US007167984B2

(12) **United States Patent**
Graveman

(10) **Patent No.: US 7,167,984 B2**
(45) **Date of Patent: Jan. 23, 2007**

(54) **METHOD AND DEVICE FOR GENERATING APPROXIMATE MESSAGE AUTHENTICATION CODES**

(75) Inventor: **Richard F. Graveman**, Morristown, NJ (US)

(73) Assignee: **Telcordia Technologies, Inc.**, Piscataway, 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.: **10/969,518**

(22) Filed: **Jan. 27, 2005**

(65) **Prior Publication Data**

US 2005/0210248 A1 Sep. 22, 2005

Related U.S. Application Data

(62) Division of application No. 09/458,336, filed on Dec. 10, 1999, now Pat. No. 6,851,052.

(60) Provisional application No. 60/111,771, filed on Dec. 10, 1998.

(51) **Int. Cl.**
H04L 9/00 (2006.01)
H04N 7/167 (2006.01)

(52) **U.S. Cl.** **713/168**; 713/155; 713/170; 380/229

(58) **Field of Classification Search** 713/168
See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

6,132,216 A *	10/2000	Muntean et al.	....	434/191
6,199,162 B1 *	3/2001	Luyster	....	713/168
6,434,699 B1 *	8/2002	Jones et al.	....	713/168
6,851,052 B1 *	2/2005	Graveman	....	713/168

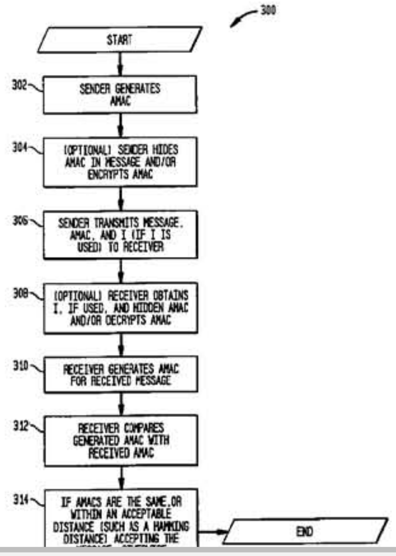
* cited by examiner

Primary Examiner—Kambiz Zand
(74) *Attorney, Agent, or Firm*—Joseph Giordano; Philip J. Feig

(57) **ABSTRACT**

An approximate message authentication code (AMAC) which, like conventional message authentication codes, provides absolute authentication of the origin of the message, yet provides an approximate integrity check for the content of the message. The approximate integrity check will be computed probabilistically and will likely be the same for messages having only a small percentage of different bits. A distance measure on the AMACs, such as a Hamming distance measure, may be used to determine whether the number of bit differences between the messages is likely to be within an acceptable amount. The AMAC is a probabilistic checksum based on a shared key. The AMAC uses the message and a shared key as inputs. Optionally, an initial value may also be used as an input. In one version of the invention, the data in the message M are permuted and arranged (physically or logically) into a table having |A| bits in each column and T^2 rows, where T is may be an odd integer. The permuted data are masked, for example, to generate an unbiased, independent, identically distributed set of bits (1s and 0s). Taking T rows at a time, the majority bit value for each column is determined and that majority value is used to generate a new row. This procedure is repeated on the T new rows of majority bits. The resulting |A| bits is the AMAC.

23 Claims, 10 Drawing Sheets


300
START
302
SENDER GENERATES AMAC
304
(OPTIONAL) SENDER HIDES AMAC IN MESSAGE AND/OR ENCRYPTS AMAC
306
SENDER TRANSMITS MESSAGE, AMAC, AND I (IF I IS USED) TO RECEIVER
308
(OPTIONAL) RECEIVER OBTAINS I, IF USED, AND HIDDEN AMAC AND/OR DECRYPTS AMAC
310
RECEIVER GENERATES AMAC FOR RECEIVED MESSAGE
312
RECEIVER COMPARES GENERATED AMAC WITH RECEIVED AMAC
314
IF AMACS ARE THE SAME OR WITHIN AN ACCEPTABLE DISTANCE (SUCH AS A HAMMING DISTANCE) ACCEPTING THE
END

