# 5th HomomorphicEncryption.org Standards Meeting

September 1-2, 2022 Geneva, Switzerland

**Organized by**

TUNE INSIGHT

inpher

ITU

# HomomorphicEncryption.org

- HomomorphicEncryption.org: an open consortium started in 2017 with industry, government and academia to standardize homomorphic encryption

  **Steering Committee.** Kristin Lauter (Facebook), Vinod Vaikuntanathan (MIT/Duality Technologies), Kim Laine (Microsoft), Kurt Rohloff (NJIT/Duality Technologies), Jung Hee Cheon (Seoul National University/CryptoLab), Shai Halevi (Algorand Foundation), Lily Chen (observer, NIST)

- 3 white papers:
  - APIs: This white paper discusses the design of API standards for homomorphic encryption.
  - Security: This white paper discusses the security standards for homomorphic encryption.
  - Applications: This white paper discusses the motivating applications for homomorphic encryption.
- Due to COVID there has been no meetings over the past 2 years

ZAMA HEAAN CRYPTO LAB SANDBOXAQ inpher TUNE INSIGHT ITU

**ISO** standardization of FHE

**DARPA-DPRIVE** has been running

**NIST PQC** selected 3 lattice-based schemes

**2022 Gödel Prize** is awarded to the following papers

ISO

ICS

## ISO/IEC AWI 18033-8

**Information security — Encryption algorithms — Part 8: Fully Homomorphic Encryption**


Algorithms to be Standardized

| Public-Key Encryption/KEMs | Digital Signatures |
|---|---|
| CRYSTALS-KYBER | CRYSTALS-Dilithium |
| | FALCON |
| | SPHINCS+ |

European Association for Theoretical Computer Science

About EATCS
How to Join
Organization
Bulletin
Conferences
Awards
Publications

**The 2022 Gödel Prize**

The 2022 Gödel Prize is awarded to the following papers

- Zvika Brakerski, Vinod Vaikuntanathan: Efficient Fully Homomorphic Encryption from (Standard) LWE. FOCS 2011: 97-106. SIAM Journal of Computing 43(2): 831-871 (2014)
- Zvika Brakerski, Craig Gentry, Vinod Vaikuntanathan: (Leveled) fully homomorphic encryption without bootstrapping. ITCS 2012: 309-325. ACM Transactions on Computation Theory 6(3): 13:1-13:36 (2014)

- New FHE initiatives (benchmarks, challenges): **HEBench**, **FHE.org**
- Progress in **hardware** and **software** implementations (efficiency and usability)

ZAMA HEAAN CRYPTO LAB SANDBOXAQ inpher TUNE INSIGHT ITU

# This workshop (5th edition)

- First time in Europe

**Organizing Committee.**

Juan R. Troncoso-Pastoriza — TUNE INSIGHT

Mariya Georgieva — inpher

Bastiaan Quast — ITU

- Around 80 registrations
- 1 keynote talk
- 24 invited short talks
- 11 accepted demo/posters

ZAMA HEAAN CRYPTO LAB SANDBOXAQ inpher TUNE INSIGHT ITU

# Agenda

September 1st

2 sessions on **Software tools and libraries**

1 sessions on **HEBench** and **Upcoming competitions in HE**

**Demo/poster presentations (2nd floor)**


September 2nd

Keynote: **The past, present and future of FHE by Prof. Zvika Brakerski**

2 sessions on **Hardware computing platforms and acceleration**

1 sessions on **Industry applications and use cases**

1 sessions on **Liaisons to standards communities** (ISO and NIST)

