US006901145B1

(12) **United States Patent**
Bohannon et al.

(10) **Patent No.: US 6,901,145 B1**
(45) **Date of Patent: May 31, 2005**

(54) **GENERATION OF REPEATABLE CRYPTOGRAPHIC KEY BASED ON VARYING PARAMETERS**

(75) Inventors: **Philip L. Bohannon**, Piscataway, NJ (US); **Bjorn Markus Jakobsson**, Hoboken, NJ (US); **Fabian Monrose**, New York, NY (US); **Michael Kendrick Reiter**, Raritan, NJ (US); **Susanne Gudrun Wetzel**, New Providence, NJ (US)

(73) Assignee: **Lucent Technologies Inc.**, Murray Hill, NJ (US)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

(21) Appl. No.: **09/501,902**

(22) Filed: **Feb. 10, 2000**

Related U.S. Application Data

(60) Provisional application No. 60/128,413, filed on Apr. 8, 1999, and provisional application No. 60/147,880, filed on Aug. 9, 1999.

(51) **Int. Cl.**[7] **H04L 9/00**

(52) **U.S. Cl.** **380/44**; 380/45; 380/47; 380/277; 380/286; 713/165; 713/168; 713/171; 713/202

(58) **Field of Search** 380/44; 713/165

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,805,222 A		2/1989	Young et al.	382/2
4,876,725 A		10/1989	Tomko	382/4
5,369,707 A	*	11/1994	Follendore, III	713/155
5,541,994 A		7/1996	Tomko et al.	380/30
5,557,346 A	*	9/1996	Lipner et al.	380/286
5,557,686 A	*	9/1996	Brown et al.	382/115
5,625,692 A	*	4/1997	Herzberg et al.	380/286
5,680,460 A		10/1997	Tomko et al.	380/23
5,712,912 A	*	1/1998	Tomko et al.	713/186
5,737,420 A		4/1998	Tomko	380/23
5,740,276 A		4/1998	Tomko et al.	382/210
5,761,330 A		6/1998	Stoianov et al.	382/127
5,790,668 A		8/1998	Tomko	380/25

(Continued)

FOREIGN PATENT DOCUMENTS

WO	WO 9605673 A1	2/1996	H04L/9/08

OTHER PUBLICATIONS

Mytec Technologies Inc., Mytec: Biometrics, downloaded from Internet website http://www.mytec.com/biometrics/ on Nov. 1, 1999.

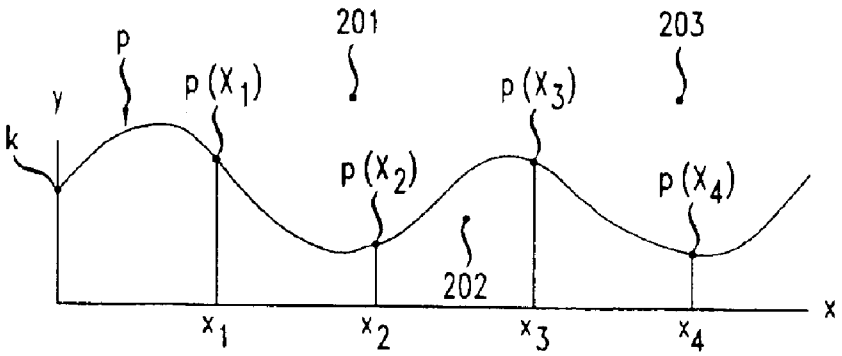
(Continued)

Primary Examiner—Thomas R. Peeso
Assistant Examiner—Syed A. Zia
(74) *Attorney, Agent, or Firm*—Jeffrey Weinick; Donald P. Dinella

(57) **ABSTRACT**

A repeatable cryptographic key is generated based on varying parameters which represent physical measurements. Locations within a share table, which locations store valid and invalid cryptographic shares, are identified as a function of received varying parameters. The share table is configured such that locations which are expected to be identified by legitimate access attempts contain valid cryptographic shares, and locations which are not expected to be identified by legitimate access attempts contain invalid cryptographic shares. The share table configuration may be modified based on prior history of legitimate access attempts. In various embodiments, the stored shares may be encrypted or compressed. A keystroke feature authentication embodiment uses the inventive techniques to implement an authentication system which authenticates based on an entered password and the manner in which (e.g. keystroke dynamics) the keystroke is entered. Another embodiment uses the inventive techniques to protect sensitive database information which is accessible using DNA measurements.

