

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.



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 |

We instituted trial on the following bases. Dec. 23–24.

| Reference(s)         | Basis    | Claim(s) Challenged       |
|----------------------|----------|---------------------------|
| Sprunk               | § 102(b) | 4, 5, 7, 17–20, and 23–25 |
| Sprunk               | § 103(a) | 21 and 26                 |
| Sprunk and Matsumura | § 103(a) | 1–3 and 12–14             |
| Sprunk and Griffin   | § 103(a) | 22                        |

#### *D. Real Parties in Interest and Related Proceedings*

The parties identify only themselves as real parties in interest. Pet. 2; Paper 5, 1. The parties identify *Gemalto S.A. v. CPI Card Group Inc.*, Civil Action No. 1:15-cv-02776 (D. Colo.) (“the related litigation”) as involving the ’833 patent. Pet. 2; Paper 5, 1.

## II. ANALYSIS

### *A. Claim Construction*

The parties agree that the ’833 patent expired on March 7, 2017. Pet. 4; Paper 6, 2. Accordingly, we accord claim terms their ordinary and customary meaning, as would be understood by a person of ordinary skill in the art at the time of the invention. *See Cisco Sys., Inc. v. AIP Acquisition, LLC*, Case IPR2014-00247, slip op. at 2 (PTAB July 10, 2014) (Paper 20) (citing *Phillips v. AWH Corp.*, 415 F.3d 1303, 1313–1317 (Fed. Cir. 2005) (en banc)). In doing so, “we look principally to the intrinsic evidence of record, examining the claim language itself, the written description, and the prosecution history, if in evidence.” *DePuy Spine, Inc. v. Medtronic*

*Sofamor Danek, Inc.*, 469 F.3d 1005, 1014 (Fed. Cir. 2006) (citing *Phillips*, 415 F.3d at 1312–17).<sup>1</sup>

In the Institution Decision, we adopted preliminary constructions for several phrases recited in the form “means for . . .,” construing those phrases in accordance with 35 U.S.C. § 112, ¶ 6, as “cover[ing] the corresponding structure, material, or acts described in the specification and equivalents thereof.” Dec. 6 (citing *Williamson v. Citrix Online, LLC*, 792

---

<sup>1</sup> We disagree with Patent Owner’s suggestion during the oral hearing that application of a district-court-type claim construction during post grant proceedings before the Board “introduces the concept of preserving the validity of the claims.” See Tr. 68:16–22. While a presumption of validity is applied by district courts in accordance with 35 U.S.C. § 282, any implication that § 282 must also be applied in proceedings before the Office “miscontrues the purposes for which that statute [was] enacted.” *In re Etter*, 756 F.2d 852, 856 (Fed. Cir. 1985) (en banc). “A statute setting rules of procedure and assigning burdens to litigants in a court trial does not automatically become applicable to proceedings before the PTO.” *Id.*

Although *Etter* considered application of a presumption of validity in the context of reexamination proceedings, its reasoning equally applies to *inter partes* review proceedings in light of the Supreme Court’s explicit recognition that “the purpose of [an *inter partes* review] proceeding is not quite the same as the purpose of district court litigation.” *Cuozzo Speed Techs., LLC v. Lee*, 136 S.Ct. 2131, 2144 (2016). “Although Congress changed the name from ‘reexamination’ to ‘review,’ nothing convinces us that, in doing so, Congress wanted to change its basic purposes, namely, to reexamine an earlier agency decision.” *Id.* In *Cuozzo*, the Supreme Court explicitly endorsed the Office’s use of the broadest-reasonable-interpretation standard for unexpired patents by analogy with reexamination proceedings; it logically follows by the same analogy that the Office’s use, in reexamination proceedings, of a claim construction standard similar to that used by district courts, but without a presumption of validity, applies to *inter partes* review proceedings.

F.3d 1339, 1348 (Fed. Cir. 2015)).<sup>2</sup> Of those preliminary constructions, Patent Owner disputes only the “means for decorrelating,” recited in each of independent claims 1, 2, and 4. See PO Resp. 3–6. Based on the complete record developed during the trial, we see no compelling reason to alter our constructions of the other “means for . . .” limitations, summarized in the table below by identifying the recited function and the corresponding structure described in the Specification of the ’833 patent. Accordingly, we adopt them for this Final Written Decision. See Dec. 10–13.

| Claim Limitation                                                                                                  | Function                                                                                                | Structure                                                               |
|-------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|
| “means for generating one of a timing signal, and a sequence of clock pulses which is dispatched at random times” | generation of one of (1) a timing signal, and (2) a sequence of clock pulses dispatched at random times | an internal clock, a random number generator, and a calibration circuit |
| “means for randomly generating interrupts” <sup>3</sup>                                                           | randomly generating interrupts                                                                          | a random number generator, a register, and a logic circuit              |
| “means for triggering the execution of a secondary program”                                                       | triggering the execution of a secondary sequence                                                        | a main program and a secondary program                                  |
| “means for execution of a secondary program”                                                                      | execution of a secondary program                                                                        | a main program                                                          |
| “means for phase shifting the timing, synchronization or status signals of the processor”                         | shifting the timing, synchronization, or status signals of a processor                                  | shift registers and a multiplexer                                       |

---

<sup>2</sup> Section 112, paragraph 6, was recodified by the America Invents Act as Section 112(f).

