**United States Patent** [19]
**Chaum**

[11] **Patent Number: 4,926,480**
[45] **Date of Patent: May 15, 1990**

[54] **CARD-COMPUTER MODERATED SYSTEMS**

[76] Inventor: **David Chaum,** 14652 Sutton St.,
Sherman Oaks, Calif. 91403

[21] Appl. No.: **198,315**

[22] Filed: **May 24, 1988**

**Related U.S. Application Data**

[63] Continuation-in-part of Ser. No. 524,896, Aug. 22, 1983, Pat. No. 4,759,063, and Ser. No. 784,999, Oct. 7, 1985, Pat. No. 4,759,064, and Ser. No. 168,802, Mar. 16, 1988, abandoned, and Ser. No. 123,703, Oct. 23, 1987.

[51] **Int. Cl.**$^5$ .............................................. **H04K 1/00**
[52] **U.S. Cl.** ........................................ **380/23;** 380/24;
380/30; 235/379; 235/380; 235/382
[58] **Field of Search** .................................... 380/23–25,
380/30, 43, 44, 47, 49, 50; 235/379–382

[56] **References Cited**

U.S. PATENT DOCUMENTS

| | | | |
|---|---|---|---|
| 4,264,782 | 4/1981 | Konheim | 380/25 |
| 4,393,269 | 7/1983 | Konheim | 380/25 |
| 4,423,287 | 12/1983 | Zeidler | 235/382 X |
| 4,529,870 | 7/1985 | Chaum | 235/379 X |
| 4,590,470 | 5/1986 | Koenig | 380/23 |
| 4,612,413 | 9/1986 | Robert et al. | 380/24 |
| 4,625,076 | 11/1986 | Okamoto et al. | 380/23 |
| 4,656,474 | 4/1987 | Mollier et al. | 235/380 X |
| 4,667,087 | 5/1987 | Quintana | 235/380 |
| 4,697,072 | 9/1987 | Kawana | 235/379 X |
| 4,710,613 | 12/1987 | Shigenaga | 235/380 |
| 4,748,668 | 5/1988 | Shamir et al. | 380/30 |
| 4,757,185 | 7/1988 | Onishi | 235/379 |
| 4,759,063 | 7/1988 | Chaum | 380/30 |
| 4,759,064 | 7/1988 | Chaum | 380/30 |
| 4,782,455 | 11/1988 | Morinouchi et al. | 235/380 X |

OTHER PUBLICATIONS

Chaum, "Design Concept For Tamper Responding System", *Proc. of Crypto* 82, Plenum Press, 1983.
Chaum et al., "A Secure And Privacy Protecting Protocol For Transmitting Personal Information Between Organizations", *Advances in Cytology: Proceedings of Crypto* 86, Springer Verlag Press, 1987.
Elgamal, "A Public Key Cryptosystem And Signature Scheme Based On Discrete Logarithms", *Advances in Cryptology: Proceedings of Crypto* 84, Springer Verlag Press, 1985.
Chaum et al., "An Improved Protocol For Demonstrating Possession Of Discrete Logarithms And Some Generalations", *Advances in Cryptology: Proceedings of Eurocrypt* 87, Springer Verlag Press, 1988.
Rivest et al., "A Method For Obtaining Digital Signatures And Public-Key Cryptosystems", *Communications of the ACM,* Feb. 1978, pp. 120–126.
Rabin, "Digitalized Signatures And Public-Key Functions As Intractable As Factorization", *MIT Technical Report MIT/LCS/TR*-212, Jan. 1979.
Peralta et al., "A Simple And Secure Way To Show The Validity Of Your Public Key", *Proceedings of Crypto* 87, Springer Verlag Press, 1988.

*Primary Examiner*—Stephen C. Buczinski
*Assistant Examiner*—Bernarr Earl Gregory
*Attorney, Agent, or Firm*—Nixon & Vanderhye

[57] **ABSTRACT**

A user controlled card computer C and communicating tamper-resistant part T are disclosed that conduct secure transactions with an external system S. All communication between T and S is moderated by C, who is able to prevent T and S from leaking any message or pre-arranged signals to each other. Additionally, S can verify that T is in immediate physical proximity. Even though S receives public key digital signatures through C that are checkable using public keys whose corresponding private keys are known only to a unique T, S is unable to learn which transactions involve which T. It is also possible for S to allow strictly limited messages to be communicated securely between S and T.

