Title (en)

SIGNATURE VERIFICATION FOR ELGAMAL SCHEMES

Title (de)

SIGNATURBESTÄTIGUNG BEI ELGAMAL-VERFAHREN

Title (fr)

VERIFICATION DE SIGNATURE POUR SYSTEMES ELGAMAL

Publication

EP 1025674 A1 20000809 (EN)

Application

EP 98952457 A 19981102

Priority

- CA 9801018 W 19981102
- US 96244197 A 19971031

Abstract (en)

[origin: WO9923781A1] A signature verification protocol is provided for ElGamal-like signature schemes. The digital signature verification scheme allows the signor of the message to verify the digital signature without using the public key. Generally the signors computer system has a private key d and a public key y derived from an element g and the private key d. The method comprises the steps of in the computer system signing a message m by generating a first signature component by combining the element g, the signature parameter k according to a first mathematical function and generating a second signature component by mathematically combining the first signature component with the private key d, the message m and the signature parameter k, and the signor verifying the signature by recovering a value k from the signature components without using the public key y and utilizing the recovered value k' in the first mathematical function to derive a value r' in order to verify the signature parameter k and k' are equivalent, thereby verifying the signature. This signature verification applies to all ElGamal-type signatures and works in any group and in particular elliptic curve groups. The signature verification method is of particular use in devices having limited computational power such as 'smart cards' or where a large number of verifications are to be performed by the signor.

IPC 1-7

H04L 9/32

IPC 8 full level

G09C 1/00 (2006.01); **H04L 9/32** (2006.01); G06F 7/72 (2006.01)

CPC (source: EP)

H04L 9/3013 (2013.01); **H04L 9/3247** (2013.01); G06F 7/725 (2013.01)

Citation (search report)

See references of WO 9923781A1

Designated contracting state (EPC)

CH DE DK FI FR GB LI SE

DOCDB simple family (publication)

WO 9923781 A1 19990514; AU 1015499 A 19990524; CA 2306468 A1 19990514; EP 1025674 A1 20000809; JP 2001522071 A 20011113; JP 4307589 B2 20090805; JP H11174957 A 19990702

DOCDB simple family (application)

CA 9801018 W 19981102; AU 1015499 A 19981102; CA 2306468 A 19981016; EP 98952457 A 19981102; JP 13174398 A 19980514; JP 2000519520 A 19981102