<sup>3</sup> Although not recited as a means-plus-function limitation, we construe the related phrase of a “random interrupt generating system” as including similar components. Dec. 11.

*“means for decorrelating”*

Each of independent claims 1, 2, and 4 recites “means for decorrelating an execution of the at least one instruction sequence of the [main] program from the internal or external electrical 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,” including or omitting the word “main” in accordance with an antecedent in the respective claims.

The “so that the execution . . .” recitations were added by amendment during prosecution after rejections under 35 U.S.C. § 112, ¶¶ 1 and 2, in which the Examiner determined that “[t]he process or act of ‘decorrelating’ is not sufficiently described to determine what this is and how it is accomplished.” Ex. 1002, 206–07, 217–30. With the amendments, the applicant explained that “[s]imply stated, decorrelation is the opposite of correlation, i.e., in the context of this application, the opposite of an operation which is correlated to a sequencing clock.” *Id.* at 223. Petitioner’s expert, Nathaniel Polish, Ph.D., opines that “[w]ith this amendment, the patent applicant is clarifying that decorrelation requires the desynchronization of ‘the execution of the at least one instruction sequence’ with ‘respect to the internal or external electrical signals.’” Ex. 1003 ¶ 45.

Petitioner relies on the express language of the claims, the prosecution history, and this testimony of its expert to contend that a person of ordinary skill in the art “would have understood the claimed function is desynchronizing the execution of instructions by the microprocessor with respect to internal or external electrical signals.[.]” Pet. 6 (citing Ex. 1003 § 45).

In addressing the structural aspect of the construction, Petitioner observes that the Specification includes a “recitation that ‘the decorrelation means comprise one or more circuits generating a sequence of clock or timing pulses which are dispatched at random times.’” Pet. 6–7 (quoting Ex. 1001, col. 2, ll. 18–21; citing Ex. 1003 ¶ 47).<sup>4</sup> Figure 1 of the ’833 patent, reproduced above, illustrates that random clock CLK2 desynchronizes execution of instructions in microprocessor 1 from external clock CLKE, and that CLK2 is generated with internal clock 11, random number generator 2, and calibration circuit 9. See Ex. 1001, col. 2, ll. 18–21, col. 3, ll. 59–61, col. 4, ll. 23–28. Figures 3A and 3B of the ’833 patent are reproduced below.

---

<sup>4</sup> In the body, we consider what Petitioner characterizes as the “first” of “a few structures” that Petitioner contends the Specification “links” to the “means for decorrelating.” Pet. 6. Petitioner additionally provides analysis for “second” and “third” structures that it describes as similarly “linked,” but argues that each of those structures “should not be construed as corresponding to the [claimed] means for decorrelating.” *Id.* at 11, 14.

In its Response, Patent Owner does not contest Petitioner’s positions with respect to the “second” and “third” structures, instead presenting a further distinct position that relies on a different formulation of the *function* performed by the “means for decorrelating.” See PO Resp. 4–6; see *infra*. Accordingly, we limit ourselves to considering Petitioner’s “first” position and to considering the position presented by Patent Owner in its Response. See *Vivid Techs., Inc. v. Am. Sci. & Eng’g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999) (stating that only those terms in controversy need to be construed, and only to the extent necessary to resolve the controversy).

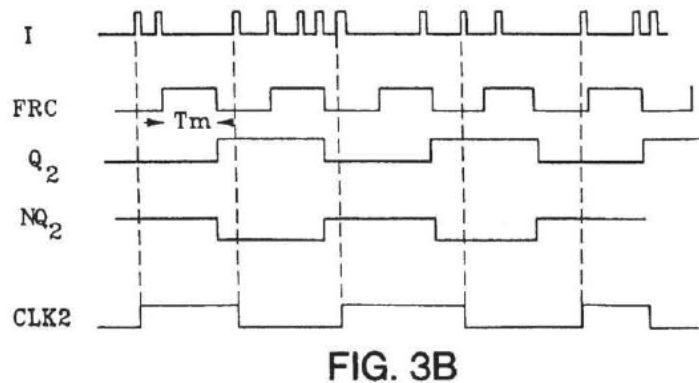
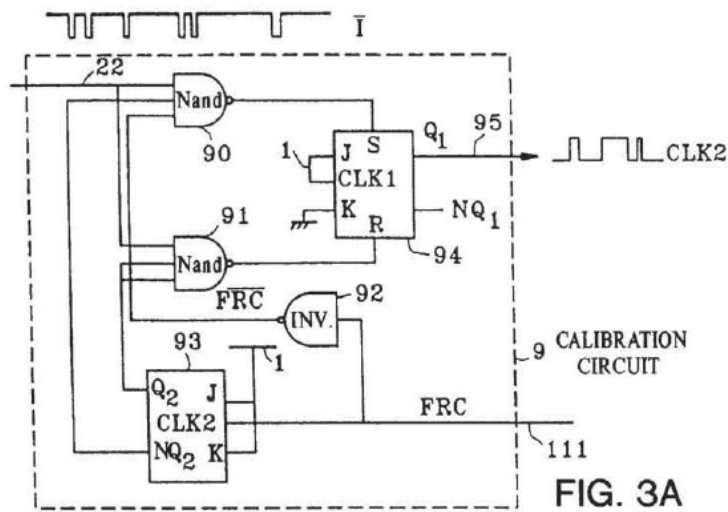


