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:

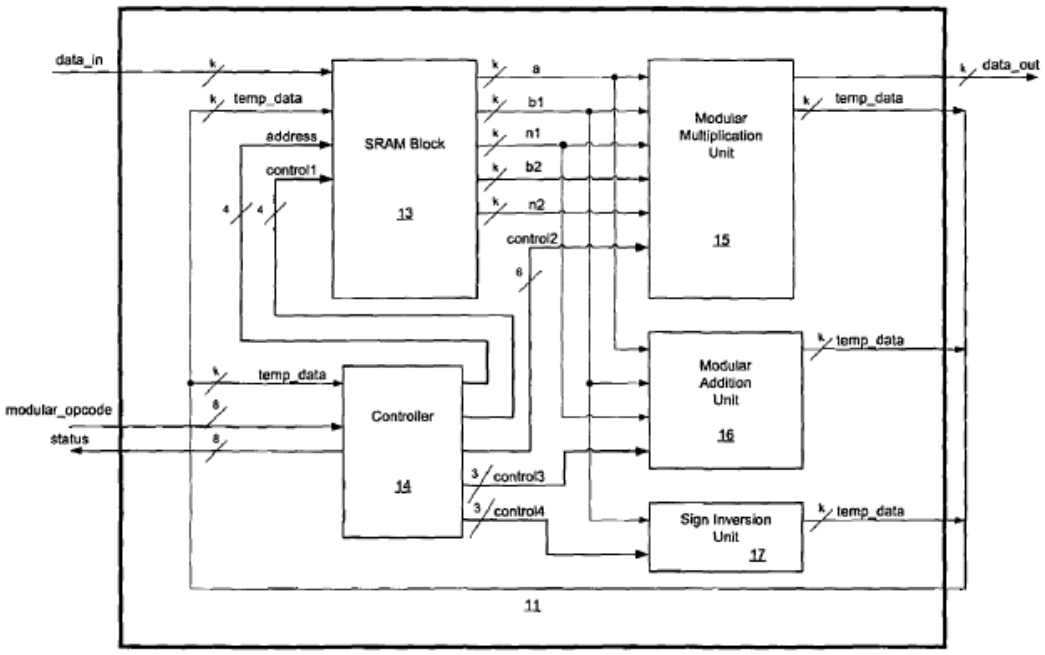

FIGURE 2

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

> unit, the addition unit and the sign inversion unit each having an output; and
>
> an arithmetic controller for controlling the storing and loading of data by the memory unit and for enabling the multiplication, addition and sign inversion units;
>
> wherein the outputs of the multiplication unit, the addition unit and the sign inversion unit are feedback to the arithmetic controller.

II. ANALYSIS

A. Claim Construction

The Board interprets claims of an unexpired patent using the broadest reasonable construction in light of the specification of the patent in which they appear. *See* 37 C.F.R. § 42.100(b); *In re Cuozzo Speed Techs., LLC*, 778 F.3d 1271, 1279–81 (Fed. Cir. 2015). Claim terms generally are given their ordinary and customary meaning, as would be understood by one of ordinary skill in the art in the context of the entire disclosure. *See In re Translogic Tech., Inc.*, 504 F.3d 1249, 1257 (Fed. Cir. 2007).

1. "multiplication unit," "addition unit," and "sign inversion unit"

Petitioner proposes the following constructions:

> "multiplication unit": "a unit *solely* capable of performing multiplication on input data.";
>
> "addition unit": "a unit *solely* capable of performing addition on input data."; and
>
> "sign inversion unit": "a unit *solely* capable of performing additive inversion on input data."

Pet. 6–8 (emphases added). In the Decision to Institute, we preliminarily determined that the multiplication, addition, and sign inversion units should not be limited to "solely" one function each, rejecting Petitioner's arguments that relied on the Specification and prosecution history of the '666 patent. Dec. 10–11.

In the Reply, Petitioner argues that our preliminary constructions were incorrect in light of the deposition testimony (Ex. 1036) of Lee Ming Cheng, Ph.D., an inventor named on the '666 patent. Reply 14–15. According to Petitioner, Dr. Cheng testified in a different proceeding that the multiplication unit depicted in Figure 5 of the '666 patent performs Montgomery multiplication, but that its components perform no other mathematical functions. Reply 14 (citing Ex. 1036, 65:15–71:3, 71:14–22, 72:21–73:4, 74:7–18).

Assuming Petitioner's characterization of Dr. Cheng's testimony is correct, such testimony nevertheless would not support Petitioner's proposed constructions. Dr. Cheng's testimony is limited to the technical details of Figure 5, an example described in the '666 patent. Petitioner has not explained persuasively why the example of Figure 5 should limit the claims. *See In re Am. Acad. of Sci. Tech. Ctr.*, 367 F.3d 1359, 1369 (Fed. Cir. 2004) ("We have cautioned against reading limitations into a claim from the preferred embodiment described in the specification, even if it is the only embodiment described, absent clear disclaimer in the specification.") (citations omitted).

In the Reply, Petitioner again points to the prosecution history of the '666 patent, arguing that it characterizes two arithmetic units of a Stojancic reference as performing multiplication, addition, and sign inversion.

Reply 15 (citing Ex. 1018, at 5). Petitioner argues that this is a disclaimer of multifunctional units. Reply 15. We are not persuaded. The portion of the prosecution history cited by Petitioner characterizes the prior art, not the scope of the claims. We agree with Patent Owner that this does not rise to the level of "clear and unmistakable disavowal." PO Resp. 8 (quoting *Biogen Idec, Inc. v. GalxoSmithKline LLC*, 713 F.3d 1090, 1095 (Fed. Cir. 2013)).

Accordingly, on the full trial record, we maintain our preliminary construction declining to limit "multiplication unit," "addition unit," and "sign inversion unit" to one function each.