**18 Claims, 9 Drawing Sheets**

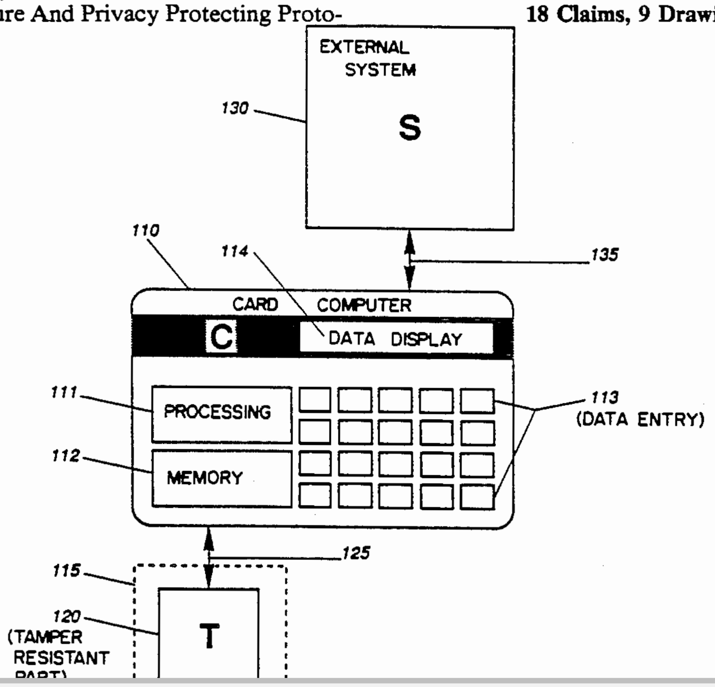


FIG. 1

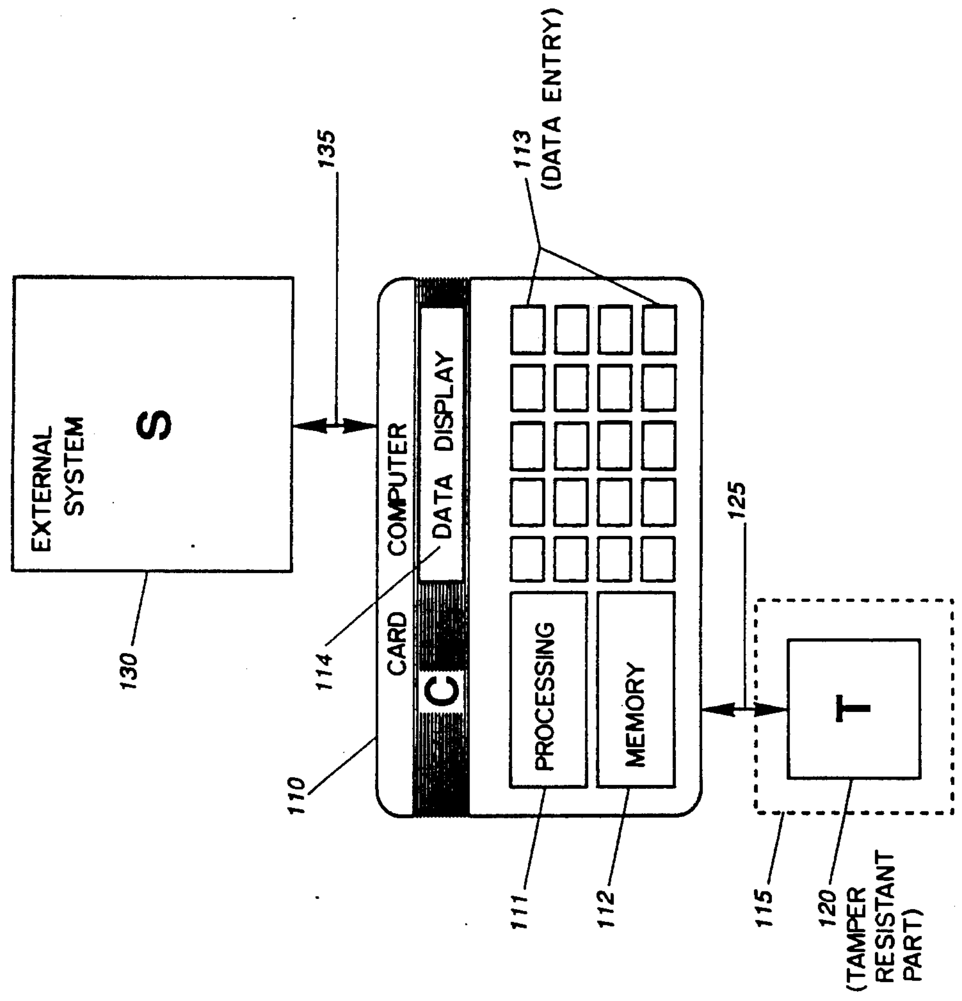

EXTERNAL SYSTEM
S
130
135
114
110
CARD COMPUTER
DATA DISPLAY
C
PROCESSING
MEMORY
111
112
113 (DATA ENTRY)
125
T
115
120 (TAMPER RESISTANT PART)

