Trials@uspto.gov
Tel: 571-272-7822

Paper 50
Entered: April 3, 2015

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

INTERNATIONAL BUSINESS MACHINES CORPORATION,
Petitioner,

v.

INTELLECTUAL VENTURES II LLC,
Patent Owner.

Case IPR2014-00180
Patent 7,634,666 B2

Before MIRIAM L. QUINN, DAVID C. MCKONE,
and JAMES A. TARTAL, *Administrative Patent Judges.*

MCKONE, *Administrative Patent Judge*.

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

I. INTRODUCTION

A. Background

International Business Machines Corp. ("Petitioner") filed a Petition (Paper 1, "Pet.") to institute an *inter partes* review of claims 1–11 of U.S. Patent No. 7,634,666 (Ex. 1005, "the '666 patent"). Intellectual Ventures II LLC ("Patent Owner") filed a Preliminary Response (Paper 9, "Prelim. Resp."). Pursuant to 35 U.S.C. § 314, in our Decision to Institute (Paper 10, "Dec."), we instituted this proceeding as to all of the challenged claims of the '666 patent.

After the Decision to Institute, Patent Owner filed a Patent Owner Response (Paper 24, "PO Resp.") and Petitioner filed a Reply to the Patent Owner Response (Paper 29, "Reply"). An oral hearing (Paper 49, "Tr.") was held on January 13, 2015.

B. Related Cases

Patent Owner has asserted the '666 patent in several United States district courts against various defendants. Pet. 1–2; Paper 7, at 2–3.

C. References Relied Upon

Petitioner relies upon the following prior art references:

US 6,963,644 B1 (issued Nov. 8, 2005, filed Apr. 6, 2000) ("Matsuzaki," Ex. 1008)

US 6,009,450 (Dec. 28, 1999) ("Dworkin," Ex. 1012)

Alexandre F. Tenca and Çetin K. Koç, *A Scalable Architecture for Montgomery Multiplication*, CHES '99, 1717 LNCS, 94–108 (1999) ("Tenca," Ex. 1014)

D. The Asserted Grounds

We instituted this proceeding based on the grounds of unpatentability set forth in the table below. Dec. 26–27.

References	Basis	Claims challenged
Matsuzaki and Dworkin	§ 103(a)	1
Matsuzaki and Dworkin	§ 103(a)	4
Matsuzaki, Dworkin, and Tenca	§ 103(a)	2, 5
Matsuzaki, Dworkin, and Tenca	§ 103(a)	3, 6
Matsuzaki, Dworkin, and the knowledge of one having ordinary skill in the art	§ 103(a)	7, 9
Matsuzaki and Dworkin	§ 103(a)	8, 11
Matsuzaki and Dworkin	§ 103(a)	10

E. The '666 Patent

The '666 patent describes a co-processor, coupled to a host processor, for executing both Rivest-Shamir-Adleman ("RSA") and Elliptic Curve Cryptography ("ECC") public key encryption algorithms. Ex. 1005, 1:6–11, 1:32–36. The two encryption algorithms share a common arithmetic operation. *Id.* at 1:25–26.

The co-processor includes a modular arithmetic unit and an interface control unit for interfacing between the arithmetic unit and the host processor. *Id.* at Fig. 1, 2:64–66. The interface control unit receives encryption key and operation code ("op-code") data from the host processor and outputs status and interrupt signals to the host processor. *Id.* at 3:2–6.

The interface control unit includes a bus interface unit, a concatenation/split unit, and a cryptographic controller with a modular-op-code generator. *Id.* at Fig. 3, 3:40–43.

Figure 2 is reproduced below:

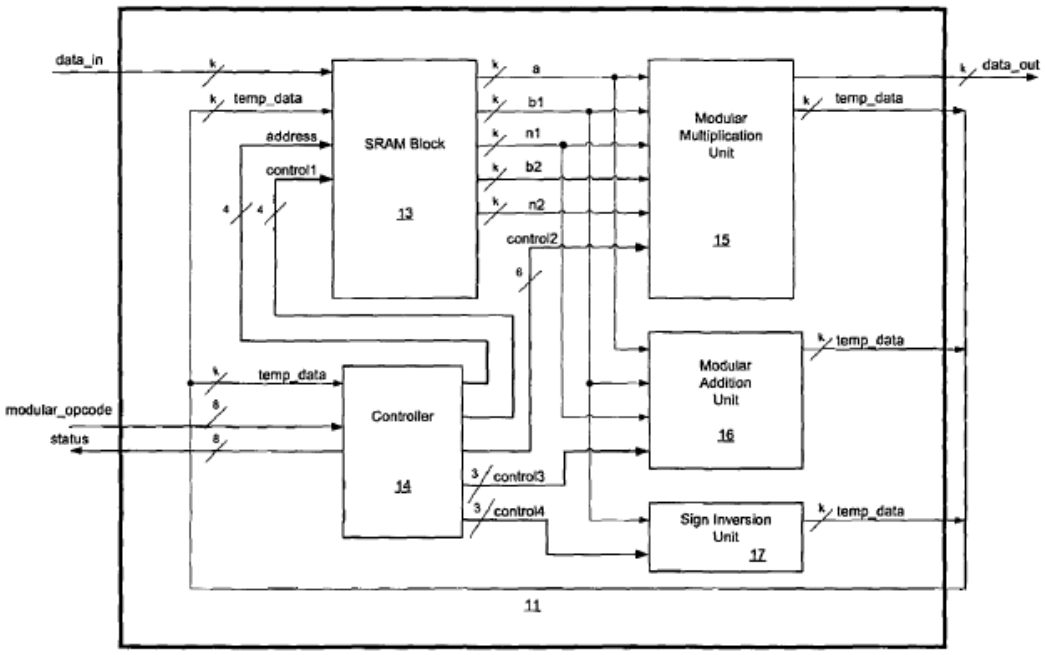

FIGURE 2

Figure 2 is a block diagram of a modular arithmetic unit. *Id.* at 2:29.

The modular arithmetic unit includes multiplication unit 15, addition unit 16, and sign inversion unit 17 for performing arithmetic manipulations related to encryption. *Id.* at Fig. 2, 3:12–14. The modular arithmetic unit also includes static random access memory ("SRAM") block 13 for storing data received from the host processor and loading them into the units that perform arithmetic manipulations. *Id.* at Fig. 2, 3:11–12. The SRAM block includes an address decoder, several SRAM elements for storing data,

an input switch (multiplexer 23), and several output switches (multiplexers 1–5). *Id.* at Fig. 4, 4:4–9. The modular arithmetic unit further includes a controller for controlling operation of the modular arithmetic unit. *Id.* at Fig. 2, 3:11–12.

As shown in Figure 2, outputs of the multiplication unit, the addition unit, and the sign inversion unit labeled "temp_data" are fed back to each of SRAM Block 13 and Controller 14. *Id.* at Fig. 2, 3:21–23, 3:29–39.

Claim 1, reproduced below, is illustrative of the claimed subject matter:

> 1. A crypto-engine for cryptographic processing of data comprising an arithmetic unit operable as a co-processor for a host processor and an interface controller for managing communications between the arithmetic unit and host processor, the arithmetic unit including:
>
> a memory unit for storing and loading data, the memory unit including
>
> an input switch for selecting input-interim data;
>
> a plurality of Static Random Access Memory elements for receiving and storing the input/interim data from the input switch;
>
> a plurality of output switches connected to the memory elements; and
>
> an address controller for controlling flow of the data through the switches and memory elements
>
> a multiplication unit, an addition unit and a sign inversion unit for performing arithmetic operations on said data, the multiplication

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.