# Threshold Cryptosystems

Martin Schaffer[1] <martin.schaffer@uni-klu.ac.at>

Public Key Cryptosystems (PKCs) are a widely spread mechanism to provide digital signatures, mutual authentication as well as key-exchange for symmetric algorithms. Based on asymmetric cryptosystems, PKCs require public (encryption/signature verification) and private (decryption/signature generation) key-components. Within existing PKCs a function (e.g. decryption) is normally computed by one single instance. However, what happens if we do not trust one single instance to e.g. decrypt a message? Thus, we need mechanisms to distribute functions. Multi-Party Computation with Threshold Security (T-MPC) provides protocols to add and multiply values within fields (see e.g. [2]), whereas private values remain *shared* and accessible by a qualified set of instances (based on a threshold). A special case of T-MPC are so-called *Threshold Cryptosystems* (TCs) where e.g. the decryption function of a PKC is performed over the shares of the private key. One of the first TCs has been proposed in [1] using secret sharing based on randomly chosen polynomials. Although the security of such cryptosystems mainly lies on a particular threshold, analysing and defending adversaries (e.g. adaptive chosen ciphertext attacks) is much more difficult than in PKCs that remain unshared. As a consequence we need distributed traceability-mechanisms that enable us to monitor the behaviour of every participant. Such mechanisms can include e.g. commitments and interactive-proofs respectively. Distributing PKCs is not limited to the "usage" of key components. Hence, a particular key management is required where parts of the key-life-cycle are adapted to shared usage. Selected aspects include "shared key generation", "shared update of private-keys", "shared re-encryption of old ciphertext" as well as "removal and addition of new shares". The aim here is to avoid side-effects and to keep the number of shares as minimal and flexible as possible. For a discussion on this topic we refer to our technical report [3].

[1] Y. Desmedt, Y. Frankel: *Threshold Cryptosystems*, Adv. in Crypt.: CRYPTO'89, Springer-Verlag, pp. 307-315, 1990.
[2] O. Goldreich et al.: *How to play any mental game – a completeness theorem for protocols with honest majority*, Proc. 19th ACM STOC, p. 218-229, 1987.
[3] M. Schaffer: *Managing Key-Shares in Distributed Public Key Cryptosystems*, Technical Report TR-syssec-05-04, University of Klagenfurt, Austria, August 2005.

[1] Universität Klagenfurt, Systemsicherheit