Figure 3A (top) is a block diagram of calibration circuit 9, and Figure 3B (bottom) represents logical sequencing diagrams of calibration circuit 9. *Id.* at col. 3, ll. 28–31. Calibration circuit 9 receives output FRC of internal clock 11 on line 111, and NAND gates 90, 91, JK flip flops 93, 94, and inverter 92 modulate internal clock FRC with output I on line 22 of random number generator 2 to generate CLK2 for driving microprocessor 1. *Id.* at col. 8, ll. 50–62.

In light of these disclosures, and consistent with the Institution Decision, we identify a structure corresponding to the “means for decorrelating” as an internal clock, a random number generator, and a calibration circuit. Dec. 9.

Patent Owner disputes the identified function for the “means for decorrelating,” and instead quotes the Specification in contending that the function should be:

[To enable] the microprocessor running the main program to go from an operation that is perfectly in phase and correlated to the external sequencing clock, to a decorrelated operation in which, as desired and depending on the embodiment chosen, the execution time of a given instruction will no longer be identical, even when the same instruction is executed several times, or in which the execution duration of an instruction sequence will be variable even if the same sequence is re-executed several times by the main program, or even in which the execution duration of an instruction will be variable, the execution time of the same instruction itself being variable.

PO Resp. 5 (quoting Ex. 1001, col. 4, ll. 12–23; citing Ex. 2001 ¶¶ 59–62; Ex. 2005). Patent Owner contends that this function is supported by the prosecution history, quoting the following excerpt (which was also partially quoted by Petitioner as support for its identification of the appropriate function):

Simply stated, decorrelation is the opposite of correlation, *i.e.*, in the context of this application, the opposite of an operation which is correlated to a sequencing clock. The Examiner’s attention is invited to . . . page 3, lines 1-4, . . . “the decorrelation means comprise a random number generator which makes it possible to desynchronize the execution of the program sequence in the processor.” This is further described at page 6, lines 6-18, indicating a certain number of elements added a microprocessor and a random number generator, which will allow the microprocessor running the main program to go from an operation that is perfectly in phase and correlated to the external sequencing clock to a decorrelated operation in which, as desired and depending on the embodiment chosen, the execution time of a given instruction no longer is identical, even when the same instruction is executed several times, or in which the execution

duration of an instruction sequence is variable even if the same sequence is re-executed several times by the main program or in which the execution duration of an instruction is variable.

PO Resp. 5–6 (quoting Ex. 1002, 223–24) (alterations by Patent Owner).

Patent Owner’s proposed construction is deficient because it fails to identify corresponding structure described in the Specification for performing the proposed function. *See Williamson* at 1351 (“Construing a means-plus-function claim term is a two-step process. The court *must* first identify the claimed function. . . . Then, the court *must* determine what structure, if any, disclosed in the specification corresponds to the claimed function.”) (citation omitted, emphases added).<sup>5</sup> In addition, the function proposed by Patent Owner as performed by the “means for decorrelating” includes multiple functional variations that are not recited in the claim itself. Although the Specification and prosecution history serve important roles in claim construction, the Federal Circuit has repeatedly warned against importing limitations from the specification into the claims. *Phillips* at 1323. Patent Owner’s proposed function for the “means for decorrelating” improperly attempts to import such limitations.

---

<sup>5</sup> When questioned at the oral hearing about this omission, Patent Owner referred to the structure identified in the Institution Decision as part of our preliminary construction, i.e. an internal clock, a random number generator, and a calibration circuit. Tr. 48:21–50:22. But that structure was identified for a different function than the one proposed by Patent Owner in its Response, which includes insufficient explanation how those components are disclosed by the ’833 patent to perform all the functional variations within Patent Owner’s proposal.

Furthermore, although we recognize that both parties provide expert testimony in support of their respective identifications of the function (Ex. 1003 ¶ 45; Ex. 2001 ¶ 59), the Federal Circuit has also warned that “extrinsic evidence in general [is] less reliable than the patent and its prosecution history in determining how to read claim terms.” *Phillips* at 1318. Expert testimony, in particular, “can suffer from bias that is not present in intrinsic evidence.” *Id.* Thus, although we have considered the testimony of both experts, we accord it less weight than the intrinsic evidence in arriving at our construction of the “means for decorrelating.”<sup>6</sup>

Consistent with the preliminary construction applied in the Institution Decision, we construe “means for decorrelating” for this Final Written Decision as having the function of desynchronizing the execution of instructions by the microprocessor with respect to internal or external signals, with corresponding structure of an internal clock, a random number generator, and a calibration circuit.

