FHE: End-to-End Encryption for Everyone (Keynote Abstract)

Marc Joye[1]

[1] *Zama, Paris, France*

Keywords
Cybersecurity, Cryptography, Homomorphic Encryption

Topic

First posed as a challenge in 1978 by Rivest et al., fully homomorphic encryption (FHE)—the ability to evaluate any function over encrypted data—was only solved in 2009 in a breakthrough result by Gentry (Commun. ACM, 2010). After a decade of intense research, practical solutions have emerged and are being pushed for standardization. This talk reviews the basics behind FHE and discusses applications thereof based on the Concrete framework.

Biography

Marc Joye is a cryptographer and security technologist, and the Chief Scientist at Zama. He has been active in the field of cryptography for more than 25 years, from low-level implementations up to protocol design. He is a co-inventor of the ACJT group signature scheme and of the Joye-Libert homomorphic encryption scheme. Prior to Zama, Marc worked in a number of security companies, including as a Research Scientist at OneSpan, as a Fellow and Security Technologist at NXP Semiconductors, as a Fellow and Distinguished Scientist at Technicolor, and as a Scientific Expert at Gemalto. He has co-authored over 170 scientific papers, has more than 11,000 citations, and has filed more than 140 patent families. Marc holds a PhD in Cryptography from UCLouvain and is a member of the IACR.

C&ESAR'22: Computer & Electronics Security Application Rendezvous, Nov. 15-16, 2022, Rennes, France

URL: https://www.linkedin.com/in/marcjoye (M. Joye)