2. "feedback"

Claim 1 requires "wherein the outputs of the multiplication unit, the addition unit and the sign inversion unit are feedback to the arithmetic controller." Petitioner proposes construing "feedback" to mean "a result that is *directly* transmitted back." Pet. 8 (emphasis added). In the Decision to Institute, we were not persuaded by Petitioner's arguments that the plain language of the claims and the Specification warranted such a construction, and declined to construe preliminarily the claims to include such a limitation. Dec. 11. Specifically, we recognized that the '666 patent describes an embodiment in which temporary data is fed back directly from the multiplication, addition, and sign inversion units to a controller. Dec. 11. This is shown in Figure 2, reproduced above, where "[t]he outputs . . . k-bit 'temp_data' of MMU 15/ MADU 16/SIU 17 go to Controller 14." Ex. 1005, 3:21–23. Nevertheless, on the record at that time, we declined to limit "feedback" based on an example of direct feedback in the Specification.

Dec. 11. Petitioner does not challenge our initial construction of "feedback" in its Reply.

In its Response, Patent Owner supports our preliminary construction in the Decision to Institute. PO Resp. 9. In response to questioning at the hearing, however, Patent Owner qualified its argument by noting that, if feedback is routed through intermediate components that change its value, the data would no longer be feedback of that value. Tr. 45:9–46:2. For example, if the value of the feedback from the multiplication unit changes before reaching the controller, it no longer would be output of the multiplication unit fed back to the controller. *Id.* Patent Owner's argument is consistent with the plain language of the claims and the Specification. It is also consistent with the testimony of Petitioner's Declarant, Dr. Çetin Koç, Ph.D., in support of Petitioner's Reply, who testifies that the temp_data signals of the '666 patent are multiplexed from the computational units to the controller. Ex. 1029 ("Koç Reply Decl.") ¶ 42.

In sum, we construe "wherein the outputs of the multiplication unit, the addition unit and the sign inversion unit are feedback to the arithmetic controller" to mean that the output values of the multiplication unit, the addition unit, and the sign inversion unit are feedback to the arithmetic controller, although those values may pass, unchanged, through intermediate components (e.g., latches and multiplexers).

B. Motions to Exclude

1. Petitioner's Motion to Exclude

Petitioner moves to exclude Exhibits 2003, 2004, and 2010(A)–(D), arguing that they are incomplete and inaccurate. Paper 35 (Pet. Mot. to

Exclude) 1–6. We do not rely on these exhibits, however. Accordingly, Petitioner's motion is moot.

Petitioner's Motion to Exclude is denied.

2. Patent Owner's Motion to Exclude

Patent Owner moves to exclude Exhibit 1036, a transcript of the deposition of Dr. Cheng (discussed above) as irrelevant and cumulative. Paper 34 (PO Mot. to Exclude) 3–7. Patent Owner argues that, in district court litigation, inventor testimony generally has little probative value. *Id.* at 4–5. As to Dr. Cheng's testimony in particular, Patent Owner contends that it does not relate to the meaning of a claim term in the art. *Id.* at 5. Patent Owner also argues that Dr. Cheng's testimony is cumulative of the testimony of Petitioner's Declarant, Dr. Koç (Ex. 1001, "Koç Decl."). PO Mot. to Exclude 6–7. Patent Owner's arguments do not show the Cheng deposition transcript to be unduly prejudicial under Federal Rule of Evidence 403. Rather, Patent Owner's arguments go to the weight we should give to the evidence. Accordingly, we decline to exclude Exhibit 1036.

Patent Owner moves to exclude Exhibits 1031, 1033, and 1035, which embody articles it argues Petitioner should have addressed in the Petition. PO Mot. to Exclude 7–10. We do not rely on these exhibits, however. Accordingly, Patent Owner's motion is moot as to these exhibits.

Patent Owner further moves to exclude Paragraphs 26–43 of the Koç Reply Declaration (Ex. 1029), arguing that they are inconsistent with Dr. Koç's first Declaration and are not responsive to Patent Owner's Response. PO Mot. to Exclude 10–13. We do not rely on these paragraphs,

however. Accordingly, Patent Owner's motion is moot as to these paragraphs.

Patent Owner's Motion to Exclude is denied.

C. Obviousness Combinations Including Matsuzaki and Dworkin

1. Overview of Matsuzaki

Matsuzaki describes a co-processor for performing ECC using Montgomery reduction. Ex. 1008, Abstract, 7:40–45. Montgomery reduction is an algorithm for performing high-speed modular arithmetic. *Id.* at 7:57–67.

Figure 1 of Matsuzaki is reproduced below:

