Tang, Pengzhi; Guo, Hongli; He, Tao

A threshold proxy signature scheme with privileged subset based on bilinearity.

Summary: Considering that different agents have different permissions in practical applications, and based on the thoughts of privilege subset, a threshold proxy signature scheme with privileged subset is proposed. Only when the privileged agents and general agents reach the appropriate threshold value respectively, can the effective threshold proxy signature be produced. The privileged agents and general agents can also supervise with each other to prevent the abuses of proxy rights of either party. Besides, the scheme can resist collusion attack and is unforgeable and undeniable with its properties of privilege subset and threshold signature. The correctness and security of the scheme are verified, and the efficiency and traffic of the scheme are reasonable.

Keywords: proxy signature; threshold proxy signature; bilinear pairing; privilege subset
doi:10.3969/j.issn.1003-5060.2014.09.009