Trials@uspto.gov
571-272-7822

Paper 24
Entered: November 6, 2017

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

CPI CARD GROUP INC.,
Petitioner,

v.

GEMALTO S.A.,
Patent Owner.

Case IPR2016-01092
Patent 5,944,833

Before TREVOR M. JEFFERSON, PATRICK M. BOUCHER, and TERRENCE W. McMILLIN, *Administrative Patent Judges*.

BOUCHER, *Administrative Patent Judge*.

FINAL WRITTEN DECISION
35 U.S.C. §318(a) and 37 C.F.R. § 42.73

CPI Card Group Inc. ("Petitioner") filed a Petition (Paper 2, "Pet.") to institute an *inter partes* review of claims 1–26 of U.S. Patent No. 5,944,833 ("the '833 patent"), and we instituted review of claims 1–5, 7, 12–14, and

17–26. Paper 8 ("Dec."), 23–24. We subsequently denied Petitioner's Request for Rehearing (Paper 11) of our denial of review of claims 6, 8–11, 15, and 16. Paper 14.

During the trial, Patent Owner timely filed a Response (Paper 12, "PO Resp."), to which Petitioner timely filed a Reply (Paper 15, "Reply"). An oral hearing was held on August 4, 2017, and a copy of the transcript was entered into the record. Paper 22 ("Tr.").

We have jurisdiction under 35 U.S.C. § 6. This Decision is a Final Written Decision under 35 U.S.C. § 318(a) as to the patentability of the claims on which we instituted trial. Based on the record before us, Petitioner has shown, by a preponderance of the evidence, that claims 1–5, 12–14, 17, 19–21, and 23–26 are unpatentable, but has not shown that claims 7, 18, or 22 are unpatentable.

I. BACKGROUND

A. The '833 Patent

The '833 patent addresses security vulnerabilities in microprocessors that result from the predictable character of regularly timed clock pulses. Ex. 1001, col. 1, ll. 14–60. As the Specification explains, "microprocessors and microcomputers sequentially execute successive instructions of a program stored in a memory, in sync with one or more timing signals referenced relative to one of the clock signals supplied to the microprocessor or microcomputer." *Id.* at col. 1, ll. 14–18. Such clock signals may be supplied either internally or externally. *Id.* at col. 1, ll. 18–19. Because the execution of each particular instruction breaks down into several steps timed

by the clock pulses, "it is possible to correlate the various phases of this program execution with the clock signals." *Id.* at col. 1, ll. 20–23.

The Specification provides examples of the types of vulnerabilities that may result. For instance, it is possible to determine the number of clock pulses delivered since the startup of a program, "or even the time that has elapsed since an event or an external or internal reference signal." *Id.* at col. 1, ll. 39–43. As a consequence, "an ill-intentioned individual would thus be able to know the successive states of the processor and use this information to gain knowledge of certain internal output data." *Id.* at col. 1, ll. 47–50. By exploiting the regularity of the clock pulses, information could be gleaned by a bad actor "on the output data or on the confidential content of the information, and in the case of cryptographic calculations, on the secret encryption key used." *Id.* at col. 1, ll. 56–60. As Patent Owner summarizes, the objective of the '833 patent is thus to render "observation of [the microprocessor's] internal data values unobservable from outside." PO Resp. 2.

To accomplish this, the '833 patent describes "decorrelating the running of at least one instruction sequence of a program from the internal or external signals of the circuit." Ex. 1001, col. 2, ll. 9–11. In particular, decorrelation may be achieved with a random-number generator that enables desynchronizing execution of the program sequence in the processor. *Id.* at col. 2, ll. 18–21. Structure for achieving such decorrelation is illustrated in Figure 1 of the '833 patent, which is reproduced below.