FIG. 2

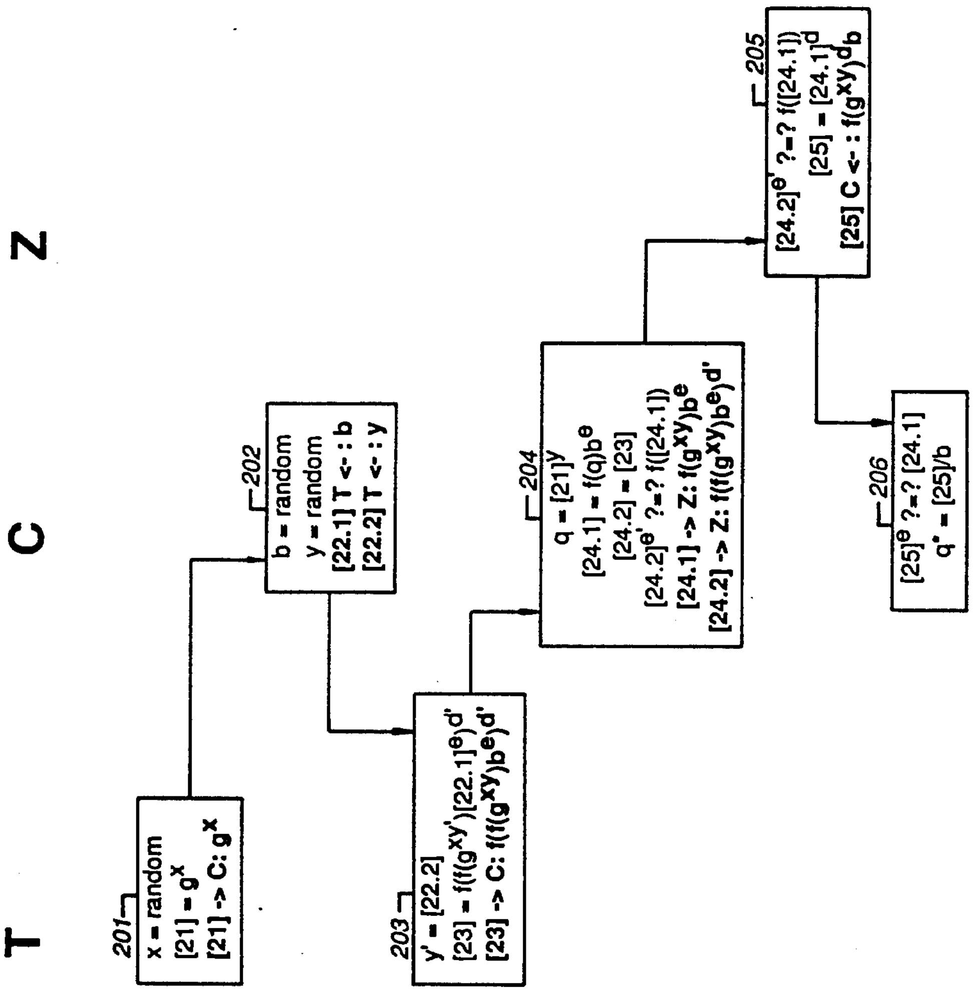

T
C
Z
201
x = random
[21] = g^x
[21] -> C: g^x
202
b = random
y = random
[22.1] T <- : b
[22.2] T <- : y
203
y' = [22.2]
[23] = f(f(g^xy')[22.1]^e)d'
[23] -> C: f(f(g^xy)b^e)d'
204
q = [21]^y
[24.1] = f(q)b^e
[24.2] = [23]