NETWORK-1 EXHIBIT [illegible]

FIG. 1
(PRIOR ART)

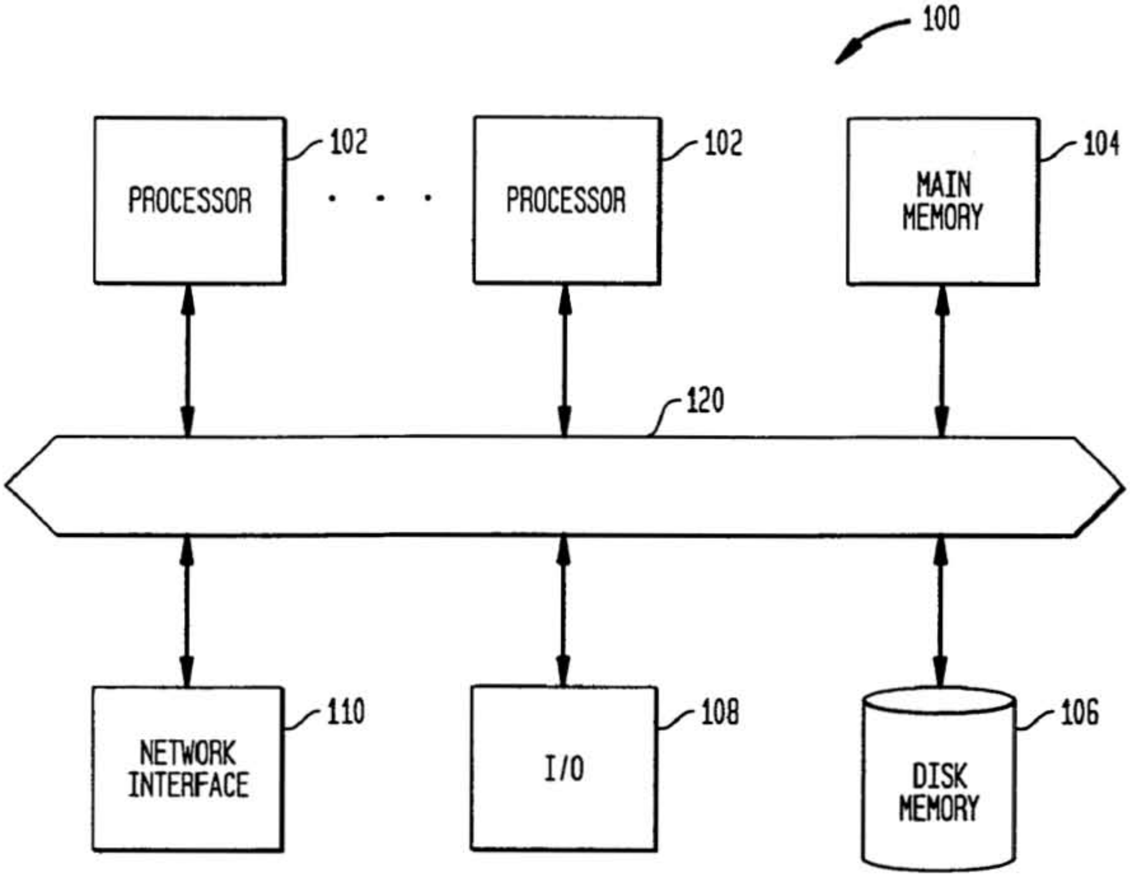


FIG. 2
(PRIOR ART)