1 sessions on **Security and precision**

ZAMA HEAAN CRYPTO LAB SANDBOXAQ inpher TUNE INSIGHT ITU

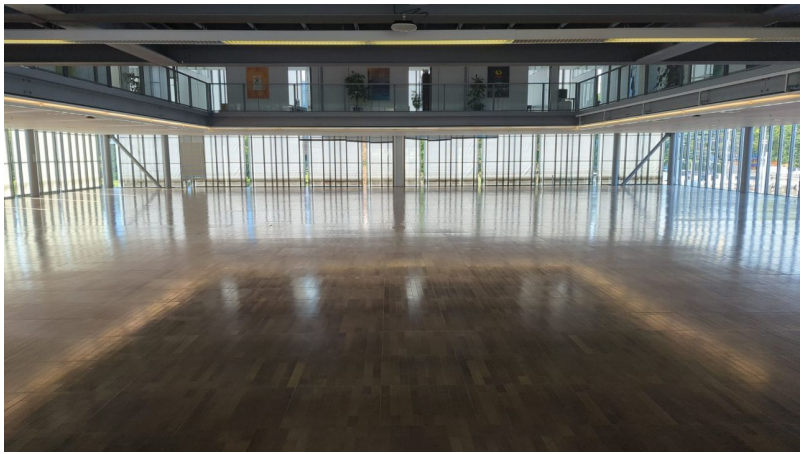
# Thanks to our sponsors






# Poster session

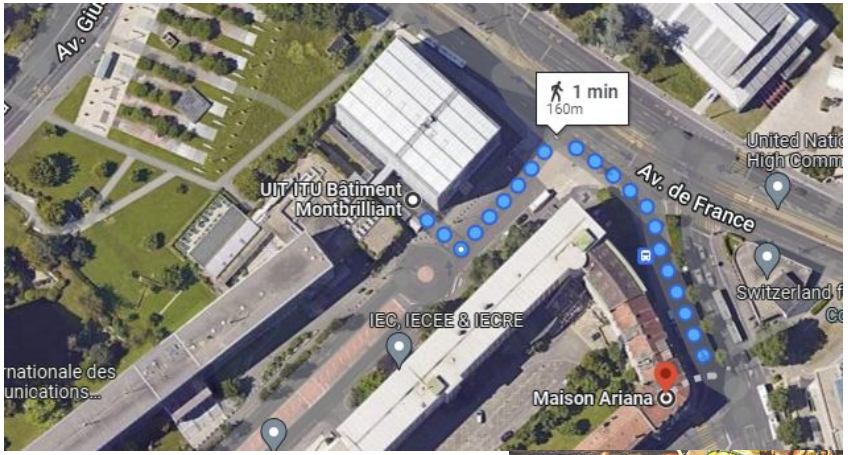
The poster session will take place at the second floor, with a cocktail



You don’t need to move your posters

# Reception

After the poster session, we will meet at the entrance of the Montbrillant building at 19:30, and we will walk to the restaurant




Maison Ariana
Rue de Montbrillant 83


ZAMA HEAAN CRYPTO LAB SANDBOXAQ inpher TUNE INSIGHT ITU

# 5th HomomorphicEncryption.org Standards Meeting

September 1-2, 2022 Geneva, Switzerland

ZAMA HEAAN CRYPTO LAB SANDBOXAQ™ inpher TUNE INSIGHT ITU

# Agenda (September 1st)

| | |
|---|---|
| 12:00-13:00 | **Registration and poster set up** |
| 13:00-13:15 | **Intro and welcome** |
| 13:15-14:15 | **Software tools and libraries (I)**<br>– *HEaaN: Encrypted Computation Library*. Junbum Shin (CryptoLab)<br>– *An overview of the Concrete Framework*. Damien Ligier, Ilaria Chillotti (Zama)<br>– *FHE Transpiler by Google*. Shruthi Gorantala (Google) - Online |
| 14:15-14:30 | **Coffee break** |
| 14:30-15:50 | **Software tools and libraries (II)**<br>– *HE libraries and software tools*. Martin Zuber (CEA)<br>– *OpenFHE library*. Yuriy Polyakov (Duality)<br>– *GenoPPML framework for an end-to-end privacy-preserving genomics ML*. Mariya Georgieva, Sergiu Carpov, Nicolas Gama, Dimitar Jetchev (Inpher)<br>– *Tune Insight's distributed analytics platform and the Lattigo library*. Jean-Philippe Bossuat, Juan R. Troncoso-Pastoriza (Tune Insight) |
| 15:50-16:05 | **Coffee break** |

