Enhancing privacy from malleability

Thomas Peters

UCLouvain & FNRS, Belgium

Public-key cryptographic primitive aims at reaching strong security guarantee to be deployed in practice. Among the usual security notions *non-malleability* seems to find a prominent place, in part due to the robustness it may bring to more complex protocols, while it is well known that combining secure tools may not necessarily maintain the security of the combination.

Well-known examples of non-malleability include strong unforgeability of digital signatures and indistinguishability against chosen-ciphertext attacks of encryption scheme, as known as CCA secure encryption. While these both notions are inescapable is some contexts they may also be too restrictive in other situations and lead to less efficient constructions.

This talk will focus on *malleability* and somehow recalls that weakening security models offers better flexibility to, on the one hand, design protocols allowing desired and controlled manipulation and, on the other hand, design new composition leading to more efficient non-malleable solution.

Especially, we will present a linearly homomorphic signature which nicely interacts with other algebraic tools built from pairings. From there we will build a publicly verifiable and partially re-randomizable encryption scheme reaching a slightly weaker notion of CCA security but offering a better privacy in the context of electronic voting.

Crypto Group, Maxwell building, 3 place du Levant, 1348 Louvain-la-Neuve.
thomas.peters@uclouvain.be