Title (en)

A METHOD FOR SECURE AND RESILIENT DISTRIBUTED GENERATION OF ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM (ECDSA) BASED DIGITAL SIGNATURES WITH PROACTIVE SECURITY

Title (de)

VERFAHREN ZUR SICHEREN UND ELASTISCHEN VERTEILTEN ERZEUGUNG DIGITALER SIGNATUREN AUF DER BASIS EINES ELLIPTISCHEN KURVENALGORITHMUS FÜR DIGITALE SIGNATUREN (ECDSA) MIT PROAKTIVER SICHERHEIT

Title (fr)

PROCÉDÉ DE GÉNÉRATION DISTRIBUÉE SÉCURISÉE ET FLEXIBLE DE SIGNATURES NUMÉRIQUES À SÉCURITÉ PROACTIVE BASÉES SUR UN ALGORITHME DE SIGNATURE NUMÉRIQUE À COURBE ELLIPTIQUE (ECDSA)

Publication

EP 3132560 A4 20171220 (EN)

Application

EP 15780610 A 20150414

Priority

- US 201461981191 P 20140417
- US 2015025804 W 20150414

Abstract (en)

[origin: WO2015160839A1] Described is system for generation of elliptic curve digital signature algorithm (ECDSA) based digital signatures. A. Secret-Share protocol is initialized between a client and a set of servers to share a set of shares of a private key s among the set of servers. The set of servers initializes a protocol to generate a digital signature on a message using the set of shares of the private key s without reconstructing or revealing the private key A. The set of servers periodically initialises a Secret-Redistribute protocol on each share of the private key A- to re-randomize the set of shares. A Secret-Open protocol is initialized to reveal the private key s to an intended recipient, wherein the private key A is used to compute the digital signature.

IPC 8 full level

H04L 9/08 (2006.01); **H04L 9/32** (2006.01)

CPC (source: EP)

H04L 9/085 (2013.01); **H04L 9/3252** (2013.01); **H04L 9/3255** (2013.01)

Citation (search report)

- [XI] CHARIKLEIA ZOURIDAKI ET AL: "Distributed CA-based PKI for Mobile Ad Hoc Networks Using Elliptic Curve Cryptography", 24 June 2004, PUBLIC KEY INFRASTRUCTURE; [LECTURE NOTES IN COMPUTER SCIENCE;;LNCS], SPRINGER-VERLAG, BERLIN/HEIDELBERG, PAGE(S) 232 - 245, ISBN: 978-3-540-22216-3, XP019007629
- [XI] IBRAHIM M H ET AL: "A robust threshold elliptic curve digital signature providing a new verifiable secret sharing scheme", MIDWEST SYMPOSIUM ON CIRCUITS AND SYSTEMS. CAIRO, EGYPT, DEC. 27 - 30, 2003; [MIDWEST SYMPOSIUM ON CIRCUITS AND SYSTEMS], PISCATAWAY, NJ, IEEE, US, vol. 1, 27 December 2003 (2003-12-27), pages 276 - 280, XP010867444, ISBN: 978-0-7803-8294-7, DOI: 10.1109/MWSCAS.2003.1562272
- See references of WO 2015160839A1

Cited by

CN110999206A; US11316668B2

Designated contracting state (EPC)

AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

DOCDB simple family (publication)

WO 2015160839 A1 20151022; CN 106664205 A 20170510; CN 106664205 B 20200605; EP 3132560 A1 20170222; EP 3132560 A4 20171220

DOCDB simple family (application)

US 2015025804 W 20150414; CN 201580019894 A 20150414; EP 15780610 A 20150414