---

<sup>6</sup> Petitioner contends that we should “discount” the testimony of Patent Owner’s expert, Çetin Kaya Koç, Ph.D., “in its entirety.” Reply 2. Dr. Koç testifies that the opinions in his Declaration “take into consideration the Board’s construction as well as the more specific meaning found in the ’833 Patent,” Ex. 2001 ¶ 62, but, according to Petitioner, “a review of Dr. Koc’s declaration reveals that on the few times he actually applied a construction of the function for the means for decorrelating, he applied [Patent Owner’s] proposed construction, not the Board’s.” Reply 2. Although the specific manner in which Dr. Koç applies a claim construction may legitimately affect the weight accorded to his testimony on specific issues, Petitioner has not filed a motion to exclude Dr. Koç’s Declaration, and the Reply articulates insufficient basis for wholesale rejection of the entirety of Dr. Koç’s opinions.

*B. Level of Skill in the Art*

Supported by their respective experts, the parties make similar contentions regarding the educational background of a person of ordinary skill in the art, but disagree with respect to the industry experience of such an individual. Pet. 22 (citing Ex. 1003 ¶ 20); PO Resp. 3 (citing Ex. 2001 ¶ 31). Petitioner contends that, at the time of filing the application that matured into the '833 patent, a person of ordinary skill in the art would have had at least bachelor's degree in "computer science, electrical or computer engineering, or a related field of study," while Patent Owner contends that such a person would have had a bachelor's degree in "computer science or computer engineering." Pet. 22; PO Resp. 3. As far as industry experience, Petitioner contends that a person of ordinary skill in the art would have had "four or more years of industry experience relating to secure integrated circuits." Pet. 22. Patent Owner contends that such extensive experience "is unnecessary" and proposes that a person of skill in the art would have had "sufficient industry experience to have had a working knowledge of computer architecture, *i.e.*, approximately 1 year of experience in computer architecture design." PO Resp. 3.

The record provides relatively little basis to discriminate between the parties' proposals, although we agree with Patent Owner that the level of industry experience proposed by Petitioner seems unjustifiably high. Nevertheless, the conclusions we set forth herein do not turn on the distinctions between the levels of skill in the art proposed by the parties. We adopt a level of skill that includes at least a bachelor's degree in computer science, electrical or computer engineering, or a related field of study, and at least two years of industry experience in computer architecture.

### C. Sprunk

Sprunk “enhances the security of a secure microprocessor by rendering it extremely difficult, if not impossible, to observe a clock signal and predict the occurrence of subsequent clock pulses therefrom.” Ex. 1004, col. 3, ll. 35–39. This is accomplished “by modulating the signal which clocks the processor on a pseudorandom basis to render the time at which each successive clock pulse occurs completely unpredictable.” *Id.* at col. 3, ll. 42–46. As Sprunk explains, such clock-signal modulation “is designed to resist analysis attempts of a pirate.” *Id.* at col. 7, ll. 25–29.

Figure 1 of Sprunk, reproduced below, illustrates.

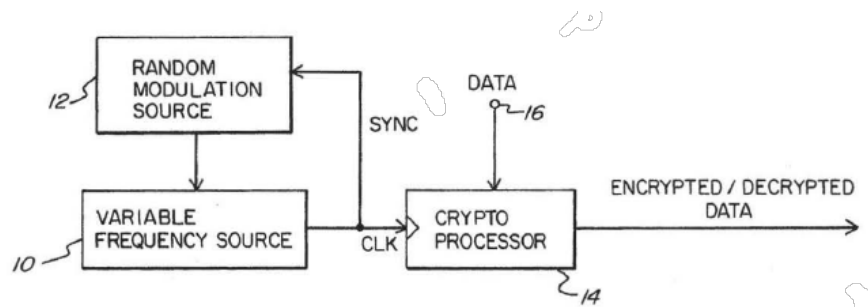
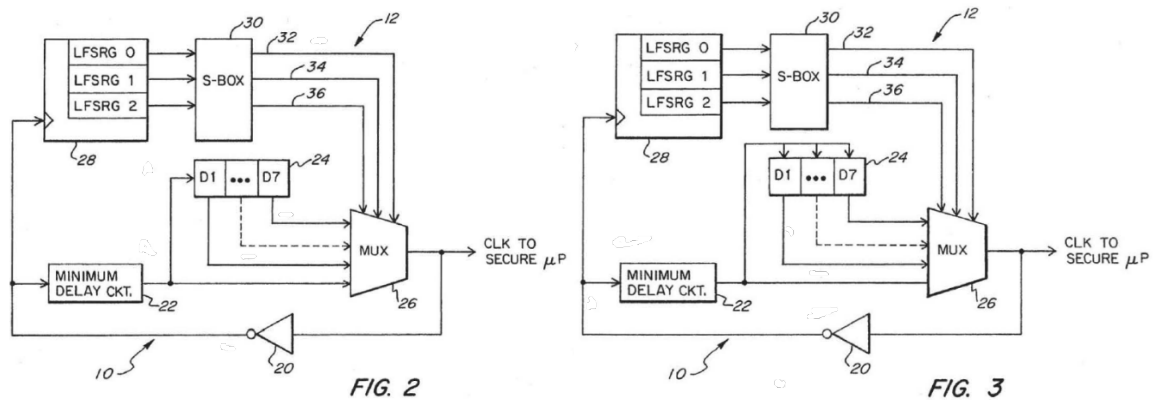


