KU LEUVEN

COSIC

Computing on Encrypted Data Hardware Day

Ingrid Verbauwhede

Stanford, June 26, 2025

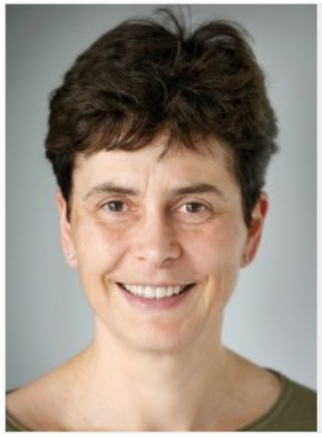
Google

erc

How it started:
ERC Advanced Grant
“Hardware acceleration for computing on Encrypted Data”

MAIN FUNDING INFO

- Programme Funding: Horizon 2020
- Sub Programme Area: ERC-2020-AdG
- Project Reference: 101020005
- From: in grant preparation
- Budget: EUR 2.425.875
- Contract type: ERC-AdG



INGRID VERBAUWHEDE

Department of Electrical Engineering

BELFORT Hardware Acceleration for Computing on Encrypted Data

This is prof. Verbauwhede's second ERC grant (Cathedral).

READ MORE

How it started: 10 years anniversary
Early work: Somewhat Homomorphic Encryption

Compact Ring-LWE crypto processor, 2014

YASHE CHES 2015 papers:

- “Modular Hardware Architecture for Somewhat Homomorphic Function Evaluation,” PhD work of Dr. Sujoy Sinha Roy
- “Accelerating Homomorphic Evaluation on Reconfigurable Hardware,” PhD work of Dr. Thomas Pöppelmann (in parallel)

Previous events

Leuven, May 2024

- Belfort
- Cornami
- Fabric
- Google
- Ingonyama
- Intel
- Kioxia
- Niobium
- Optalysys
- Zama

Hardware, Compilers

Today

- 0xParc
- AMD
- AWS
- Belfort
- CipherSonic
- Cornami
- Duality
- Fabric
- Google
- Intel
- LatticaAI
- Monadic DNA
- Niobium
- Nokia Bell Labs
- Optalysys
- Sunscreen

Hardware, Compilers, Applications

Program: morning

08:30 – 09:00 (30min)	**Welcome Coffee**
09:00 – 09:10 (10min)	**Welcome Talk** Ingrid Verbauwhede (Belfort / KU Leuven)
09:10 – 09:35 (25min)	**The Power of Scale** Paul Master (Cornami)
09:35 – 10:00 (25min)	**Niobium's Modular FHE Accelerator: Architecture, Market, Challenge and Directions** David Archer (Niobium Microsystems)
10:00 – 10:15 (15min)	**End-to-end encrypted group voice calls** Emad Heydari Beni (Nokia Bell Labs)
10:15 – 10:30 (15min)	**From Hardware to Private AI: Seamless Paths to Deployment** Rotem Tsabary (LatticaAI)
10:30 – 10:50 (20min)	**Coffee Break**
10:50 – 11:15 (25min)	**Lessons Learned On the Very Long Road From the First-Ever FHE Co-Design to Real-World Products** Kurt Rohloff (Duality Technologies)
11:15 – 11:40 (25min)	**FHE for all: Practical Applications on Hardware Platforms with HEIR** Shruthi Gorantala (Google) Wouter Legiest (Google & COSIC (KU Leuven))
11:40 – 12:05 (25min)	**Our Curious Adventures Enabling ProgCrypto from F(HE) to Z(K): Designing, Programming and Deploying the Verifiable Processing Unit (VPU)** Michael Gao (Fabric Cryptography)
12:05 – 14:00 (1h 55min)	**Lunch**

KU LEUVEN

Afternoon

12:05 – 14:00 (1h 55min)	**Lunch**
14:00 – 14:30 (30min)	**From Theory to Throughput: Deploying FHE in the Cloud with AMD, AW & Belfort** Girish Malipeddi (AMD) Mark Azadpour (AWS) Laurens De Poorter (Belfort)
14:30 – 14:55 (25min)	**Accelerating Secure Genomics: Tales from the FHE Trenches** Vishakh (Monadic DNA)
14:55 – 15:25 (30min)	**Coffee Break**
15:25 – 15:50 (25min)	**FrogZone** Justin Glibert (0xPARC)
15:50 – 16:05 (15min)	**FHE That Ships: Our Journey from Research to Real Deploym** Ajay Joshi (CipherSonic Labs)
16:05 – 16:20 (15min)	**Parasol: A FHE compiler pioneering circuit bootstrapping** Ravital Solomon (Sunscreen)
16:30 – 17:15 (45min)	**Panel** Ingrid Verbauwhede (Belfort, moderator) Flavio Bergamaschi (Optalysys) Alexander Viand (Intel Labs) Pankaj Rohatgi (Google)

KU LEUVEN

THANK YOU!!

- Dr. Emad Heydari Beni (Cosic & Nokia Bell Labs), co-organizer
- Maria Sal (Stanford), local knows all!
- Prof. Subhasish Mitra (Stanford), local support
- Google, local support and funding
- ERC grant, funding

- All of you here!

KU LEUVEN

Welcome!