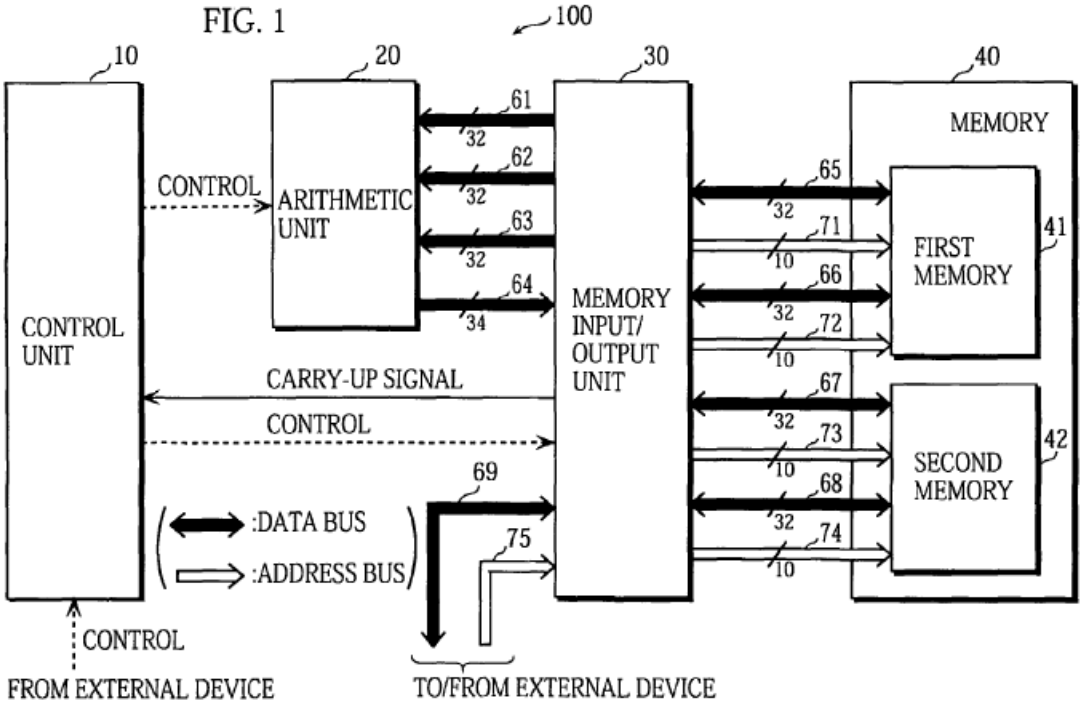

Figure 1 is a block diagram of a multi-word arithmetic co-processor that performs arithmetic calculations based on instructions from a host device.

Id. at 7:39–45, 7:53–56. The co-processor includes a control unit, an arithmetic unit, a memory input/output unit, and a memory. *Id.* at 7:48–51.

The memory input/output unit transfers data among the arithmetic unit, the memory, and an external device. *Id.* at 8:31–35. It includes an address generating unit and a bus switch with a plurality of selector circuits that connect data buses from the arithmetic unit to the memory according to instructions from the control unit. *Id.* at Fig. 3, 9:43–53. The memory includes two dual-port memories that store data on which arithmetic is performed, as well as intermediate calculation results. *Id.* at Fig. 1, 8:17–25.

Figure 17, reproduced below, is an example of an arithmetic unit:

FIG. 17

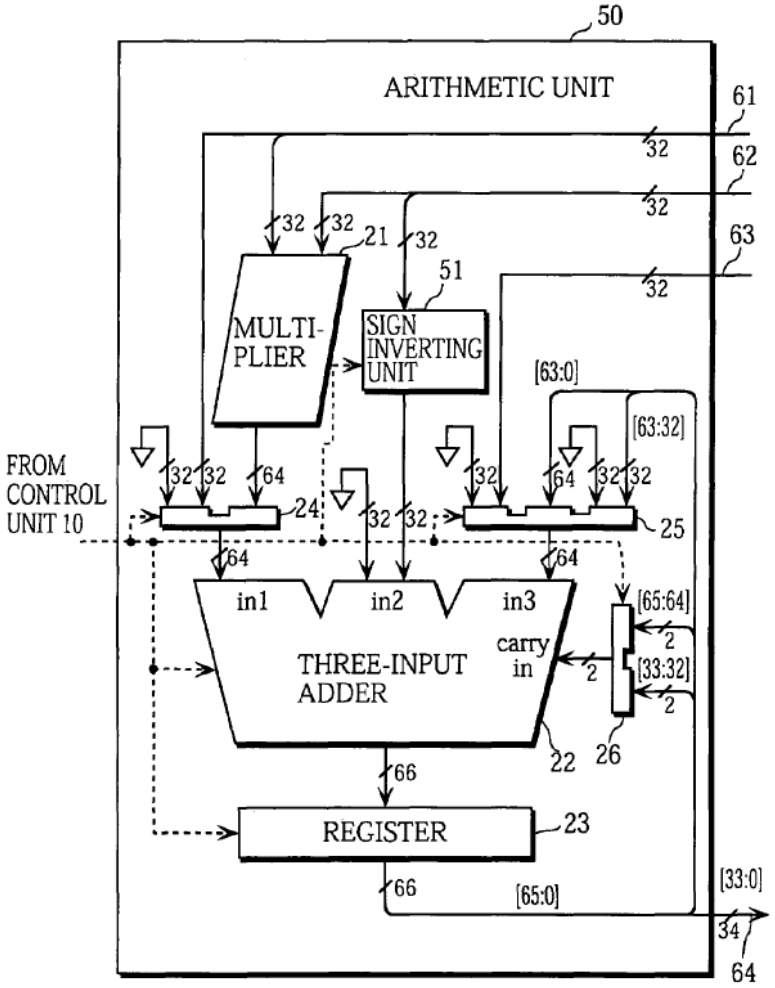

Figure 17 is a block diagram of circuity for an arithmetic unit. *Id.* at 7:26–28. The arithmetic unit can include multiplier 21, adder 22, and sign inverting unit 51. *Id.* at Fig. 17, 19:1–13. The arithmetic unit performs calculations on data from the memory pursuant to instructions from control unit 10. *Id.* at 10:10–18. The output of adder 22 is feedback to control unit 10. *Id.* at 9:5–12. As can be seen from Figure 17, however, the outputs of

multiplier 21 and sign inverting unit 51 are inputs to adder 22, rather than feedback to control unit 10.