FIG. 1

Figure 1 is a block diagram of a cryptographic processor that is “clocked by a random and unpredictable clock signal.” *Id.* at col. 3, ll. 11–13.

Unpredictable pulse stream CLK is output from variable frequency source 10, variably tuned or selected using substantially random modulation circuit 12, and used to clock crypto processor 14 for encryption or decryption of data entered via terminal 16. *Id.* at col. 4, ll. 5–13.

Details of substantially random modulation circuit 12 are illustrated in Figures 2 and 3 of Sprunk, reproduced below.



In similar illustrations, Figure 2 (left) and Figure 3 (right) show substantially random modulation circuit 12 as comprising a series of delay stages 24, multiplexer 26, a plurality of linear feedback shift register generators (“LFSRGs”) 28 and, optionally, substitution box (“S-Box”) 30. *Id.* at col. 4, ll. 36–40. LFSRGs 28 and S-Box 30 provide control signals that multiplexer 26 uses to select one of the delays provided by delay stages 24 for each clock pulse. *Id.* at col. 4, ll. 40–43. A detailed understanding of the various specific ways that Sprunk performs the delay selection is unnecessary for our analysis; it is sufficient to observe that Sprunk teaches that such delay selection results in providing a clock signal “modulated to provide a substantially random . . . and unpredictable series of clock pulses for clocking a secure microprocessor.” *Id.* at col. 7, ll. 25–28.

### 1. Anticipation of Independent Claim 4

Petitioner challenges independent claim 4 as anticipated under 35 U.S.C. § 102(b) by Sprunk. Pet. 26–28. “To be anticipatory, a reference must describe, either expressly or inherently, each and every claim limitation and enable one of skill in the art to practice an embodiment of the claimed invention without under experimentation.” *Am. Calcar, Inc. v. Am. Honda*

*Motor Co., Inc.*, 651 F.3d 1318, 1341 (Fed. Cir. 2012) (citing *In re Gleave*, 560 F.3d 1331, 1334 (Fed. Cir. 2009))

Petitioner presents an analysis in which it parses the claim as reciting an “improved integrated circuit” that comprises two components: “a microprocessor having a main program” and “means for decorrelating,” each of which is further defined by the claim. Pet. 26–28. We agree that this is the natural reading of the claim and address Patent Owner’s different parsing of the claim below. *See infra*, Section II.C.1.b.

Petitioner addresses the first component by observing that Sprunk’s microprocessor executes instructions of an algorithm in synchronization with a clock signal, thereby disclosing “a microprocessor having a main program arranged to execute at least one instruction sequence . . . in synchronization with internal or external signals of the integrated circuit.” Pet. 26 (citing Ex. 1004, col. 2, ll. 11–13).

Petitioner addresses the second component by pointing to the illustration in Figure 1 of Sprunk, in which “Sprunk desynchronizes the execution of instructions by the microprocessor 14 from internal clock 10 by modulating the output of the clock 10 with a random function to provide the microprocessor 14 with a random clock signal.” *Id.* at 27 (citing Ex. 1004, col. 2, ll. 7–13, col. 1, ll. 50–54). Noting that the random modulation of internal clock 10 is performed with a random number generator in the form of LFSRGs, Petitioner identifies the desynchronization function as performed by an internal clock (clock 10), a random number generator (LFSRG 0 – LFSRG 2), and a calibration circuit (circuit 12). *Id.* at 28. This analysis is consistent with our construction of “means for decorrelating”

because it identifies both the function and structure that define that construction.

Based on these identifications, Petitioner demonstrates, by a preponderance of the evidence that claim 4 is anticipated by Sprunk.

Patent Owner draws two distinctions in response, neither of which is persuasive. First, Patent Owner contends that Sprunk's invention is embodied on two separate chips ("two-chip theory"). PO Resp. 6, 7, 11–16, 18, 20, 21, 25, 31, 32, 34, 42, 55. Second, Patent Owner contends that Sprunk's operation is not controlled by a "main program" ("main-program control theory"). *Id.* at 16–18, 20, 29, 33, 34, 50, 55. We address each of these purported distinctions in turn below.