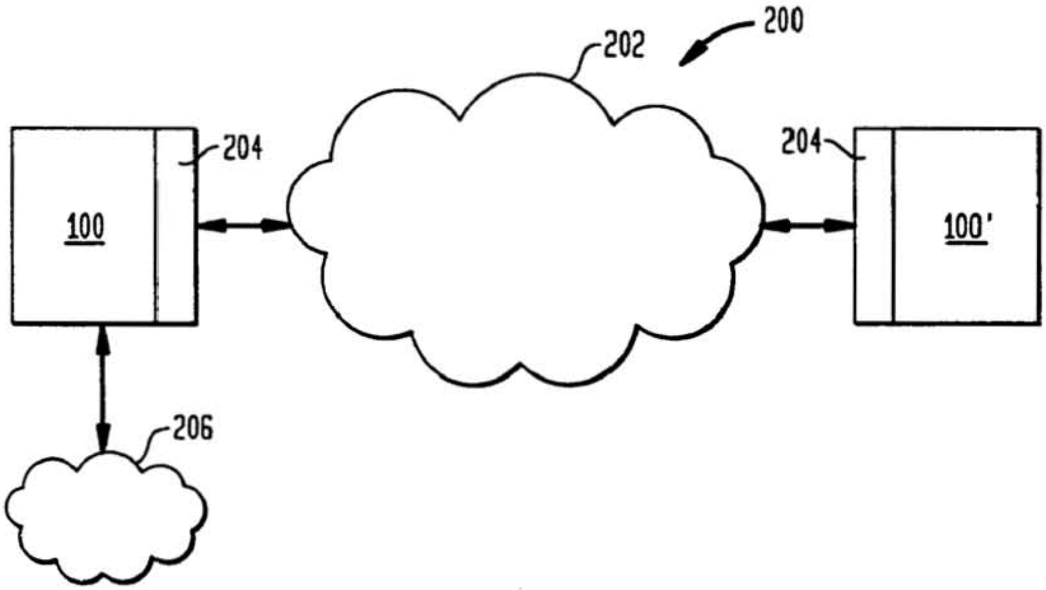


FIG. 3

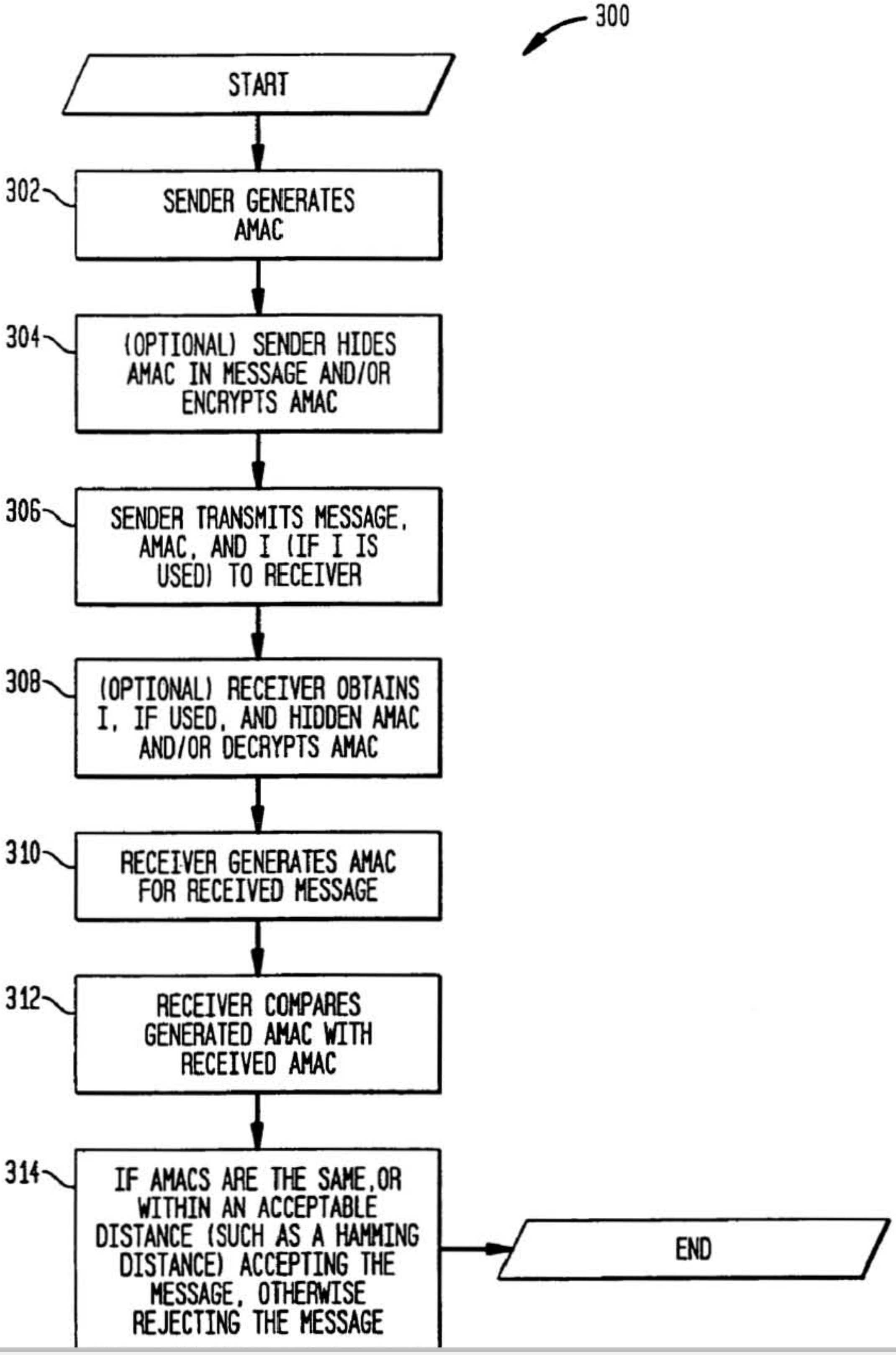

300
START
302
SENDER GENERATES AMAC
304
(OPTIONAL) SENDER HIDES AMAC IN MESSAGE AND/OR ENCRYPTS AMAC
306
SENDER TRANSMITS MESSAGE, AMAC, AND I (IF I IS USED) TO RECEIVER
308
(OPTIONAL) RECEIVER OBTAINS I, IF USED, AND HIDDEN AMAC AND/OR DECRYPTS AMAC
310
RECEIVER GENERATES AMAC FOR RECEIVED MESSAGE
312
RECEIVER COMPARES GENERATED AMAC WITH RECEIVED AMAC
314
IF AMACS ARE THE SAME, OR WITHIN AN ACCEPTABLE DISTANCE (SUCH AS A HAMMING DISTANCE) ACCEPTING THE MESSAGE, OTHERWISE REJECTING THE MESSAGE
END

