

CBT 2025 - Thursday 25 September 2025

Meeting room – Bât. U3

Note that Welcome and keynote take place in Amphi Condat, main building (see back page)

CBT 2025 Chairs	
09:15-09:30	Welcome & Report <i>Note that Welcome and keynote take place in Amphi Condat, main building</i>
09:30-10:30	Keynote talk: Privacy: technology and policy <i>Bart Preneel</i> This talk explores the evolving landscape of privacy technologies and the policy debates that surround them. We will examine technical approaches for protecting privacy, including methods to hide communication content, techniques to protect metadata (including identities and locations), and methods to ensure privacy-preserving data processing with verifiable guarantees. Case studies such as proximity tracing, digital payments, and cryptocurrencies will illustrate both the potential and the challenges of these technologies in practice. The talk will also address tensions with government demands for exceptional access, from historical examples such as the Clipper chip and Dual EC DRBG to more recent disputes over access to content on confiscated devices and client-side scanning. We will conclude by outlining key open research challenges at the intersection of privacy, security, and policy.
10:30-10:50	Coffee/Tea Break
10:50-12:20	Session 1: Layer 2 and cryptography tools <i>Session Chair: Jordi Herrera-Joancomartí</i>
10:50-11:20	Fast Off-Chain Payments with Second-Layer Privacy <i>Sven Gnap, Kari Kostiainen and Ghassan Karame.</i>
11:20-11:50	AUPCH: Auditable Unlinkable Payment Channel Hubs <i>Mohsen Minaei, Pedro Moreno-Sanchez, Srinivasan Raghuraman, Panagiotis Chatzigiannis and Duc Le</i>
11:50-12:20	Threshold Signatures for Central Bank Digital Currencies <i>Mostafa Abdelrahman, Filip Rezabek, Lars Hupel, Kilian Glas and Georg Carle</i>
12:20-13:50	Lunch Break

13:50-15:20

Session 2: Blockchain uses and applications

Session Chair: Cristina Pérez-Solà

13:50-14:20

Blockchain-Based Lotteries via Single Secret Leader Election

Tegrid Fettuh and Oğuz Yayla

14:20-14:50

Towards a Resource Based Blockchain E-Voting System

Ricardo Almeida, Laura Ricci, Fabrizio Baiardi, Damiano Maesa, Catalin Dragan and Nishanth Sastry

14:50-15:20

Analysing the Adoption of Terms of Use in SSI Digital Wallets

Stefano Bistarelli, Chiara Luchini and Francesco Santini

15:20-15:40

Coffee/Tea Break

15:40-17:10

Session 3: Blockchain foundations

Session Chair: TBD

15:40-16:10

Multiple Selfish Miners on Nakamoto's Consensus Fruitchain, and Strongchain - An

Empirical Evaluation

Martin Perešini, Tomáš Hladký, Jakub Kubík and Ivan Homoliak

16:10-16:40

EVMpress: Precise Type Inference for Next-Generation EVM Decompilation

Jung Hyun Kim, Soomin Kim, Jaeseung Choi and Sang Kil Cha

19:00

Workshop gala dinner