2. Overview of Dworkin

Dworkin describes a processor for performing finite field and integer arithmetic for ECC and RSA cryptography. Ex. 1012, 1:5–6, 1:26–33, 1:36–38. Figure 2 is reproduced below:

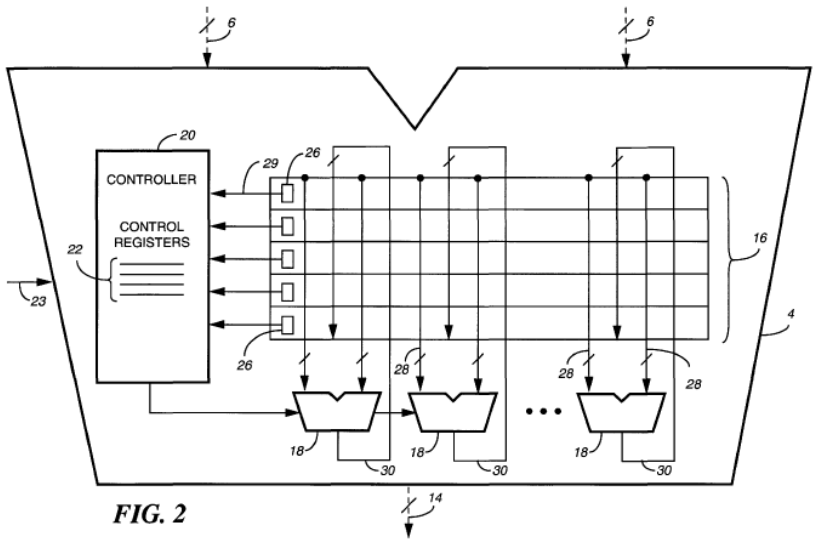

FIG. 2

Figure 2 illustrates an arithmetic-logic unit ("ALU") for performing the arithmetic calculations of the processor, including finite field and integer arithmetic. *Id.* at 2:46–47, 3:1–5. The ALU includes several sub-ALUs 18 that perform functions such as XOR, shift left, shift right, XOR-shift, integer add, and integer subtract. *Id.* at 3:41–44. According to Petitioner's declarant, Dr. Çetin Koç, one of the operations disclosed in Dworkin is Montgomery reduction. Ex. 1001 ¶ 146 (citing Ex. 1012, 7:21–38).

The ALU includes special purpose registers 16 and controller 20. The controller sequences the steps of a computational operation to be performed

by the ALU pursuant to control bits stored in the special purpose registers. Ex. 1012, 3:6–17.

3. Petitioner has not shown that Matsuzaki and Dworkin teach the Claimed Feedback

Petitioner contends that claim 1 would have been obvious over Matsuzaki and Dworkin. Specifically, Petitioner argues that: Matsuzaki's arithmetic device is a co-processor and the external device it communicates with is a host processor (Pet. 23–24); Matsuzaki's memory input/output unit, in particular the bus switch, is an input switch and a plurality of output switches (*id.* at 24–26); Matsuzaki's address generating unit is an address controller (*id.* at 27); Matsuzaki's arithmetic unit, specifically the embodiment shown in Figure 17, includes a multiplication unit, an addition unit, and a sign inversion unit (*id.* at 27–28); and Matsuzaki's control unit is an arithmetic controller (*id.* at 28–29).

With regard to the feedback limitation, Petitioner argues that Matsuzaki's carry-up signal (Ex. 1008, 9:54–63, Fig. 1) feeds information from the arithmetic unit back to the control unit, which Petitioner contends is an arithmetic controller. Pet. 29–30. Petitioner concedes, however, that "[t]he only element of independent claim 1 one could argue is not taught by Matsuzaki, in combination, as claimed, is that 'outputs' (plural) of the multiplication unit, the addition unit, and the sign inversion unit are directly sent back to the arithmetic controller." *Id.* at 17; *accord* Ex. 1001 ¶ 116. As can be seen in Figure 17 (reproduced above) the outputs of the multiplier and sign inversion unit are fed to the adder, rather than the controller. The adder operates on (and, thus, changes) those values and outputs a single

feedback to the controller. Thus, we find that Matsuzaki does not disclose the feedback limitation of claims 1 and 4.

Nevertheless, Petitioner contends that the feedback limitation is taught by Dworkin, and that a person of ordinary skill in the art would have combined Matsuzaki and Dworkin. Pet. 17. In the Petition, Petitioner, relying on Dr. Koç, contended (with reference to Figure 2 of Dworkin) that a first sub-ALU 18 corresponds to a multiplication unit, a second sub-ALU 18 corresponds to an addition unit, and a third sub-ALU 18 corresponds to a sign inversion unit, and that each of these sub-ALUs directly sends back its output to controller 20. *Id.* at 30–31 ("Dworkin discloses wherein the outputs of the multiplication unit (e.g., sub-ALU 18), the addition unit (e.g., sub-ALU 18) and the sign inversion unit (e.g., sub-ALU 18) are directly sent back to the arithmetic controller (e.g., controller 20)."); Ex. 1001 ¶¶ 117–18.

Patent Owner argues that this is a mischaracterization of Dworkin; for example, Dworkin does not disclose a sign inversion unit. PO Resp. 13. Petitioner now concedes that Dworkin does not disclose each of these arithmetic units and, indeed, claims it never made such an assertion. Reply 7. Petitioner argues for the first time on Reply that Dworkin discloses multiple generic computational units (rather than the claimed arithmetic units), with each unit sending its output back to the controller. *Id.*

We are not persuaded by Petitioner. The contention presented by Petitioner in the Petition, as quoted above, was that Dworkin fed the output of an addition unit, a multiplication unit, and a sign inversion unit directly to a controller. Pet. 30. Neither the Petition nor the Koç Declaration argues that Matsuzaki could be modified by feeding the outputs of its three arithmetic units back to the controller by applying a teaching of Dworkin to

feed the outputs of multiple generic computational units directly to a controller. *See* Pet. 30–31; Ex. 1001 ¶¶ 117–18. Nor does the Petition explain how, or why, this modification of Matsuzaki would be accomplished. *Id.* Accordingly, we are not persuaded that the Petition presents sufficient evidence to support this late presented contention of obviousness.

At the hearing, Petitioner argued that its Reply arguments and evidence were not presented in detail because Dr. Koç believed that this was a trivial aspect of Dworkin that did not need to be explained. Tr. 11:15–24. Petitioner argues that it was only necessary to present this evidence after Patent Owner's expert demonstrated "confusion" and "misunderstanding" as to what Dworkin teaches. *Id.* at 12:1–22. Nevertheless, Petitioner's argument and evidence in the Reply also does not show that Dworkin teaches the claimed feedback. Patent Owner has presented persuasive evidence that Dworkin does not feedback the outputs of multiple computational units to a controller. Petitioner's Reply evidence and argument does not rebut adequately Patent Owner's position.