24 Claims, 3 Drawing Sheets



DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

U.S. PATENT DOCUMENTS

5,802,175	A *	9/1998	Kara	380/277
5,832,091	A	11/1998	Tomko et al.	380/30
5,991,408	A *	11/1999	Pearson et al.	713/186
6,035,042	A *	3/2000	Mittenthal	380/37
6,317,834	B1 *	11/2001	Gennaro et al.	713/186

OTHER PUBLICATIONS

Mytec Technologies Inc., Mytec: Products—Mytec Gateway, downloaded from Internet website http:// www.mytec.com/products/gateway on Nov. 1, 1999.

Mytec Technologies Inc., Mytec: Why Mytec, downloaded from Internet website http://www.mytec.com/why-mytec.htm on Nov. 1, 1999.

Mytec Technolgies Inc., Mytec: Mytec: Products—Touchstone Pro, downloaded from Internet website http//:www.mytec.com/products/touchstone on Nov. 1, 1999.

BIOPassword, Net Nanny Software International Inc. 1994–1998, Bellevue, WA USA, pp. 2–9, 1–3.

F. Monrose, M.K. Reiter, and S. Wetzel, "Password hardening based on keystroke dynamics," *Proceedings of the 6th ACM Conference on Computer and Communications Security*, Nov. 1999, pp. 73–82.

C. Soutar and G.J. Tomko; "Secure Private Key Generation Using a Fingerprint," Cardtech/Securetech Conference Proceedings, vol. 1, May 1996, pp. 245–252.

European Patent Search Report, Application No. 00302540.0–1237–, The Hague, Jun. 5, 2002.

Shamir, A., *How to Share a Secret*, Communications of the ACM, vol. 22, No. 11, Nov., 1979, pp. 612–613.

Davida, G. I:, et al:, *On Enabling Secure Applications Through Off–line Biometric Identification*, IEEE, 1998, pp. 148–157.

Monrose, F. et al:, *Password Hardening Based on Keystroke Dynamics*, ACM, 1999, pp. 73–82.

* cited by examiner

DOCKET ALARM
Find authenticated court documents without watermarks at docketalarm.com.

FIG. 1

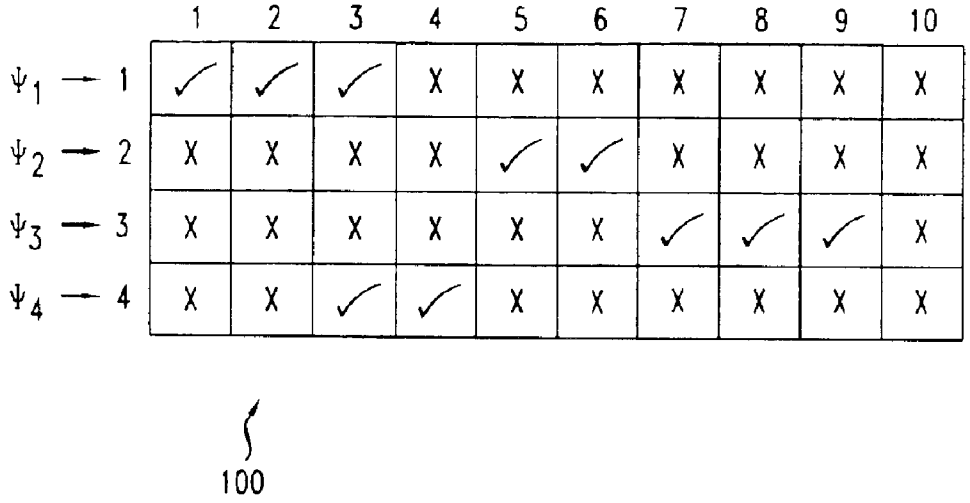
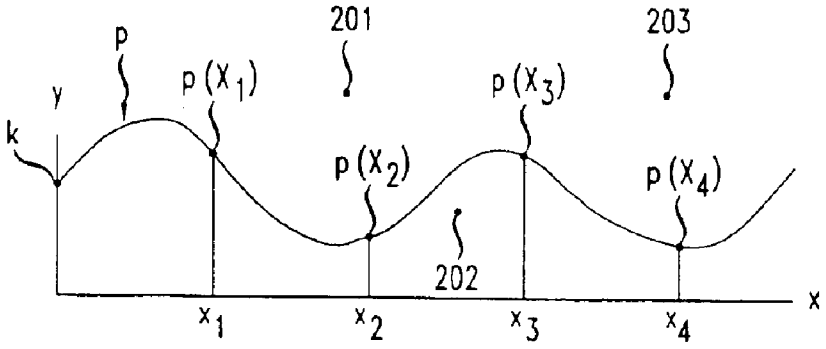