ZAMA HEAAN CRYPTO LAB SANDBOXAQ inpher TUNE INSIGHT ITU

# Agenda (September 1st - cont)

| | |
|---|---|
| 16:05-16:35 | **Benchmarking**<br>*– HEBench – A framework for benchmarking HE workloads. The Homomorphic Encryption Benchmarking Community.*<br>Flavio Bergamaschi, Ernesto Zamora Ramos (Intel) |
| 16:35-17:05 | **Upcoming competitions in HE**<br>*– iDash: A community's effort to benchmark and accelerate the development of homomorphic encryption solutions to protect biomedical data sharing and analysis.* Xiaoqian Jiang, Arif O.Harmanci (UTHealth), Miran Kim (Hanyang University) - Online<br>*– FHE.org challenge*. Pascal Paillier (Zama) - Online |
| 17:05-17:20 | **HE Demos and posters lightning talks** |
| 17:20-17:30 | **First day ending remarks** |
| 17:30-18:30 | **Demo/Poster and networking session (2nd floor)** |
| 19:30-22:00 | **Welcome dinner and networking** |

ZAMA HEAAN CRYPTO LAB SANDBOXAQ inpher TUNE INSIGHT ITU

# Poster Session

| | |
|---|---|
| *Practical Integrity Protection for FHE.*<br>Christian Knabenhans, Alexander Viand, Anwar Hithnawi | *PIE: p-adic Encoding for High-Precision Arithmetic using Homomorphic Encryption.*<br>Gaetan Delavignette, Luke Harmon, Arnab Roy, David Silva |
| *Field Instruction Multiple Data.*<br>Khin Mi Mi Aung, Enhui Lim, Jun Jie Sim, Benjamin Hong Meng Tan, Huaxiong Wang, Sze Ling Yeo | *Affordable and Practical Acceleration of CKKS-based Fully Homomorphic Encryption.*<br>Rashmi Agrawal, Leo de Castro, Rabia Yazicigil, Anantha Chandrakasan, Vinod Vaikuntanathan, Chiraag Juvekar, Ajay Joshi |
| *MOSFHET: Optimized Software for FHE over the Torus.*<br>Antonio Guimarães, Edson Borin, and Diego F. Aranha | *The Lattigo library: Multiparty Homomorphic Encryption in Go.*<br>Jean-Philippe Bossuat, Christian Mouchet, Juan R. Troncoso-Pastoriza |
| *OpenFHE: Open-Source Fully Homomorphic Encryption Library.*<br>Ahmad Al Badawi and Jack Bates and Flavio Bergamaschi and David Bruce Cousins and Saroja Erabelli and Nicholas Genise and Shai Halevi and Hamish Hunt and Andrey Kim and Yongwoo Lee and Zeyu Liu and Daniele Micciancio and Ian Quah and Yuriy Polyakov and Saraswathy R.V. and Kurt Rohloff and Jonathan Saylor and Dmitriy Suponitsky and Matthew Triplett and Vinod Vaikuntanathan and Vincent Zucca | *Secure Collaborative Design of Experiments with Homomorphic Encryption.*<br>Jin Chao, Khin Mi Mi Aung, Zhang Xin |
| | *An FHE-based framework to help Catalan Social Entities.*<br>Sergi Rovira, Vanesa Daza |
| *Multi-Key Homomorphic Encryption for Collaborative Camera Attribution.*<br>Alberto Pedrouzo-Ulloa, Fernando Pérez-González, David Vázquez-Padín | *HECO: Automatic Code Optimizations for Efficient Fully Homomorphic Encryption.*<br>Alexander Viand, Patrick Jattke, Miro Haller, Anwar Hithnawi |

ZAMA HEAAN CRYPTO LAB SANDBOXAQ inpher TUNE INSIGHT ITU

# Ending Remarks

Huge progress and proliferation of **software tools and libraries**

- Increased performance and versatility in active FHE Libraries
- Multiple approaches to use the most adapted scheme for each problem
- ML applications as the showcase
- Friendlier interfaces for non-security experts and data scientists
- And also progress in compilers/transpilers

Efforts on standardizing and homogenizing benchmarking and evaluation, with **HEBench**