According to Patent Owner, if any sub-ALU 18 feeds information back to controller 20, it is only the left-most sub-ALU. PO Resp. 15–18. Patent Owner supports its arguments with the declaration testimony of Dr. Patrick Schaumont, Ph.D. (Ex. 2001, "Schaumont Decl.").

Patent Owner contends that Figure 6 of Dworkin illustrates in more detail the sub-ALUs shown in Figure 2 configured to perform finite field multiplication. PO Resp. 15 (citing Ex. 2001 ¶ 58). Figure 6 is reproduced below:

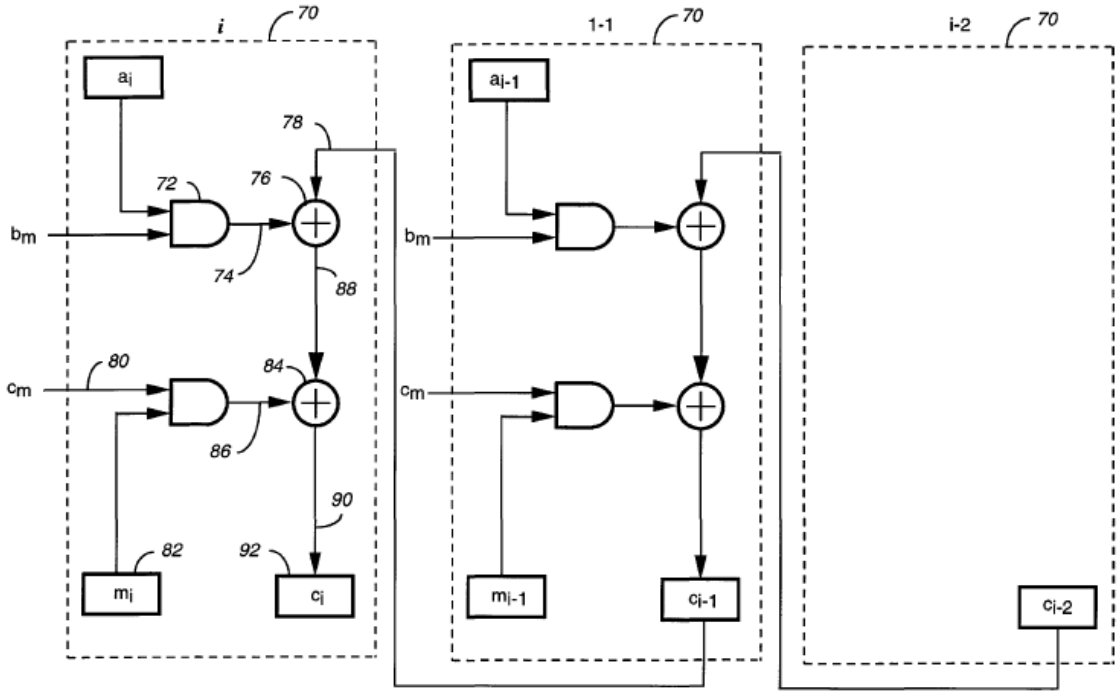

FIG. 6

Figure 6 is circuit diagram of a finite-field multiplier. Ex. 1012, 2:21–22. According to Patent Owner, each block 70 of Figure 6 corresponds to the logic performed by a sub-ALU 18 of Figure 2. PO Resp. 15; Ex. 2001 (Schaumont Decl.) ¶ 60). For example, the left-most block 70 (*i*) of Figure 6 corresponds to the left-most sub-ALU 18 of Figure 2. *Id.* Patent Owner further argues that the inputs (e.g., a_j, b_m, etc.) to the logic of each block come from corresponding cells of the special purpose registers 16 shown in Figure 2 and shown in more detail in Figure 5. PO Resp. 16; Ex. 2001 ¶ 62. We agree with these arguments regarding the correspondence of Figures 2, 5, and 6. Each box 70 in Figure 6 is referred to as "a detailed circuit implementation of the bit-slice 41 of FIG. 5 for finite field multiplication." Ex. 1012, 5:11–13. According to Dworkin, "[a] sub ALU 18 shown in

FIG. 2 may be implemented by the circuitry of block 52 of FIG. 5," which is included in bit-slice 41. *Id.* at 4:8–10.

Regarding the operation of the logic shown in Figure 6, Patent Owner contends that b_m and c_m are control bits, but are not described as feedback from any sub-ALU. PO Resp. 17; Ex. 2001 ¶¶ 64–65. Patent Owner argues that the output c_{j-2} of box 70(i-2) is fed as an input to box 70(i-1) and the output c_{j-1} of box 70 (i-1) is fed as an input to box 70. PO Resp. 16–17; Ex. 2001 ¶ 62. According to Patent Owner, only the output c_j of box 70(i) is returned on output data bus 30 (Figure 2) to the left-most cell of the C register. PO Resp. 17; Ex. 2001 ¶ 63. Because only the left-most cells of registers 26 of Figure 2 are feedback to controller 20, Patent Owner argues, the output of only the left-most sub-ALU of Figure 2 is feedback to the controller. PO Resp. 17–18; Ex. 2001 ¶¶ 63, 89. Patent Owner's arguments and evidence are persuasive as they are consistent with what is depicted clearly in Figure 6.

Petitioner, in its Reply, disagrees with Patent Owner's characterization of Dworkin. Petitioner relies on the Koç Reply Declaration to explain its competing theory of Dworkin's operation.