#### *a. Two-Chip Theory*

In presenting its two-chip theory, Patent Owner effectively gives weight to the preamble ("An improved integrated circuit") by arguing that "Sprunk does not teach 'an improved integrated circuit' with a decorrelation means as required by these claims, but instead teaches conventional separate [integrated circuits], which are fundamentally different." PO Resp. 10; *see* Tr. 39:15–23 (Patent Owner asserting at oral hearing that "'improved' needs to be taken into consideration"). Patent Owner specifically contends that "the 'means for decorrelating' must be in the same [integrated circuit] in which the execution of at least one of the program's instruction sequences is decorrelated from the electrical signals of the [integrated circuit]." PO Resp. 10. Patent Owner further contends that this "single [integrated circuit] requirement is confirmed by the specification [of the '833 patent], which repeatedly refers to the microprocessor or microcomputer type as being

‘monolithic,’ *i.e.*, a single [integrated circuit].” *Id.* at 11 (citing Ex. 1001, col. 3, ll. 52–58, col. 10, ll. 40–44, col. 7, l. 40, col. 10, ll. 41, 45, 49, 52, 55, 58, 60).

“Generally, . . . the preamble does not limit the claims.” *DeGeorge v. Bernier*, 768 F.2d 1318, 1322 n.3 (Fed. Cir. 1985). But we need not decide whether the preamble is limiting in this instance because, as Petitioner contends, Sprunk “expressly describes that its invention can be embodied on a single chip.” Reply 3. In addressing the preamble, under the assumption that “it is limiting,” the Petition observes that Sprunk discloses that the embodiment of Figure 2 “can be implemented in very large scale integration (VLSI) using a minimum area for the modulator.” Pet. 26 (citing Ex. 1001, col. 5, ll. 40–42; Ex. 1003 ¶ 94). Petitioner’s expert, Dr. Polish, testifies that a person of ordinary skill in the art would have understood such very large scale integration, using a minimum area for the modulator, “to be an integrated circuit.” Ex. 1003 ¶ 94.

Patent Owner, supported by testimony of its expert, Dr. Koç, disputes that interpretation, arguing that “Sprunk describes the crypto processor in Fig. 1 as a ‘conventional’ crypto processor,’ *i.e.*, a separate integrated circuit, encapsulated in a package, which cannot be opened without destroying the crypto processor.” PO Resp. 13 (citing Ex. 1004, col. 4, ll. 9–13; Ex. 2001 ¶ 79) (emphasis by Patent Owner). Dr. Koç equates use of the word “conventional” to description of “a standard ‘off-the-shelf’ component,” asserting that “[w]hen it comes to these types of conventional processors, because they are purchased from the manufacturer already fully designed, one can add additional circuitry around the packaged processor, but one cannot make changes inside the packaged processor.” Ex. 2001 ¶ 79.

Sprunk's use of the word "conventional" in describing the cryptoprocessor ("in a single instance, out of more than forty references to its processor," Reply 3) cannot bear the weight that Patent Owner and its expert wish to place upon it. We agree with Petitioner that the more compelling understanding of this isolated reference "indicate[s] that the processor portion of [Sprunk's] invention was a prior art design and no changes were required to the design of the processor itself." Reply 3–4 (citing Ex. 1011 ¶ 8). That understanding is supported by Dr. Polish's testimony that "[o]ne skilled in the art would not interpret the use of 'conventional' in association with Sprunk's cryptoprocessor to mean it was a separately packaged and encapsulated chip." Ex. 1011 ¶ 8. Furthermore, Dr. Koç acknowledged during cross-examination that Sprunk does not "say his processor is encapsulated in its own package anyplace other than the words 'conventional crypto processor'"; does not "say his packaging incorporating his processor cannot be opened without destroying the processor"; does not "say that he buys his cryptoprocessor"; and does not "say that his processor is off the shelf." Ex. 1010, 52:7–53:2.

We are also not persuaded by Patent Owner's argument that a portion of Sprunk (i.e., Ex. 1004, col. 6, ll. 61–66) refers to analog circuits: "The circuits described in this excerpt are special analog circuits, and they cannot be placed in the same monolithic digital chip." PO Resp. 14 (citing Ex. 2001 ¶ 80). Even if Sprunk discloses some embodiments that may be implemented with separate chips by using analog circuits that does not impugn the relevance of Sprunk's disclosure identified by Petitioner, i.e., VLSI and digital circuits, to support Petitioner's anticipation analysis. A prior-art reference's disclosure of a nonanticipatory embodiment does not

negate the invalidating effect under 35 U.S.C. § 102 of any other anticipatory alternative embodiments. *Celeritas Techs., Ltd. v. Rockwell Intern. Corp.*, 150 F.3d 1354, 1361 (Fed. Cir. 1998); *Upsher-Smith Labs., Inc. v. PamLab, L.L.C.*, 412 F.3d 1319, 1322–23 (Fed. Cir. 2005).

