Universität St.Gallen

Computer Science Insights @HSG - School of Computer Science

Wednesday, December 7th, 2022 - 10:00, SQUARE 11-2091 (Arena)

Two Variants of Structure-Preserving Signatures and Their Applicationsl

Daniel Slamanig

Structure-preserving signatures (SPS) are pairing-based signatures that have proven to be an invaluable building block for privacy-preserving cryptographic primitives. This talk focuses on two variants of SPS. Firstly, we will take a look at SPS on equivalence classes (SPS-EQ). Instead of signing messages being vectors of group elements, SPS-EQ sign equivalence classes of the message space. We will look into natural applications of this concept, yielding conceptually novel and attractive variants of primitives such as blind signatures or compact anonymous credentials. Secondly, we will look at Threshold SPS. Those are threshold signatures satisfying the constraints imposed by SPS. They allow multiple parties to jointly sign a message, resulting in a standard, single-party SPS signature, and can thus be used as a replacement for applications based on SPS. The talk will be concluded by a discussion of open research questions. The work presented in this talk is based on joint work with a set of incredible co-authors.

Dr. Daniel Slamanig is a computer scientist working as a scientist in the Center for Digital Safety and Security of the AIT Austrian Institute of Technology in Vienna. His main research interests are in the field of cryptography, with a focus on public key cryptographic primitives, their foundations and applications. He is one of the designers of the Picnic family of post-quantum digital signature schemes, a third-round candidate in NIST's post-quantum crypto standardization project. He received his PhD in computer science in 2011 from the University of Klagenfurt, where he worked on the design of efficient (privacy-enhancing) public-key cryptography. Previously he has been a postdoctoral (2012-2015) and then senior researcher (2015-2017) in the cryptography group at IAIK Graz University of Technology.

From insight to impact.