A Self-Certified and Sybil-Free Framework for Secure Digital Identity Domain Buildup

Leonardo A. Martucci, Karlstad University

An attacker who can control arbitrarily many user identities can break the security properties of most conceivable systems. This is called a “Sybil attack”. We present a solution to this problem that does not require online communication with a trusted third party and that in addition preserves the privacy of honest users. Given an initial so-called Sybil-free identity domain, our proposal can be used for deriving Sybil-free unlinkable pseudonyms associated with other identity domains. The pseudonyms are self-certified and computed by the users themselves from their cryptographic long-term identities.