An improved certificateless strong key-insulated signature scheme in the standard model.

Summary: Exposure of secret keys may be the most devastating attack on a public key cryptographic scheme since such that security is entirely lost. The key-insulated security provides a promising approach to deal with this threat since it can effectively mitigate the damage caused by the secret key exposure. To eliminate the cumbersome certificate management in traditional PKI-supported key-insulated signature while overcoming the key escrow problem in identity-based key-insulated signature, two certificateless key-insulated signature schemes without random oracles have been proposed so far. However, both of them suffer from some security drawbacks and do not achieve existential unforgeability. In this paper, we propose a new certificateless strong key-insulated signature scheme that is proven secure in the standard model. Compared with the previous certificateless strong proxy signature scheme, the proposed scheme offers stronger security and enjoys higher computational efficiency and shorter public parameters.

Keywords: certificateless strong key-insulated signature; secret key exposure; key replacement attack; malicious KGC attack; standard model
doi:10.3934/amc.2015.9.353