Abstract:

We consider the problem of constructing continuous cryptographic primitives, which would be very useful in situations when a participant provides an inexact key, e.g., in biometric applications. We present several candidates for continuous hard-to-invert functions. In these candidates, we introduce constructions based on tropical and supertropical circuits, thus attempting to bring tropical mathematics to the attention of the cryptographic community.