(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
6 January 2005 (06.01.2005)

PCT

(10) International Publication Number
WO 2005/001751 A1

(51) International Patent Classification[7]: G06K 9/00, H04K 1/00, H04L 9/00

(21) International Application Number: PCT/US2004/017545

(22) International Filing Date: 2 June 2004 (02.06.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/475,242 2 June 2003 (02.06.2003) US

(71) Applicant *(for all designated States except US)*: **REGENTS OF THE UNIVERSITY OF CALIFORNIA** [US/US]; University of California, Los Angeles, 10920 Wilshire Blvd, Suite 1200, Los Angeles, CA 90024-1406 (US).

(72) Inventors; and

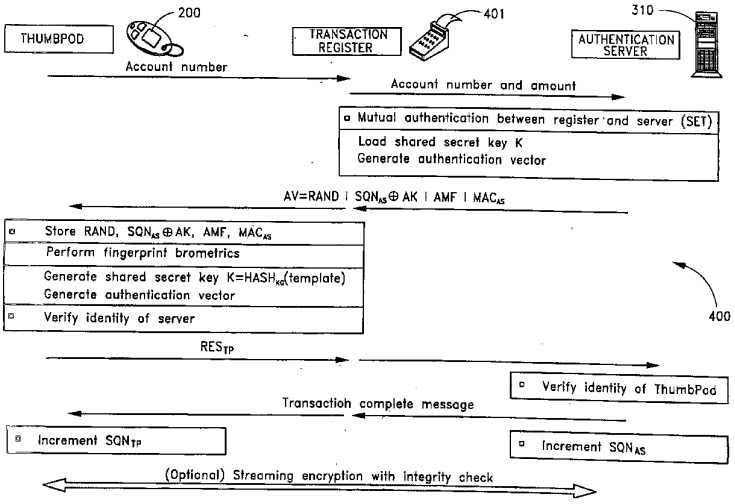
(75) Inventors/Applicants *(for US only)*: **VERBAUWHEDE, Ingrid, M.** [—/US]; 1123 23rd Street, #C, Santa Monica, CA 90403 (US). **SCHAUMONT, Patrick, R.** [—/US]; 10439 Holman Avenue, Los Angeles, CA 90024 (US). **HWANG, David, D.** [—/US]; 540 Kelton Avenue, #205, Los Angeles, CA 90024 (US). **LAI, Bo-Cheng** [—/US]; 10125 Palms Boulevard, #204, Los Angeles, CA 90034 (US). **YANG, Shenglin** [—/US]; 3170 Sawtelle Boulevard, Apt. #203, Los Angeles, CA 90066 (US). **SAKIYAMA, Kazuo** [—/US]; 3200 Sawtelle Boulevard, Apt. #202, Los Angeles, CA 90066 (US). **FAN, Yi** [—/US]; 310 S. Kenmore Avenue, Apt. #202, Los Angeles, CA 90020 (US). **HODJAT, Alireza** [—/US]; 2624 Kansan Avenue, #14, Santa Monica, CA 90404 (US).

(74) Agent: **DELANEY, Karoline, A.**; KNOBBE, MARTENS, OLSON AND BEAR, LLP, 2040 Main Street, Fourteenth Floor, Irvine, CA 92614 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

[Continued on next page]

(54) Title: SYSTEM FOR BIOMETRIC SIGNAL PROCESSING WITH HARDWARE AND SOFTWARE ACCELERATION



(57) Abstract: A secure embedded system that uses cryptographic and biometric signal processing acceleration is described. In one embodiment, the secure embedded system is configured as a wireless pay-point protocol for brick-and-mortar and e-commerce applications in which biometric information is localized and does not require transmission of biometric data for authentication. In one embodiment, a key-generation function uses a dynamic key generator and static biometric components. In one embodiment, an embedded system design methodology provides hardware and software acceleration transparency.

WO 2005/001751 A1

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declaration under Rule 4.17:

— *of inventorship (Rule 4.17(iv)) for US only*

Published:

— *with international search report*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SYSTEM FOR BIOMETRIC SIGNAL PROCESSING WITH HARDWARE AND SOFTWARE ACCELERATION

Reference to Related Application

[0001] The present application claims priority benefit if U.S. Provisional Application No. 60/475,242, filed June 2, 2003, titled "SYSTEM FOR BIOMETRIC SIGNAL PROCESSING WITH HARDWARE AND SOFTWARE ACCELERATION," the entire contents of which is hereby incorporated by reference.