FIG. 4A

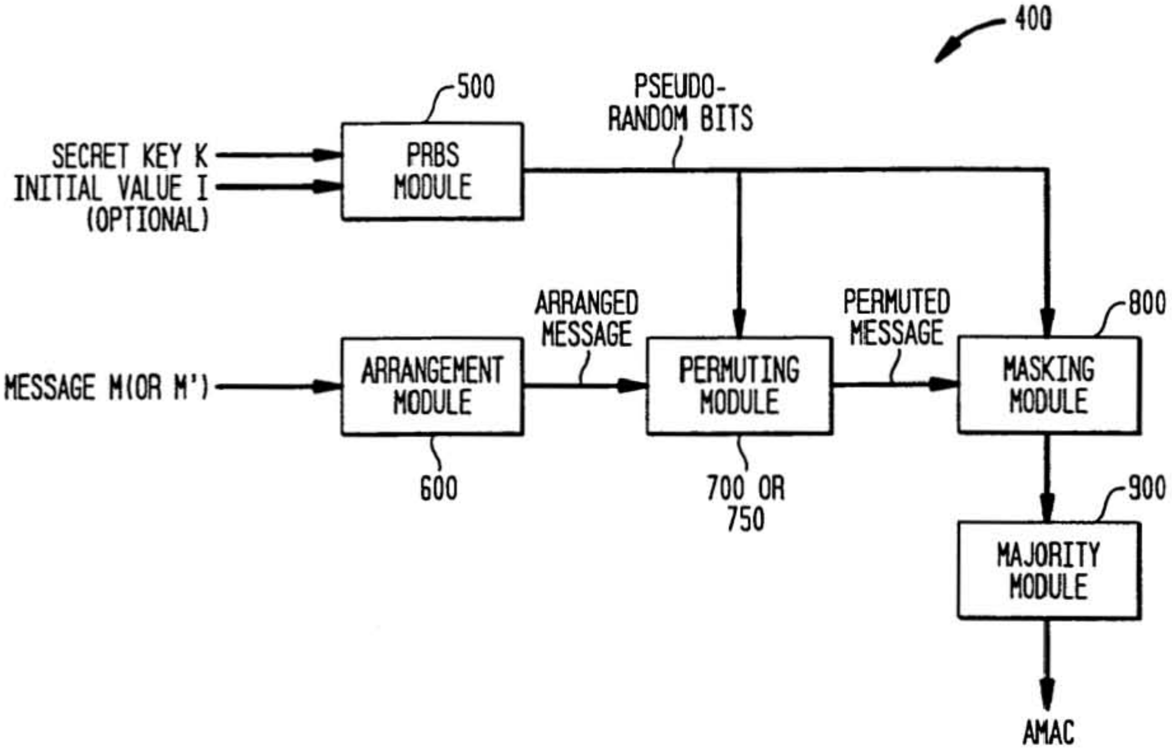
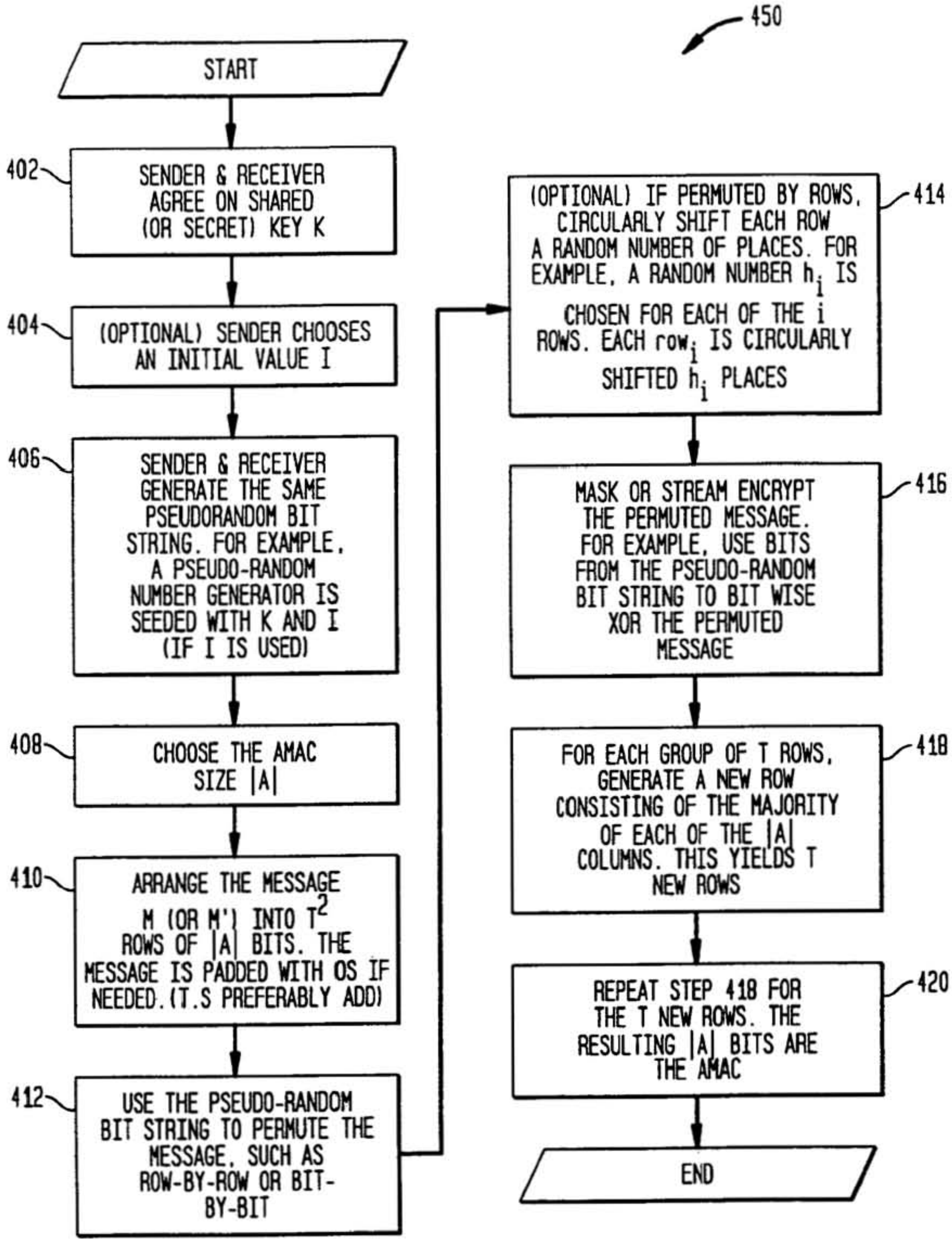