Petitioner's theory relies on pseudo-code reproduced in Dworkin (Ex. 1012, 4:20–28), which Dworkin characterizes as a series of steps implementing finite-field multiplication (*id.* at 4:16–19). Reply 7–9. According to Petitioner, Dworkin calculates a first partial product, with the first bit corresponding to the output of the left-most sub-ALU 18 of Figure 2, stores it in register C, and shifts the entire first partial product (all of register C) to the left; calculates a second partial product, with its second bit corresponding to the output of the next sub-ALU 18 to the right, stores it in

register C, and shifts the entire second partial product to the left; and repeats this process with subsequent partial products and sub-ALUs, with the output of each sub-ALU eventually reaching the controller. *Id.* (citing Ex. 1029 ¶¶ 30–40). Dr. Koç's Reply Declaration largely repeats the arguments in the Reply, adding annotated drawings from Dworkin, but otherwise adding no additional evidence. Ex. 1029 ¶¶ 30–40.

Petitioner, however, does not point to evidence sufficient to explain how shifting the partial products to the left results in sub-ALU's to the right of the left-most sub-ALU feeding their outputs back to the controller. Petitioner relies on the pseudo-code reproduced in Dworkin. This pseudo-code describes, at a high level, the general algorithm used in Dworkin's implementation of finite field multiplication. Figures 5 and 6, on which Patent Owner relies, depict in detail the structure used to implement the pseudo-code's algorithm. Ex. 1012, 3:49–5:29. Patent Owner has introduced persuasive evidence and testimony, based on these figures and the corresponding description, showing that the output of each sub-ALU 18 other than the left-most sub-ALU 18 is fed as an input to the next sub-ALU to the left rather than fed back to the controller. We credit this evidence.

Petitioner does not rebut persuasively Patent Owner's evidence or point to sufficient evidence that supports the contention that each of these sub-ALU outputs (other than the left-most) is nevertheless shifted to the controller. Indeed, upon being asked to testify on cross examination regarding Figures 5 and 6, Dr. Koç stated that his Reply Declaration did not address those figures or their inner workings and that he would need time to prepare in order to testify about them. Ex. 2016, 36:25–37:24. Petitioner and its Declarant failed to provide a detailed analysis of Dworkin in the

Petition and further have failed to address, in the Reply, Patent Owner's rebuttal evidence, which we find very persuasive.

In short, Petitioner has not shown that Dworkin teaches feeding back the output of multiple separate computational units to a controller. Accordingly, Petitioner has not shown that Matsuzaki and Dworkin teach "the outputs of the multiplication unit, the addition unit and the sign inversion unit are feedback to the arithmetic controller," as recited in claim 1. For the same reasons, Petitioner has not shown that Matsuzaki and Dworkin teach "wherein the outputs of the multiplication unit, an addition unit and a sign inversion unit are feedback to the arithmetic controller," as recited in independent claim 4. Claims 2, 3, and 8 depend from claim 1 and claims 5–7 and 9–11 depend from claim 4. Because Petitioner has not shown that Matsuzaki and Dworkin teach each limitation of any of claims 1–11, Petitioner has not met its burden of proving, by a preponderance of the evidence, that any of claims 1–11 would have been obvious.

4. Petitioner has not shown a Reason to Combine Matsuzaki and Dworkin

Regarding claim 1, Petitioner contends that both Matsuzaki and Dworkin address hardware implementations of cryptographic co-processors, teach Montgomery reduction, and have similar methods and internal control methodologies. Pet. 31. Accordingly, Petitioner argues, "one having ordinary skill in the art would combine the 'outputs' (plural) of Dworkin with the disclosure of Matsuzaki." *Id*. 31 (citing Ex. 1001 (Koç Decl.) ¶¶ 144–49). Petitioner's reason for combining Matsuzaki and Dworkin for claim 1 is substantially the same. Pet. 44 (citing Ex. 1001 ¶¶ 144–49). The

parties dispute whether Petitioner has provided a sufficient reason why a skilled artisan would have combined Matsuzaki and Dworkin.

According to the Supreme Court, the conclusion of obviousness based on a combination of references must be supported with explicit analysis of a reason to combine those references:

> Often, it will be necessary for a court to look to interrelated teachings of multiple patents; the effects of demands known to the design community or present in the marketplace; and the background knowledge possessed by a person having ordinary skill in the art, all in order to determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue. To facilitate review, this analysis should be made explicit.

KSR Int'l Co. v. Teleflex Inc., 550 U.S. 398, 418 (2007). The Federal Circuit has stated that such reasons must be more than "mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006); *accord Innogenetics, N.V. v. Abbott Labs.*, 512 F.3d 1363, 1374 (Fed. Cir. 2008) (agreeing with the district court's reasoning that "some kind of motivation must be shown from some source, so that the jury can understand why a person of ordinary skill would have thought of either combining two or more references or modifying one to achieve the patented method"). "[W]hether there is a reason to combine prior art references is a question of fact." *Kinetic Concepts, Inc. v. Smith & Nephew, Inc.*, 688 F.3d 1342, 1367 (Fed. Cir. 2012). To that end, we look to the evidence presented by Petitioner to determine if it supports an articulable reason to combine.

In the Petition, Petitioner contends that Matsuzaki and Dworkin both describe cryptographic co-processors that perform Montgomery reduction using similar methods and internal controls. Pet. 31; Ex. 1001 ¶¶ 145–48. Patent Owner characterizes Petitioner's argument as merely pointing out similarities between the references and argues that this is not sufficient to show a reason to combine because it does not explain *why* a skilled artisan would have combined them. PO Resp. 36–37. At the hearing, Petitioner contended that a skilled artisan would have combined the references to "ha[ve] granular control on how computations are performed," Tr. 19:7–8, and "to be able to have this optimal hardware with multiple components," *id.* at 19:15–16. Petitioner also argued that a skilled artisan would have combined the references "in order to create a processor that performs both ECC and RSA efficiently and quickly." Tr. 21:7–10. Petitioner contended that it presented these arguments in its Petition, at page 31, and in Dr. Koç's Declaration, at ¶¶ 145 and 148. *Id.* at 19:17–22; 21:12–16.

