Huang, Qiong; Yang, Guomin; Wong, Duncan S.; Susilo, Willy

Ambiguous optimistic fair exchange: definition and constructions.

Summary: Optimistic fair exchange (OFE) is a protocol for solving the problem of exchanging items or services in a fair manner between two parties, a signer and a verifier, with the help of an arbitrator which is called in only when a dispute happens between the two parties. In almost all the previous work on OFE, after obtaining a partial signature from the signer, the verifier can present it to others and show that the signer has indeed committed itself to something corresponding to the partial signature even prior to the completion of the transaction. In some scenarios, this capability given to the verifier may be harmful to the signer. In this paper, we propose the notion of ambiguous optimistic fair exchange (AOFE), which is a variant of OFE and requires additionally that the verifier cannot convince anybody about the authorship of a partial signature generated by the signer. We present a formal security model for AOFE in the multi-user setting and chosen-key model, and propose a generic construction of AOFE that is provably secure under our model. Furthermore, we propose an efficient instantiation of the generic construction, security of which is based on Strong Diffie-Hellman assumption and Decision Linear assumption without random oracles.

Keywords: optimistic fair exchange; ambiguity; signature; NIZK proof; standard model
doi:10.1016/j.tcs.2014.09.043