Hong, Jeongdae; **Kim, Jinil**; **Kim, Jihye**; **Franklin, Matthew K.**; **Park, Kunsoo**
Fair threshold decryption with semi-trusted third parties. (English) Zbl 1208.94046
Int. J. Appl. Cryptogr. 2, No. 2, 139-153 (2010).

Summary: A threshold decryption scheme is a multi-party public key cryptosystem that allows any sufficiently large subset of participants to decrypt a ciphertext, but disallows the decryption otherwise. Many threshold cryptographic schemes have been proposed so far, but fairness is not generally considered in this earlier work. In this paper, we present fair threshold decryption schemes, where either all of the participants can decrypt or none of them can. Our solutions employ semi-trusted third parties (STTP) and offline semi-trusted third parties (OTTP) previously used for fair exchange. We consider a number of variants of our schemes to address realistic alternative trust scenarios. Although we describe our schemes using a simple hashed version of ElGamal encryption, our methods generalise to other threshold decryption schemes and threshold signature schemes as well.

MSC:

94A60 Cryptography

Keywords:

threshold decryption; fairness; semi-trusted third parties; STTP; optimistic protocol; ElGamal encryption

Full Text: DOI