**Upcoming competitions in HE**, also based on the benchmarking frameworks

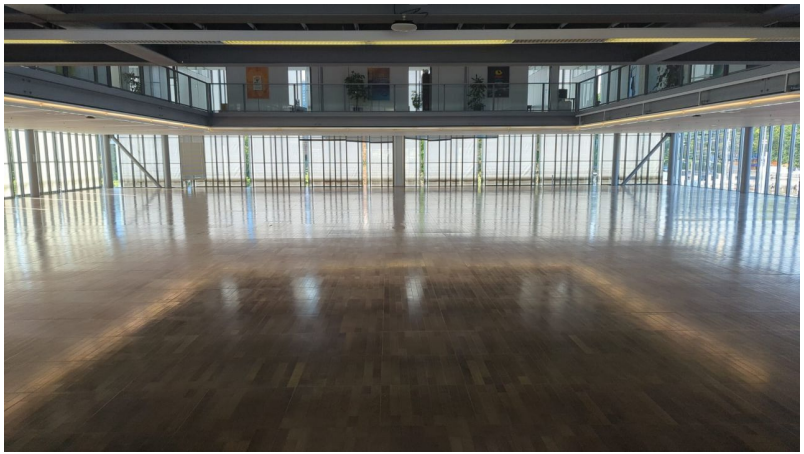
- iDash http://www.humangenomeprivacy.org/2022/
- FHE.org

Joint community with big impulse and effort

ZAMA HEAAN CRYPTO LAB SANDBOXAQ inpher TUNE INSIGHT ITU

# Poster session

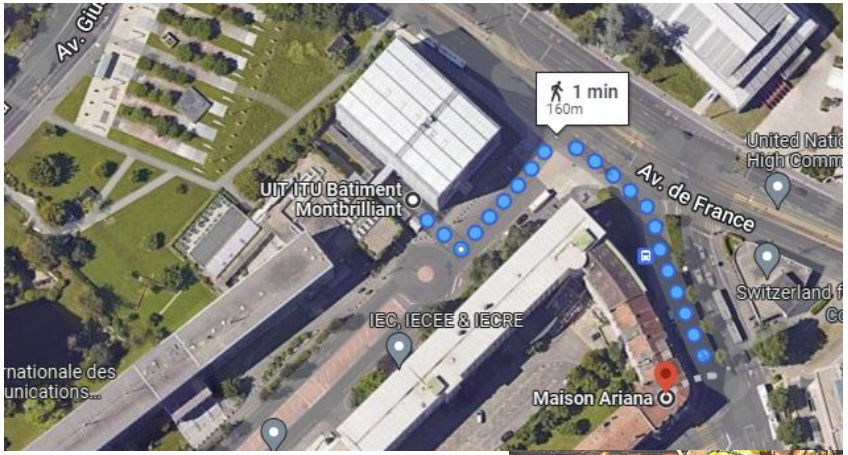
The poster session will take place at the second floor, with a cocktail



You don’t need to move your posters

# Reception

After the poster session, we will meet at the entrance of the Montbrillant building at 19:30, and we will walk to the restaurant




Maison Ariana
Rue de Montbrillant 83


ZAMA HEAAN CRYPTO LAB SANDBOXAQ inpher TUNE INSIGHT ITU

# Agenda (September 2nd)

| | |
|---|---|
| 8:00-9:00 | **Registration and networking breakfast** |
| 9:00-9:15 | **Intro and welcome** |
| 9:15-10:15 | **Keynote talk**<br>– *The past, present and future of FHE*. Zvika Brakerski (Weizmann Institute of Science) |
| 10:15-11:15 | **Hardware computing platforms and acceleration for HE (I)**<br>– *Hardware Acceleration of FHE*. Pradip Bose, Omri Soceanu, Nir Drucker, John Buselli (IBM) - Online<br>– *Accelerating FHE with Silicon Photonics*. Florent Michel (Optalysys)<br>– *Full circuit FHE acceleration on Cornami HW*. Vineet Chadha (Cornami) |
| 11:15-11:45 | **Coffee break / posters / networking** |
| 11:45-12:50 | **Hardware computing platforms and acceleration for HE (II)**<br>– *DPRIVE: The rise of novel computing platforms for FHE*. Rosario Cammarota (Intel, online), Kurt Rohloff (Duality)<br>– *Hardware acceleration for FHE*. Ingrid Verbauwhede (KULeuven)<br>– *GPU acceleration of HE*. Erkay Savas (Sabanchi University) - Online |
| 12:50-13:45 | **Lunch** |

