Public Traceability in Threshold Decryption

Nathan Papon*[1]

[1]Laboratoire Traitement et Communication de lÍnformation – Télécom Paris, Institut Mines-Télécom [Paris], Institut Polytechnique de Paris – France

Résumé

Tracing techniques have been used to identify users who have leaked their decryption keys in a secure multi-receiver encryption system. Very recently, in the field of distributed cryptography, where trust is distributed, Boneh et al. extended traitor tracing to the framework of threshold decryption, where a single user doesn't hold the whole secret to decrypt but needs to collaborate with others. However, the tracing capacity in their collusion-secure codes-based schemes is still centralized: only the authority holding the secret tracing key can perform tracing. We continue in the direction of not relying on a single entity and propose decentralizing tracing in this context so that the tracing procedure does not need to rely on any secret key and can be done by anyone. Technically, as binary collusion-secure codes only support secret tracing, we switch to robust q-ary IPP codes supporting public tracing. This requires us to generalize the bipartite threshold KEM for two users in Boneh et al.'s paper to q-partite KEM for q users. In terms of security, their static one-sided security in the binary case is not appropriate, which requires us to define an adaptive one-sided security notion for q-partite KEM to be compatible with q-ary IPP codes. Finally, we generalize the Boneh et al. construction to achieve this security notion and achieve public traceability for threshold decryption without degrading efficiency.
Collaboration with Sébastien Canard and Duong Hieu Phan

*Intervenant