In the Petition Petitioner's stated reason to combine Matsuzaki and Dworkin to arrive at claim 1 is limited to:

> Both Matsuzaki and Dworkin address hardware implementations of fast cryptographic co-processors. (Ex. 1001, Koc Decl., ¶ 145.) Matsuzaki and Dworkin also teach Montgomery reduction, similar methods of processing cryptographic data, and internal control methodology. (Ex. 1001, Koc Decl., ¶¶ 146–48.) Therefore, one having ordinary skill in the art would combine the "outputs" (plural) of Dworkin with the disclosure of Matsuzaki.

Pet. 31. Thus, contrary to Petitioner's argument at the hearing, the only reason to combine stated in the Petition itself is the purported similarities between the references.

The reasons to combined given by Dr. Koç in his Declaration (Ex. 1001 ¶¶ 145–148)[1] also are limited to the purported similarities of the references.

In Paragraph 145, Dr. Koç testifies that Matsuzaki and Dworkin both address the same problem, namely "optimal hardware implementation of a cryptographic co-processor with multiple components." Ex. 1001 ¶ 145. According to Dr. Koç, both Matsuzaki and Dworkin describe specific components that could be used in both ECC and RSA encryption.[2] *Id.* The import of this testimony is that Matsuzaki and Dworkin address the same problem using similar technology. Dr. Koç does not explain why a skilled artisan would have incorporated features from Dworkin (i.e., its form of feedback) into Matsuzaki's solution.

In Paragraph 146 of Exhibit 1001, Dr. Koç testifies that both Matsuzaki and Dworkin teach hardware implementations of Montgomery

[1] Petitioner's incorporation of argument from the Koç Declaration is arguably contrary to 37 C.F.R. § 42.6(a)(3) ("Arguments must not be incorporated by reference from one document into another document."). Nevertheless, we exercise our discretion and consider them. In any case, the arguments in the Koç Declaration add very little to the reason stated in the body of the Petition, as explained below.

[2] Patent Owner and Petitioner dispute whether Matsuzaki teaches toward or away from performing RSA encryption. PO Resp. 43–46; Reply 5–6. We do not reach this issue because, even if we assume Matsuzaki teaches performing RSA encryption, Petitioner has not explained why that teaching is evidence of a reason to combine Matsuzaki and Dworkin.

reduction[3] and that "the common disclosure of Montgomery reduction in Matsuzaki and Dworkin would lead one having ordinary skill in the art to consider their teachings together." Here, Dr. Koç testifies that the prior art references have similar hardware implementations, but we are not persuaded that this testimony explains why the references would have been combined.

In Paragraph 147 of Exhibit 1001, Dr. Koç testifies that Matsuzaki and Dworkin teach similar methods of processing cryptographic data. In Paragraph 148, Dr. Koç testifies that Matsuzaki and Dworkin teach similar ways of controlling the computations that are performed by their respective arithmetic units. This testimony also focuses on the similarity of the references, and does not address why the references would have been combined.

In Paragraph 149 of Exhibit 1001, Dr. Koç concludes, "based upon all of these specific similarities, as well as common sense," that a skilled artisan would have combined Matsuzaki and Dworkin. Petitioner reiterates, in its Reply, that it is relying solely on the purported similarities of the references to show a reason to combine: "These similarities would have motivated a PHOSITA to combine 'the 'outputs' (plural) of Dworkin with the disclosure of Matsuzaki.'" Reply 3. Not only is the Petition silent as to "granular control," "optimal hardware," and "efficiency," Petitioner has introduced no factual support for these arguments.

[3] The parties dispute whether Dworkin teaches Montgomery reduction. PO Resp. 47; Reply 5. We do not reach this issue because, even if we assume Dworkin teaches Montgomery reduction, Petitioner has not explained why that evidences a reason to combine Matsuzaki and Dworkin.

To be sure, "the legal determination of obviousness may include recourse to logic, judgment, and common sense, in lieu of expert testimony." *Wyers v. Master Lock Co.*, 616 F.3d 1231, 1239 (Fed. Cir. 2010). We conclude, however, that merely pointing out similarities between Matsuzaki and Dworkin and invoking the words "common sense" (Ex. 1001 ¶ 149) is not a sufficient articulation of a reason to combine. *Cf. Perfect Web Techs., Inc. v. InfoUSA, Inc.*, 587 F.3d 1324, 1330 (Fed. Cir. 2009) ("We reiterate that, on summary judgment, to invoke 'common sense' or any other basis for extrapolating from prior art to a conclusion of obviousness, a district court must articulate its reasoning with sufficient clarity for review."). In any case, the technology at issue here is not "easily understandable"; rather, it is sufficiently complex such that expert testimony is particularly helpful to our resolution of the factual dispute regarding the purported reasons to combine the references. *Wyers*, 616 F.3d at 1240 & n.5 (citing *Centricut, LLC v. Esab Group, Inc.*, 390 F.3d 1361, 1369 (Fed. Cir. 2004)). Thus, the lack of expert testimony supporting a sufficient reason to combine Matsuzaki and Dworkin weighs heavily against Petitioner.

At the hearing, Petitioner further contended that Dr. Koç presented additional reasons to combine in his Reply Declaration. Tr. 25:7–10 (citing Ex. 1029 ¶¶ 6–25). These paragraphs address whether Dworkin describes Montgomery reduction (Ex. 1029 ¶¶ 7–13); present additional arguments regarding the similarity of Matsuzaki and Dworkin (*id.* ¶¶ 14–22); and contend that Matsuzaki teaches RSA encryption (*id.* at 23–25). We see no testimony, however, regarding reasons to combine the references. In sum, Petitioner has introduced no factual support for a reason to combine other than the purported similarity of Matsuzaki and Dworkin.

