Mu, Yi; Zhang, Fangguo; Susilo, Willy

Deniable partial proxy signatures. (English) Zbl 1115.94307


Summary: This paper describes a proxy signature scheme where a signer can delegate a partial signing right to a party who can then sign on behalf of the original signer to generate a partial proxy signature. A partial proxy signature can be converted into a full signature with the aid of the original signer. Our proxy signature scheme has the feature of deniability, i.e., only the designated receiver can verify the partial proxy signature and the full signature associated to him, while they are not transferable. This paper also describes an application of our scheme in a deniable optimistic fair exchange.

For the entire collection see [Zbl 1063.68009].

MSC:

94A62 Authentication, digital signatures and secret sharing

Full Text: DOI