The portion of Sprunk cited by Patent Owner remarks that its frequency source “can” comprise an analog circuit—not that it is required—and Petitioner correctly counters that “Sprunk expressly and repeatedly describes that his frequency sources 10 and 50 can be implemented as digital as well as analog circuits.” Ex. 1004, col. 6, l. 62; Reply 6–7 (citing Ex. 1004, col. 4, ll. 1–5 (“Frequency source 10 can comprise an analog or digital circuit”), col. 7, ll. 2–3 (“In a digital implementation, any type of ring oscillator can be used for single frequency source 50.”)). Furthermore, Dr. Koç acknowledged on cross-examination that the digital frequency sources described in Sprunk would not inhibit placing them in the same chip as the processor. Ex. 1010, 278:16–23.

For these reasons, we agree with Petitioner, and find, that Sprunk discloses that its relevant structure can be embodied on a single chip, contrary to Patent Owner’s two-chip theory. In light of this finding, we are not persuaded by Patent Owner’s argument that Sprunk lacks an internal clock, which forms part of the structural aspect of our construction of “means for decorrelating.” See PO Resp. 18 (“There is no internal clock of the crypto processor mentioned in the Sprunk patent; therefore, there is only one clock, which is the one produced outside the chip and applied to it.”). Patent Owner provides insufficient reasoning to support its position that the claims require two clocks, *see id.* at 19, and Sprunk’s variable frequency

source 10 is a clock internal to the VLSI chip identified by Petitioner.  
Pet. 26–28.

*b. Main-Program Control Theory*

Patent Owner’s main-program control theory is grounded in a different parsing of the language of independent claim 4 than the one applied by Petitioner—and different than the one we find above to be the natural reading of the claim language. In its Response, Patent Owner omits words from the claim in asserting that independent claim 4 (and claims that depend therefrom) “also require[s] the [integrated circuit] include ‘a main program arranged . . . in synchronization with . . . electrical signals . . . and means for decorrelating . . . of the main program.’” PO Resp. 16 (quoting Ex. 1001, col. 11, ll. 49–53) (alterations by Patent Owner). With this parsing, Patent Owner asserts that, “[i]n other words, the ‘main program’ must have control over the means for decorrelating’ in the [integrated circuit].” *Id.*

At the oral hearing, we questioned Patent Owner about its parsing of the claim language to support its contention that the claim requires such “main program control.” Tr. 42:6–45:10. Patent Owner further explained that “the language ‘arranged to execute’ would also modify the means for decorrelating.” *Id.* at 45:3–4. That is, rather than read the claim in straightforward fashion as reciting a microprocessor having “a main program” and a “means for decorrelating,” each further defined by the claim, Patent Owner relies on the language “arranged to execute” to infer a further link between the “main program” and the “means for decorrelating.” Essentially, Patent Owner does not read the “means for decorrelating” as a distinct element of the “microprocessor,” but instead reads the “main

program” merely as “arranged to execute” such a “means for decorrelating,” as well as “arranged to execute” “at least one instruction sequence in the microprocessor.”

We find such a contorted reading of the claim language unnatural and inconsistent with the plain language of the claim. Patent Owner’s reading suffers from an evident deficiency in that the position it takes with respect to its “main-program control theory” is inconsistent with its position with respect to its “two-chip theory.” That is, for purposes of its two-chip theory argument, Patent Owner construes the claim such that the “means for decorrelating” is a distinct component of the recited “microprocessor,” but advocates for a construction without that requirement to support its main-program control theory.

Patent Owner also relies on the written description of the ’833 patent to support its main-program control theory, citing portions of the Specification consistent with its reading of the claim. PO Resp. 16 (quoting Ex. 1001, col. 4, ll. 60–63 (“it is the main program which will choose whether the clock for sequencing the microprocessor will be the external clock CLKE or a decorrelation clock CLK2”), col. 7, ll. 22–26 (“the microprocessor, controlled by a program it will execute, will be able to use this program to activate the means for decorrelating the instruction execution sequencing of this program by loading, for example, registers R2 or 8, or by calling secondary programs”)). In addition, Patent Owner relies on the testimony of its expert, Dr. Koç, who quotes the same language. Ex. 2001 ¶ 82.

Although we have considered these disclosures, as well as the testimony of Dr. Koç, we agree with Petitioner that Patent Owner “is

improperly reading any ‘main program control’ limitations from the specification into the claims to avoid the prior art.” Reply 8. “[T]he claim construction inquiry . . . begins and ends in all cases with the actual words of the claim.” *Renishaw PLC v. Marposs Società per Azioni*, 158 F.3d 1243, 1248 (Fed. Cir. 1998) (citations omitted). Although claims must be read in view of the specification, of which they are a part, the Federal Circuit has repeatedly warned that “it is important not to import into a claim limitations that are not a part of the claim.” *Superguide Corp. v. DirecTV Enter., Inc.*, 358 F.3d 870, 875 (Fed. Cir. 2004). Furthermore, the Federal Circuit has cautioned that “we must disregard the testimony of an expert that is . . . ‘based on an incorrect understanding of the claim[s].’” *Homeland Housewares, LLC v. Whirlpool Corp.*, 865 F.3d 1372, 1378 (quoting *Cordis Corp. v. Boston Sci. Corp.*, 658 F.3d 1347, 1357 (Fed. Cir. 2011)). That is the situation here, where Dr. Koç relies on the same strained reading of the claim language to support his opinion.