We now address whether Petitioner's evidence of similarity is sufficient to show a reason to combine. Patent Owner, citing *InTouch Technologies, Inc. v. VGO Communications, Inc.*, 751 F.3d 1327 (Fed. Cir. 2014), argues that evidence of similarity is not sufficient, by itself, to show a reason to combine Matsuzaki and Dworkin. PO Resp. 39–40. The *InTouch* court discounted an expert's testimony that "primarily consisted of conclusory references to her belief that one of ordinary skill in the art *could* combine these references, not that they *would* have been motivated to do so." 751 F.3d at 1352. We agree that Petitioner's evidence suffers from the same deficiency. By arguing that Matsuzaki and Dworkin are similar, Petitioner essentially argues that a skilled artisan could have combined them. But that leaves open the question whether a skilled artisan would have had a reason or motivation to do so.

At the hearing, Petitioner contended that multiple similarities between two references is a sufficient reason to combine, arguing that

> according to *KSR*, . . . a court can look to interrelated teachings of multiple references, the effects of the demands known to the design community or present in the marketplace, and the background knowledge possessed by persons having ordinary skill in the art, all to determine whether there is a reason to combine the references.

Tr. 20:11–18. Here, Petitioner paraphrases the quote from *KSR* reproduced above. Importantly, that quote continues: "To facilitate review, this analysis should be made explicit." *KSR*, 550 U.S. at 418. Petitioner does not explain, or present evidence to show, how the purported interrelated teachings of Matsuzaki and Dworkin, along with any demand and background knowledge, would have led a skilled artisan to combine

Matsuzaki and Dworkin. Although evidence of interrelated teachings is one factor to consider, *KSR* identifies many other factors that can be considered "*all* in order to determine" whether there is a reason to combine the references—hence, evidence bearing on one factor alone may be insufficient to carry Petitioner's evidentiary burden. Here, Petitioner has failed to present explicitly a cogent reason why the similarities of the references alone evidence sufficient reason to combine.

As Patent Owner argues, *KSR* provides several possible reasons why a skilled artisan might combine references, including combining known elements to yield predictable results, simply substituting one element for another element that is known to be interchangeable, and using a known technique from one field to improve devices in another field in a predictable way. PO Resp. 32 (citing *KSR*, 550 U.S. at 415–18). Petitioner does not introduce evidence that a combination of Matsuzaki would have been predictable. Nor does Petitioner contend that Dworkin's technique would have been a simple substitution for Matsuzaki's. Rather, Petitioner argued, when pressed at the hearing for a more precise statement of how the references would have been combined, that a skilled artisan "would take the multiple feedbacks of the outputs of the computational units of Dworkin and add those to the returning back of the carry-up signal of the Matsuzaki reference." Tr. 17:21–18:2. Petitioner, however, offers no evidence that Dworkin's feedback is advantageous or that adding this feedback to Matsuzaki would have improved Matsuzaki in a similar or predictable way. Such evidence is not implied merely by the similarity of the references.

After the hearing, Petitioner brought to our attention *Tyco Healthcare Group LP v. Ethicon Endo-Surgery, Inc.*, 774 F.3d 968 (Fed. Cir. 2014).

Ex. 1042, 9:15–10:9. *Tyco* does not support Petitioner's arguments. In *Tyco*, the Federal Circuit concluded that it would have been obvious to substitute a curved blade feature of a surgical device disclosed in a first prior art reference for the straight blade disclosed in a second reference in order to employ the benefits disclosed in the first reference. 774 F.3d at 977–78. Addressing another set of claims, the *Tyco* court concluded that it would have been obvious to substitute a dual cam structure disclosed in a first prior art reference for a single cam structure disclosed in another, even though the two references were from different fields of endeavor, because the first reference explicitly disclosed that a wide variety of surgical devices could benefit from the feature. 774 F.3d at 978–79. In both instances, the Federal Circuit relied on explicit disclosure in the art of the benefits of the feature to be added and applied the principle articulated in *KSR* that "if a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill." *KSR*, 550 U.S. at 417. As explained above, Petitioner has not introduced evidence sufficient to show that Dworkin's feedback technique provides an improvement that would be similarly applicable to the system disclosed in Matsuzaki.

In sum, we have evaluated the evidence introduced by Petitioner, including the Koç Declaration and the Koç Reply Declaration, and find that Petitioner has not shown sufficiently a reason, with rational underpinning, to combine Matsuzaki and Dworkin. Evidence that Matsuzaki and Dworkin have similarities and argument that the combination is mere "common sense" are not enough. Accordingly, we conclude that Petitioner has not met

its burden of showing, by a preponderance of the evidence, that any of claims 1–11 would have been obvious over Matsuzaki and Dworkin.

III. CONCLUSION

For the reasons given, we are not persuaded that Petitioner has shown by a preponderance of the evidence that claims 1–11 of the '666 patent are unpatentable based on the challenges on which trial was instituted.

IV. ORDER

For the reasons given, it is

ORDERED that claims 1–11 of U.S. Patent No. 7,634,666 B2 have not been shown by a preponderance of the evidence to be unpatentable;

FURTHER ORDERED that Petitioner's Motion to Exclude is denied;

FURTHER ORDERED that Patent Owner's Motion to Exclude is denied; and

FURTHER ORDERED that, because this is a Final Written Decision, parties to the proceeding seeking judicial review of the decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

PETITIONER:
Kenneth R. Adamo
Eugene Goryunov
KIRKLAND & ELLIS LLP
kenneth.adamo@kirkland.com
eugene.goryunov@kirkland.com

PATENT OWNER:

Herbert D. Hart III
Jonathan R. Sick
Peter J. McAndrews
MCANDREWS, HELD & MALLOY, LTD.
hhart@mcandrews-ip.com
jsick@mcandrews-ip.com
pmcandrews@mcandrews-ip.com