

LICENSING OPPORTUNITY

MOVA – A new undeniable digital signature scheme

Keywords

Digital signature, security, cryptography, e-commerce

Patent status

US patent application

Contact Inventor

Prof. Serge Vaudenay
EPFL - LASEC (Laboratoire de sécurité et de cryptographie)
CH-1015 Lausanne, Switzerland
e-mail: serge.vaudenay@epfl.ch
web: <http://lasecwww.epfl.ch/>
Tel: +41 21 693 76 96

Contact Technology Transfer Office

Mehdi Aminian
EPFL - SRI (Service des relations industrielles)
CH-1015 Lausanne, Switzerland
mehdi.aminian@epfl.ch
Tel : +41 21 693 54 61
Fax : +41 21 693 70 40

File Nr. 6.0474 (please mention when contacting us)

The Security and Cryptography Laboratory (LASEC) of EPFL has recently developed a new undeniable digital signature scheme.

A digital signature is a string of characters allowing to bind a document to a person or an entity. After he received the document and the signature, the recipient can authenticate them, by his own, using a public key.

The undeniable signatures have the particularity to be verifiable only with the cooperation of the signer. Indeed, an interactive protocol is established in order to specify the validity of the signature.

Innovative aspects

- The mathematical techniques used for this new scheme are based on particular functions named group characters

Main advantages

- The signature length is far smaller than standard ones

Potential Commercial Uses

- Electronic payment & e-commerce
- Traceability of goods and non traceable orders transmission
- Software protection