FIG. 2



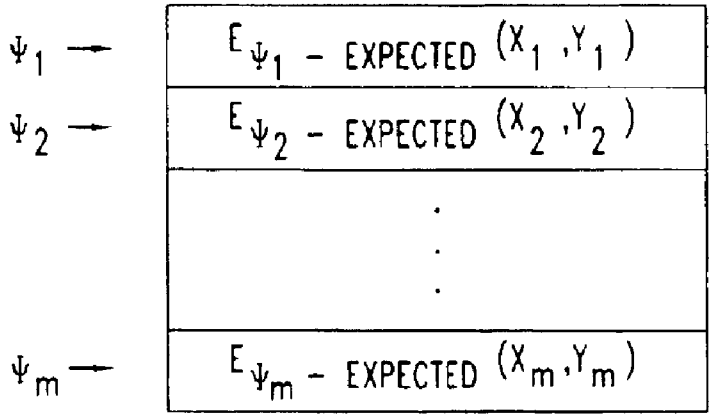
DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

FIG. 3

(1,1) 1	(1,2) 2	(1,3) 3	(1,4) 4
(2,1) 5	(2,2) 6	(2,3) 7	(2,4) 8
(3,1) 9	(3,2) 10	(3,3) 11	(3,4) 12
(4,1) 13	(4,2) 14	(4,3) 15	(4,4) 16

300

FIG. 4



400

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

FIG. 5

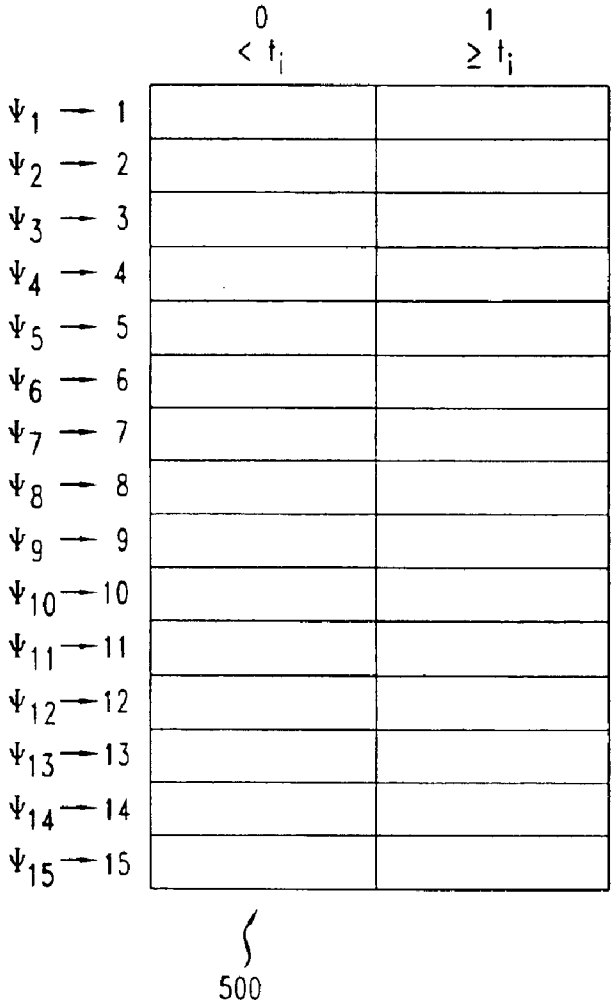


FIG. 6

SUCCESSFUL ACCESS ATTEMPT	MEASURED PARAMETERS
LAST	$\emptyset_1, \emptyset_2, \ldots \emptyset_m$
LAST-1	$\emptyset_1, \emptyset_2, \ldots \emptyset_m$
LAST-2	$\emptyset_1, \emptyset_2, \ldots \emptyset_m$
. . .	
LAST-n	$\emptyset_1, \emptyset_2, \ldots \emptyset_m$

600

DOCKET ALARM Find authenticated court documents without watermarks at docketalarm.com.

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.