Government Interest Statement

Portions of the subject matter of this application were invented under a contract with an agency of the United States Government, under NSF contract No. 0098361.

Background

Field of the invention

[0002] The present invention relates to systems using biometric signal processing for authentication in connection with a secure communication protocol.

Description of the Related Art

[0003] In February 2003, a computer hacker breached the security systems of Visa and MasterCard and accessed 5.6 million valid account numbers, which represents approximately 1% of all 574 million valid account numbers in the United States. Though the accounts were not used fraudulently, a burdensome recall and replacement of valid cards throughout many financial institutions was required. On the Internet, a number of black-market sites sell active credit card account numbers and expiration dates for a modest price. In brick-and-mortar credit card scenarios, photograph identification or signatures are inconsistently checked in normal purchases; hence, fraudulent transactions are commonplace. These situations are just a few which expose the current flaw in traditional transaction

protocols, which is mainly a flaw in authentication. Identity theft results in losses of well over a billion dollars a year for credit card issuers, and is even more widespread since the advent of e-commerce on the Internet. The primary reason for the continued success of identity theft is the lack of the ability to prove that an account is used by the genuine, authorized, consumer.

Summary

[0004] The present invention solves these and other problems by providing a secure embedded system that uses cryptographic and biometric signal processing to provide identity authentication. In one embodiment, the secure embedded system is configured as a wireless pay-point device, called a thumbpod, for brick-and-mortar and/or e-commerce applications. In one embodiment, the thumbpod localizes a sensitive biometric template and does not require transmission of biometric data for authentication. In one embodiment, a key-generation function uses a dynamic key generator and static biometric components. An embedded system design methodology known as hardware/software acceleration transparency is provided to improve performance of the thumbpod. In one embodiment, acceleration transparency is provided in a systematic method to accelerate Java functions in both software and hardware of, for example, an encryption function.

[0005] In one embodiment, the thumbpod is designed as a secure embedded device that provides a protocol for wireless pay-point transactions in a secure manner. The protocol uses secure cryptographic primitives as well as biometric authentication techniques. The security protocol used in the thumbpod is based on a protocol that uses the thumbpod as an interface between an authentication server and a user.

[0006] In one embodiment, the thumbpod includes a microcontroller, a fingerprint image sensor, signal processing hardware acceleration, cryptographic hardware acceleration, and a memory module enclosed within a form factor similar to an automobile keychain transmitter. The thumbpod provides flexible communication via ports, such as, for example, a port for wireless communication and/or a wired port for fast wire-line communication. The wireless port can be, for example, an infrared port, a radio-frequency port, an inductive coupling port, a capacitive coupling port, a Bluetooth port, a wireless Ethernet port, etc. The

wired port can be, for example, a USB port, a firewire port, a serial port, an Ethernet port, etc. The thumbpod can be used for a wide variety of authentication-related transactions, such as, for example, wireless credit card payments, keychain flash memory replacement, universal key functionality (house, car, office), storage of sensitive medical data, IR secure printing, etc.

[0007] In one embodiment, a security protocol binds the user to the device through biometrics, combines biometrics and traditional security protocols, protects biometric data by keeping at least a portion of the biometric data in a protected form that does not leave the device, and provides that biometric calculations are provided on the device. In one embodiment, biometric algorithms are provided to fit a relatively constrained environment of embedded devices. In one embodiment, algorithms are provided in fixed point arithmetic. In one embodiment, memory storage optimization and hardware acceleration are provided by converting a least a portion of one or more software algorithms into hardware.

Brief Description of the Drawings

[0008] The various features of the present are described with reference to the following figures.

[0009] Figure 1 shows layers of an embedded security protocol system.

[0010] Figure 2 shows one embodiment of a thumbpod device.

[0011] Figure 3A is a block diagram of an authentication protocol having a relatively strong one-way authentication protocol between the server and the device and a relatively week security protocol between and the device and the user.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.