[24.2]^e' ?=? f([24.1])
[24.1] -> Z: f(g^xy)b^e
[24.2] -> Z: f(f(g^xy)b^e)d'
205
[24.2]^e' ?=? f([24.1])
[25] = [24.1]^d
[25] C <- : f(g^xy)^d b
206
[25]^e ?=? [24.1]
q* = [25]/b

FIG. 3

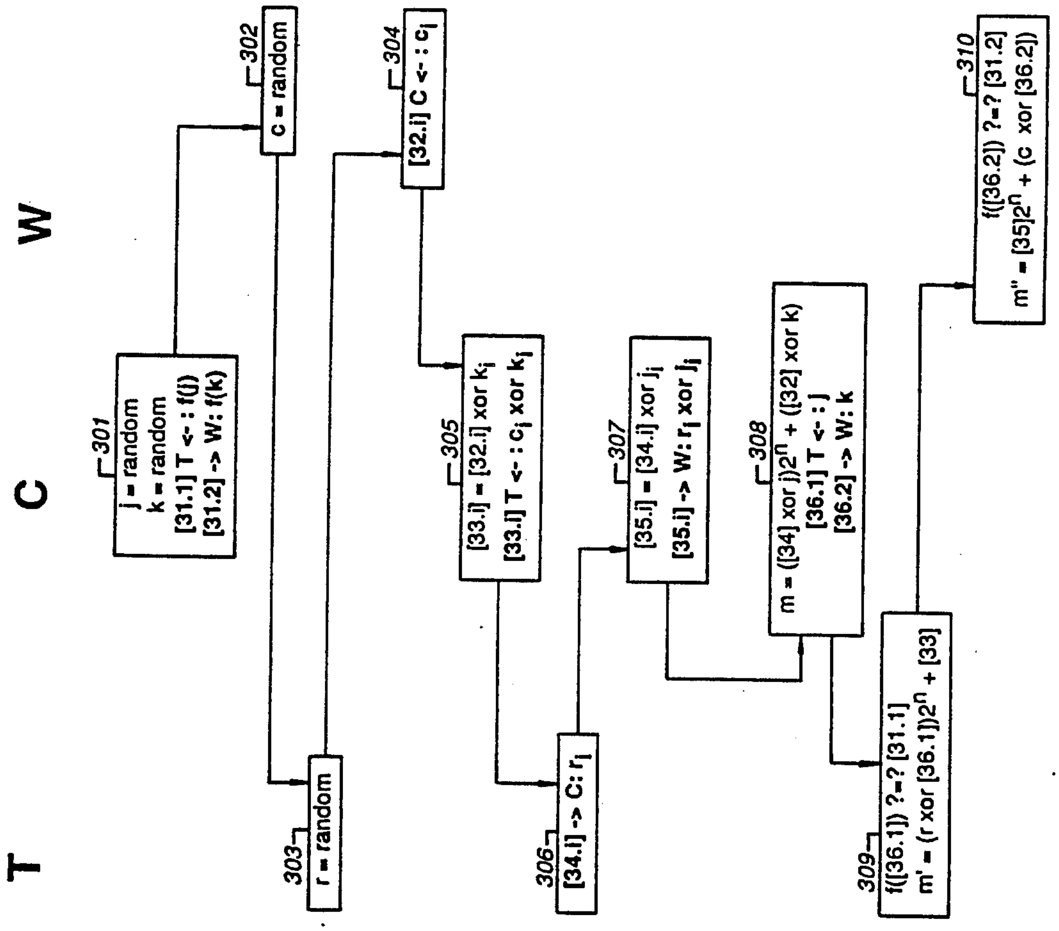
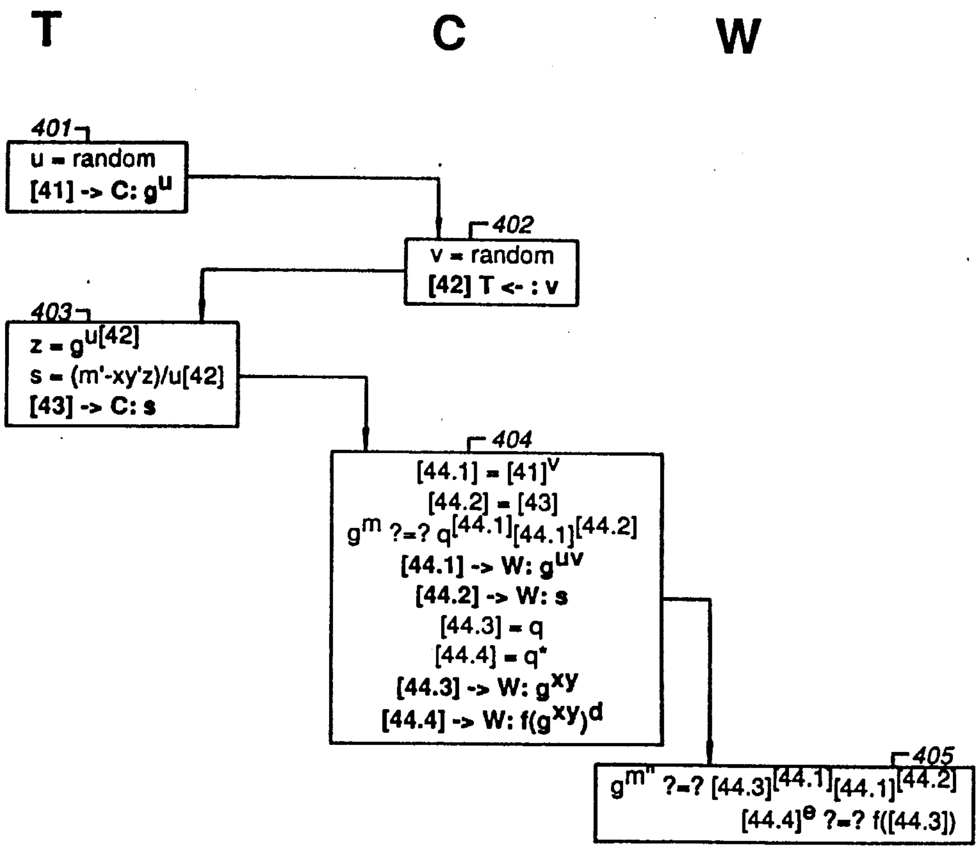