400
500
PSEUDO-RANDOM BITS
SECRET KEY K
INITIAL VALUE I (OPTIONAL)
PRBS MODULE
ARRANGED MESSAGE
PERMUTED MESSAGE
800
MESSAGE M(OR M')
ARRANGEMENT MODULE
PERMUTING MODULE
MASKING MODULE
600
700 OR 750
900
MAJORITY MODULE
AMAC

FIG. 4B


450
START
402
SENDER & RECEIVER AGREE ON SHARED (OR SECRET) KEY K
404
(OPTIONAL) SENDER CHOOSES AN INITIAL VALUE I
406
SENDER & RECEIVER GENERATE THE SAME PSEUDORANDOM BIT STRING. FOR EXAMPLE, A PSEUDO-RANDOM NUMBER GENERATOR IS SEEDED WITH K AND I (IF I IS USED)
408
CHOOSE THE AMAC SIZE |A|
410
ARRANGE THE MESSAGE M (OR M') INTO T^2 ROWS OF |A| BITS. THE MESSAGE IS PADDED WITH 0S IF NEEDED. (T.S PREFERABLY ADD)
412
USE THE PSEUDO-RANDOM BIT STRING TO PERMUTE THE MESSAGE, SUCH AS ROW-BY-ROW OR BIT-BY-BIT
414
(OPTIONAL) IF PERMUTED BY ROWS, CIRCULARLY SHIFT EACH ROW A RANDOM NUMBER OF PLACES. FOR EXAMPLE, A RANDOM NUMBER h_i IS CHOSEN FOR EACH OF THE i ROWS. EACH row_i IS CIRCULARLY SHIFTED h_i PLACES
416
MASK OR STREAM ENCRYPT THE PERMUTED MESSAGE. FOR EXAMPLE, USE BITS FROM THE PSEUDO-RANDOM BIT STRING TO BIT WISE XOR THE PERMUTED MESSAGE
418
FOR EACH GROUP OF T ROWS, GENERATE A NEW ROW CONSISTING OF THE MAJORITY OF EACH OF THE |A| COLUMNS. THIS YIELDS T NEW ROWS
420
REPEAT STEP 418 FOR THE T NEW ROWS. THE RESULTING |A| BITS ARE THE AMAC
END

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.

WHAT WILL YOU BUILD? | sales@docketalarm.com | 1-866-77-FASTCASE

fastcase®
Smarter legal research.