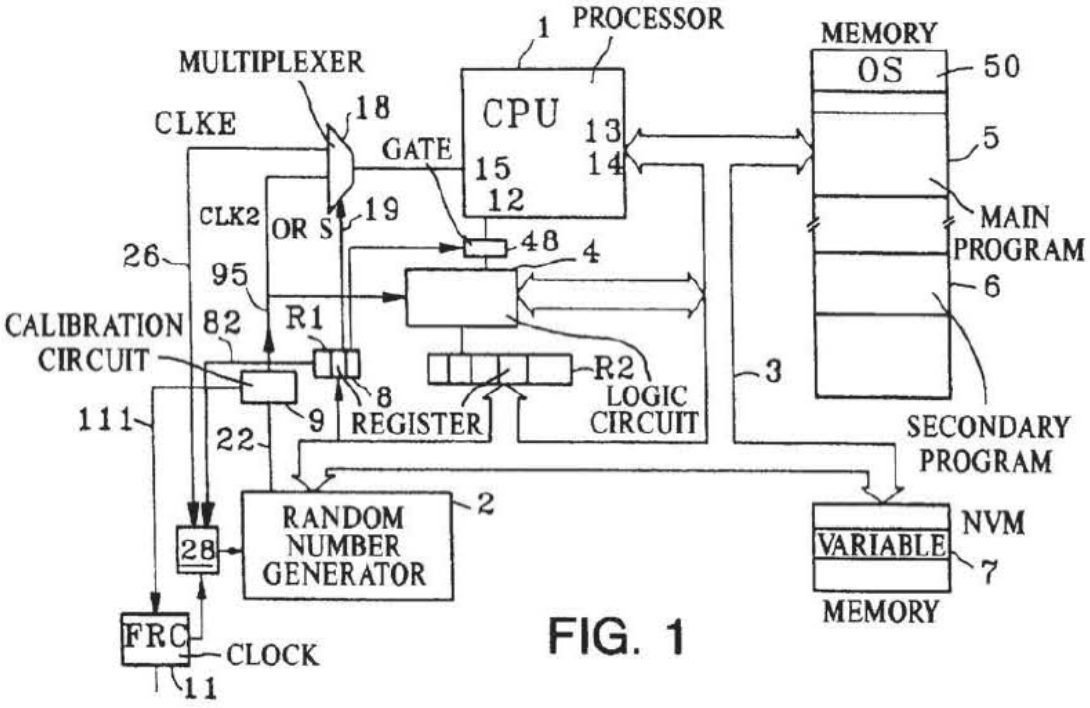

FIG. 1

Figure 1 is a schematic diagram of electronic circuits of a microcomputer. *Id.* at col. 3, ll. 24–25.

The microcomputer includes random-number generator 2, which can run on internal clock 11. *Id.* at col. 3, ll. 59–61. Internal clock 11 ("FRC") may be embodied by "a free fixed frequency oscillator, de-synchronized and phase shifted relative to the external clock CLKE" of the microcomputer. *Id.* at col. 4, ll. 23–28. Random-number generator 2 either supplies a random value that is loaded into various devices of the microcomputer via data bus 3, or generates a pulse signal of variable periodicity at output 22. *Id.* at col. 4, ll. 40– 44. To serve as a clock for processor 1, this signal "must be sent" to calibration circuit 9, whose output 95 (i.e., "decorrelation clock" CLK2) is sent to multiplexing circuit 18. *Id.* at col. 4, ll. 50–53. Decorrelation clock CLK2, thus, results from modulation of internal clock 11 with the output of random-number generator 2. *See id.* at col. 8, l. 50– col. 9, l. 36. Input 19 to multiplexing circuit 18 controls the multiplexing

with one or more bits of register 8, which can be loaded by random-number generator 2 or with a value determined by main program 5. *Id.* at col. 4, ll. 52–57. That is, selection of whether the clock used for sequencing processor 1 is external clock CLKE or decorrelation clock CLK2 is determined either randomly or by main program 5. *Id.* at col. 4, ll. 57–63. Random interrupts may be generated similarly, by loading register R2 with a value determined by random number generator 2 or by main program 5. *Id.* at col. 5, ll. 20–23.

B. Illustrative Claim

Independent claim 4 is illustrative of the claims at issue:

> 4. An improved integrated circuit comprising a microprocessor having a main program arranged to execute at least one instruction sequence in the microprocessor in synchronization with internal or external electrical signals of the integrated circuit and means for decorrelating an execution of the at least one instruction sequence of the main program from the internal or external signals of the integrated circuit so that the execution of the at least one instruction sequence is desynchronized with respect to the internal or external electrical signals.

C. Instituted Grounds of Unpatentability

Petitioner relies on the following references. Pet. 3.

Sprunk	US 5,404,402	Apr. 4, 1995	Ex. 1004
Griffin	US 5,249,294	Sep. 28, 1993	Ex. 1005
Matsumura	US 4,908,038	Mar. 13, 1990	Ex. 1006

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.