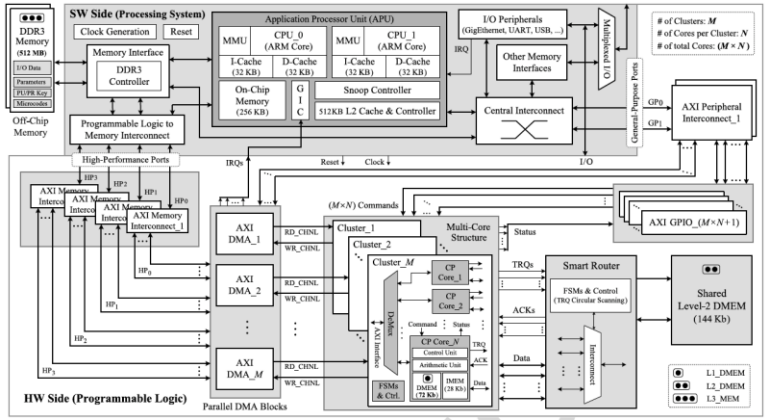
- E.g., the MNIST handwritten digit classification from the previous slide takes about 20 seconds per image (Stopar et al., ESORICS 2019)

HW/SW codesign on reprogrammable SoC (e.g., Xilinx UltraScale+) combines the best of hardware and software

- Several parallel accelerator cores on HW
- SW for control, table searches, and less critical operations

We have designed **several accelerators for FE**

- Multi-input FE based on Paillier encryption
- FE for quadratic functions based on pairings and discrete logs



FENTEC

M. Bahadori, K. Järvinen: ”A Programmable SoC-Based Accelerator for Privacy-Enhancing Technologies and Functional Encryption”, IEEE Transactions on VLSI Systems 28(10):2182-2195, 2020.