ZAMA HEAAN CRYPTO LAB SANDBOXAQ inpher TUNE INSIGHT ITU

# Agenda (September 2nd - cont)

| | |
|---|---|
| 13:45-14:45 | **Industry applications and use cases**<br>– *The use of PETs for data aggregation*. Jihoon Cho, Kyoohyung Han (Samsung)<br>– *PETs applications in Asia Pacific*. Tim Scott (Deloitte Australia) - Online<br>– *Contributions and Case Studies from the UN Privacy-Enhancing Technologies Task Team*. Raphaël de Fondeville (UN PET Lab) |
| 14:45-15:45 | **Liaisons to standards communities**<br>– *ISO Updates on the development of ISO/IEC JCT1 18033 – Part 8, FHE*. Rosario Cammarota (Intel) - Online<br>– *Toward recommendations for advanced cryptography*. Luís Brandão (NIST/Strativia) |
| 15:45-16:05 | **Coffee Break / posters / networking** |
| 16:05-17:05 | **Security and precision of FHE**<br>– *Updates on FHE Security standardisation efforts*. Rachel Player (RHUL)<br>– *Security on FHE*. Nicolas Gama (SandboxAQ)<br>– *On the precision loss in approximate encryption*. Anamaria Costache (NTNU) |
| 17:05-17:35 | **Status updates of the HE.org standards community** |
| 17:35-17:50 | **Sneak peek of the next meeting** |
| 17:50-18:00 | **Conclusions and next steps** |
| 18:00 | **Farewell** |

ZAMA HEAAN CRYPTO LAB SANDBOXAQ inpher TUNE INSIGHT ITU

# HES in Seoul ($6^{th}$)

- Homomorphic Encryption Standardization Workshop
  - Organizers: Jung Hee Cheon (SNU/CryptoLab), Jihoon Cho (Samsung)
  - Venue: Seoul, South Korea

- Date: Mar 23 (Thu) – 24 (Fri)
  - fhe.org: Mar 26 (Sun), Tokyo
  - Real World Crypto: 27 (Mon) - 29 (Wed), Tokyo

- Program: Follow HES Geneva *and*
  - DeepDive$^{Tech}$ and Experience$^{Compilers/APIs}$
  - Standard/Libraries update with HEBench Results
  - Success Stories on HE applications
  - Community building

- Any suggestions will be appreciated

# Ending Remarks (2nd day)

FHE has come a long way; the limits now are the **secrets of the universe**

Next **efficiency revolution in FHE**: combination of algorithmic improvements and **novel hardware platforms**, bringing overheads from $10^6$x down to ~1x

Industry applications:

- Opportunities and challenges posed by different **regulatory frameworks** (need to involve regulators)
- Identified key industries, but still need of **education and awareness** (best practices and design patterns)
- Relation to other techniques (FL, DP, MPC, TEEs,...): generalizations/synergies with other PETs communities

Ongoing **standards**

- ISO/IEC JCT1 18033 – Part 8, FHE / NIST-PEC (NIST Report on FHE?) / ITU-T SG-17
- Related activities and synergies (Confidential Computing, IEEE Hardware Security,...)
- Still work to be done in standardization for our community (APIs, applications, HE hardware?)

**Security and precision**:

- Lattice estimator (security) <-> Noise estimator (correctness/accuracy)?
- ISO/IEC JTC1 SC27 WG2 whitepaper on parameter selection
- Confidence on current security standards vs ongoing attack efforts

Software tools and benchmarking: **HEBench** https://hebench.org Join us: https://hebench.org/join-us

Reforged community with renewed traction and impulse, with new working groups

ZAMA HEAAN CRYPTO LAB SANDBOXAQ inpher TUNE INSIGHT ITU

# Thanks!

See you in Korea

ZAMA HEAAN CRYPTO LAB SANDBOXAQ inpher TUNE INSIGHT ITU