T
C
W
301
j = random
k = random
[31.1] T <- : f(j)
[31.2] -> W: f(k)
302
c = random
303
r = random
304
[32.i] C <- : c_i
305
[33.i] = [32.i] xor k_i
[33.i] T <- : c_i xor k_i
306
[34.i] -> C: r_i
307
[35.i] = [34.i] xor j_i
[35.i] -> W: r_i xor j_i
308
m = ([34] xor j)2^n + ([32] xor k)
[36.1] T <- : j
[36.2] -> W: k
309
f([36.1]) ?=? [31.1]
m' = (r xor [36.1])2^n + [33]
310
f([36.2]) ?=? [31.2]
m'' = [35]2^n + (c xor [36.2])

FIG. 4


T
C
W
401
u = random
[41] -> C: $g^u$
402
v = random
[42] T <- : v
403
z = $g^{u[42]}$
s = (m'-xy'z)/u[42]
[43] -> C: s
404
[44.1] = $[41]^v$
[44.2] = [43]
$g^m$ ?=? $q^{[44.1]}[44.1]^{[44.2]}$
[44.1] -> W: $g^{uv}$
[44.2] -> W: s
[44.3] = q
[44.4] = q*
[44.3] -> W: $g^{xy}$
[44.4] -> W: $f(g^{xy})^d$
405
$g^{m''}$ ?=? $[44.3]^{[44.1]}[44.1]^{[44.2]}$
$[44.4]^e$ ?=? f([44.3])

# 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