

Graduate School Event

Thesis Defense: Towards Efficient Secure Group Messaging

Miguel Cueto Noval
Pietrzak Group

Host: Carrie Bernecky

The widespread adoption of apps like Whatsapp and Signal has translated into billions of people all around the world communicating on a regular basis by making use of services that offer end-to-end encryption and even provide security guarantees when a user's device is compromised.This was made possible by the introduction of the Double Ratchet Algorithm, which was designed for a setting where communication takes place between two parties. However, in practice, many apps offer the possibility of creating groups. The protocols they use to secure communication are inefficient for large group which has the undesirable consequence that the aforementioned apps have established limits on the group size of roughly 1000 users. This has motivated the introduction of the Messaging Layer Security (MLS) standard by the IETF which is based on a primitive called Continuous Group Key Agreement (CGKA).This primitive allows a group of users to maintain a shared secret key that is frequently rotated by the group members in order to change group membership, achieve forward secrecy (FS) and post compromise security (PCS). Most protocols are based on binary trees where the nodes are associated to a pair formed by public key and a secret key. Each leaf corresponds to one of the group members and a user knows the secret keys associated to nodes along the path from their leaf to the root. When a user wants to update their key material they have to change $ \log(N) $ many keys. This requires uploading $ \log(N) $ many ciphertexts to communicate the new keys to the rest of the group members in a way that respects the tree structure.In this thesis we study how much communication between group members is required in order to add and remove users from a group as well as in order to provide PCS when we consider CGKAs built using standard cryptographic primitives like pseudo-random functions and public-key encryption. Furthermore, we also consider the case of MLS and provide the first lower bound showing that its communication complexity is much worse than previously believed, i.e., it is very far from $ \log(N) $. Finally, we also propose a variant of MLS which provably achieves the same security properties with a much lower communication cost.

Tuesday, July 28, 2026 11:00am - 12:00pm
Moonstone Bldg / Ground floor / Seminar Room F (I24.EG.030f) and Zoom

This invitation is valid as a ticket for the ISTA Shuttle from and to Heiligenstadt Station. Please find a schedule of the ISTA Shuttle on our webpage: https://ista.ac.at/en/campus/how-to-get-here/ The ISTA Shuttle bus is marked ISTA Shuttle (#142) and has the Institute Logo printed on the side.