ABSTRACT

A new digital signature primitive, called expander signature, and discuss its application in block chain. The most promising advantage of expander signature is that a signer can generate all signatures at once using a powerful computer, and stores expander keys personally. Each time the signer wants some of his signatures to be verified, he releases the related expander key. No matter when or where, the signer can do this via a resource-limited device, for example, a personal portable terminal. We formally define the syntax and security of expander signature. Under our precisely defined security model, we give generic constructions of expander signature from both public key infrastructure-based and identity-based signature schemes. The security of our constructed expander signature schemes rigorously depends on the underlying public key signature schemes. The expander keys do not leak any information about the signer's secret key and the size of the expander keys is constant no matter how many times the expander has been occurred. Finally, we give an application example of expander signature in blockchain.