US005841866A

# United States Patent [19]

**Bruwer et al.**

[11] **Patent Number: 5,841,866**

[45] **Date of Patent: Nov. 24, 1998**

[54] **SECURE TOKEN INTEGRATED CIRCUIT AND METHOD OF PERFORMING A SECURE AUTHENTICATION FUNCTION OR TRANSACTION**

[75] Inventors: **Frederick Johannes Bruwer**; **Pieter Jacobus Pretorius**; **Theodor Johannes Dippenaar**, all of Verwoerdburg, South Africa

[73] Assignee: **Microchip Technology Incorporated**, Chandler, Ariz.

[21] Appl. No.: **537,292**

[22] Filed: **Sep. 29, 1995**

[30] **Foreign Application Priority Data**

Sep. 30, 1994 [ZA] South Africa ..... 94/7654
Oct. 5, 1995 [ZA] South Africa ..... 95/8377

[51] **Int. Cl.**[6] ..... **H04L 9/00**
[52] **U.S. Cl.** ..... **380/23**; 380/25
[58] **Field of Search** ..... 380/23, 25

[56] **References Cited**

U.S. PATENT DOCUMENTS

| | | | |
|---|---|---|---|
| Re. 29,525 | 1/1978 | Willnott . | |
| 4,380,762 | 4/1983 | Capasso . | |
| 4,385,296 | 5/1983 | Tsuraki et al. . | |
| 4,426,637 | 1/1984 | Apple et al. . | |
| 4,529,980 | 7/1985 | Liotine et al. . | |
| 4,535,333 | 8/1985 | Twodolbki . | |
| 4,574,247 | 3/1986 | Jacob . | |
| 4,590,470 | 5/1986 | Koenig . | |
| 4,596,985 | 6/1986 | Bongard et al. . | |
| 4,638,433 | 1/1987 | Schindler . | |
| 4,652,860 | 3/1987 | Weishaupt et al. . | |
| 4,686,529 | 8/1987 | Kleefeldt . | |
| 4,710,613 | 12/1987 | Shigenaga | 380/25 |
| 4,723,121 | 2/1988 | Van Den Doorn et al. . | |
| 4,737,770 | 4/1988 | Brunius et al. . | |
| 4,750,118 | 6/1988 | Heitschel et al. . | |
| 4,779,898 | 10/1988 | Micznik et al. . | |
| 4,835,487 | 5/1989 | Kataoka et al. . | |
| 4,847,614 | 7/1989 | Keller . | |
| 4,855,713 | 8/1989 | Brunius . | |
| 4,878,052 | 10/1989 | Schulze . | |
| 4,885,788 | 12/1989 | Takaragi et al. | 380/25 |
| 4,890,108 | 12/1989 | Drori et al. . | |
| 4,912,463 | 3/1990 | Li . | |
| 4,928,098 | 5/1990 | Daummeger . | |
| 4,931,789 | 6/1990 | Pimmow . | |
| 4,951,029 | 8/1990 | Severson . | |
| 4,988,992 | 1/1991 | Heitschel et al. . | |
| 5,001,332 | 3/1991 | Schrenk . | |
| 5,049,867 | 9/1991 | Stouffer . | |
| 5,055,781 | 10/1991 | Takeuchi . | |
| 5,103,221 | 4/1992 | Memmola . | |
| 5,148,159 | 9/1992 | Clark et al. . | |
| 5,153,581 | 10/1992 | Hazard | 380/25 |
| 5,191,610 | 3/1993 | Hill et al. | 380/23 |
| 5,299,262 | 3/1994 | Brickell et al. | 380/30 |
| 5,347,580 | 9/1994 | Molva et al. | 380/25 |
| 5,491,752 | 2/1996 | Kaufman et al. | 380/25 |

FOREIGN PATENT DOCUMENTS

| | | |
|---|---|---|
| 0 244 332 A1 | 11/1987 | European Pat. Off. . |
| 0 459 781 A1 | 12/1991 | European Pat. Off. . |
| 2 685 520 | 6/1993 | France . |
| WO 93/20538 | 10/1993 | WIPO . |
| WO 94/11829 | 5/1994 | WIPO . |

*Primary Examiner*—Savlatore Cangialosi
*Attorney, Agent, or Firm*—Oblon, Spivak, McClelland, Maier & Neustadt, P.C.

[57] **ABSTRACT**

A method of operating a circuit such as an integrated circuit carried on a plastic card which includes the steps of accepting a challenge, and generating a first response to the challenge using a first algorithm which operates on at least the challenge and a secret key derived from information relating to the circuit. The challenge may be generated, and accepted, by the circuit, with a corresponding challenge being generated externally of the circuit. Alternatively, the challenge is generated externally of the circuit and is then accepted by the circuit. A token count may be stored in the circuit and the first response is generated if a decrement command is successfully carried out on the token count.

**50 Claims, 3 Drawing Sheets**

