EPFL-TTO

EPFL Innovation Park J
CH-1015 Lausanne
Switzerland
+41 21 693 70 23
http://tto.epfl.ch/

Research Contact

Prof. Serge Vaudenay
+41 21 693 76 96
serge.vaudenay@epfl.ch

TTO Contact

Dr. Thomas Bourgeau
+41 21 693 33 54
thomas.bourgeau@epfl.ch

Licensing Opportunity

TTO – Technology Transfer Office

Generate, verify and deny an undeniable signature

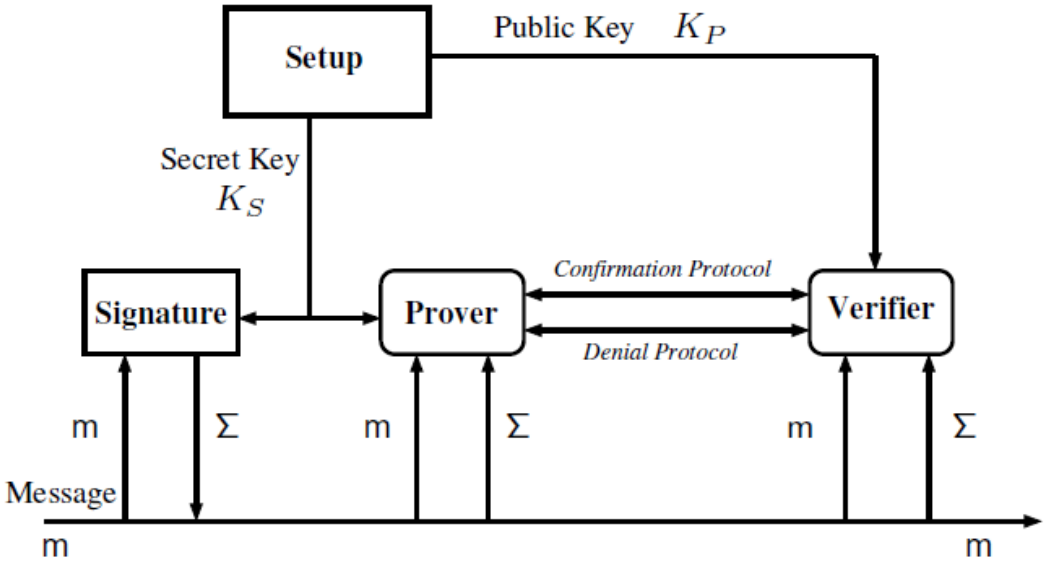

Figure 1: Undeniable signature with small signature length, i.e. less than 80 bits, providing full scalability of the signature length against security

Ref. Nr

6.0474

Keywords

Cryptography, undeniable signature, security.

Intellectual Property

US Patent US7461261B2 granted

Publications

Monnerat, Jean, and Serge Vaudenay. "Generic homomorphic undeniable signatures", Asiacrypt, 2004.

Date

06/02/2023

Description

An undeniable signature is a cryptographic scheme similar to a classical digital signature except that the recipient of a message cannot verify its validity using only the public key of the signer: he needs also to interact with this one in order to be convinced of validity of the signature. In some applications such as signing a contract it is desirable to keep the signer's privacy by limiting the ability to verify this signature. Undeniable signatures solve this problem by adding a new component called the denial protocol in addition to the normal components of signature and verification. However, the signature length can be an issue in several applications such as bank payments, in which the card holder wishes to keep a trace of each transaction in the card.

Advantages

The aim of the invention is to propose the generation, verification and denial of an undeniable signature which has a size smaller than the currently available undeniable signatures, i.e. less than 80 bits. Our scheme can achieve (very) short signatures offering full scalability of the signature length against security. Other nice properties are batch verification and low computational costs that can facilitate practical implementations in environments with communication constraints.

Applications

- Electronic signatures
- Cybersecurity