Distance-bounding, privacy-preserving attribute-based credentials

Daniel Bosk[1], Simon Bouget[1], Sonja Buchegger[1], and Sébastien Gambs[2]

[1]KTH Royal Institute of Technology,
{dbosk,bouget,buc}@kth.se
[2]Université du Quebec à Montréal, sebastien.gambs@uqam.ca

May 20, 2020

Abstract

Distance-bounding anonymous credentials could be used for any location proofs that do not need to identify the prover and thus could make even notoriously invasive mechanisms such as location-based systems privacy-preserving. There is, however, no secure distance-bounding protocol for general *attribute-based* anonymous credentials. Brands and Chaum's (EUROCRYPT'93) protocol combining distance-bounding and Schnorr comes had the right idea, but does not fulfil the requirements of modern distance-bounding protocols. We need a secure distance-bounding zero-knowledge proof-of-knowledge resisting mafia fraud, distance fraud, distance hijacking and terrorist fraud.

Our approach is another attempt toward combining distance bounding and Schnorr to construct a distance-bounding zero-knowledge proof-of-knowledge. We construct such a protocol and prove it secure in the (extended) DFKO model for distance bounding. We also performed a symbolic verification of security properties needed for resisting these attacks, implemented in Tamarin.

Encouraged by results from Singh et al. (NDSS'19), we take advantage of lessened constraints on how much can be sent in the fast phase of the distance-bounding protocol and achieve a more efficient protocol. We also provide a version that does not rely on being able to send more than one bit at a time which yields the same properties except for (full) terrorist fraud resistance.