Accordingly, Patent Owner’s arguments that Sprunk lacks main-program control, including its argument that data output shown in Figure 1 of Sprunk “is not a *control* output,” are not persuasive because they are not commensurate with the scope of the claim. See PO Resp. 16–18.

For these reasons, we conclude that Petitioner demonstrates, by a preponderance of the evidence, that independent claim 4 is anticipated by Sprunk.

*2. Anticipation of Dependent Claims 5, 7, 17–20, and 23–25 by Sprunk*

Petitioner challenges dependent claims 5, 7, 17–20, and 23–25 as anticipated under 35 U.S.C. § 102(b) by Sprunk. Pet. 28–38. Each of these claims depends directly or indirectly from claim 4.

*a. Claim 5*

Claim 5 recites that “the decorrelation means comprises at least one circuit for generating a sequence of timing pulses which are dispatched at random times to the microprocessor by generation of a random number.” Ex. 1001, col. 11, ll. 59–62. In addressing this limitation, Petitioner observes that “Sprunk in Figure 1 discloses a circuit including a modulator 12 that randomly modulates a clock source 10 to provide a random stream of clock pulses CLK to microprocessor 14.” Pet. 29. Petitioner specifically identifies circuit elements 28 and 30 in modulator 12, as shown in Figures 2 and 3 of Sprunk, as “produc[ing] a random number for generating the random timing pulses.” *Id.* In addition, Petitioner notes that Figures 4, 5, 6, and 7 of Sprunk also illustrate embodiments in which “random control signals (respectively elements 44, 52, 64, and 74) are used in the generation of random clock pulses CLK.” *Id.* With these identifications, Petitioner makes a sufficient showing because each of these embodiments discloses circuits that use a random number to generate a sequence of random timing pulses to the microprocessor. *See id.*

We are not persuaded by Patent Owner’s response, which emphasizes that the claim recites timing pulses “dispatched” at random times, arguing that “[f]or sequences of timing pulses to be dispatched, there must be main program control.” PO Resp. 19–20. Patent Owner does not proffer a

construction of “dispatched” that would compel such a requirement, and we agree with Petitioner that “[t]he language of claim 5 is clear that a circuit dispatches the timing pulse[s] at random times, not a ‘main program.’”

Reply 9. The Petition shows sufficiently that Sprunk’s circuit dispatches its timing pulses, CLK, at random times.

Accordingly, we conclude that Petitioner demonstrates, by a preponderance of the evidence that claim 5 is anticipated by Sprunk.

*b. Claim 7*

Claim 7 recites that the “integrated circuit includes logic circuits and connecting busses connected such that sequencing of operations of the microprocessor factors in times required to access logic circuits of the integrated circuit, including signal propagation times in the busses and through the logic circuits.” Ex. 1001, col. 11, l. 66–col. 12, l. 5. For this limitation, Petitioner relies on a purported admission by Patent Owner in the related litigation. Pet. 30.

We agree with Patent Owner that this reliance is misplaced. PO Resp. 21–22. As Patent Owner explains, the assertions made in the related

litigation relate to infringement positions against certain of Petitioner's products, and are not discussions of the prior art. *Id.*<sup>7</sup>

Accordingly, we conclude that Petitioner does not demonstrate, by a preponderance of the evidence that claim 7 is anticipated by Sprunk.

*c. Claim 17*

Claim 17 recites that “the decorrelation means comprises a random number generator for de-synchronizing execution of the at least one instruction sequence in the microprocessor.” Ex. 1001, col. 12, ll. 50–52. The Petition's identification of the LFSRG circuits described by Sprunk is sufficient to carry Petitioner's burden with respect to this element. Pet. 30–33; *see supra*, Section II.C.1 (identification of LFSRGs in Sprunk provides sufficient showing of random number generator aspect of “means for decorrelating” construction). Patent Owner does not challenge Petitioner's analysis with respect to this claim in its Response.

We conclude that Petitioner demonstrates, by a preponderance of the evidence that claim 17 is anticipated by Sprunk.

---

<sup>7</sup> We do not consider Petitioner's argument in its Reply that “the '833 Patent itself admits the feature of claim 7 is part of the prior art.” Reply 10 (citing Ex. 1001, col. 1, ll. 28–32). Such an argument is not advanced in the original Petition. *Intelligent Bio-Systems, Inc. v. Illumina Cambridge Ltd.*, 821 F.3d 1359, 1369 (Fed. Cir. 2016) (“It is of the utmost importance that petitioners in the IPR proceedings adhere to the requirement that the initial petition identify ‘with particularity’ the ‘evidence that supports the grounds for the challenge to each claim’ [as required by 35 U.S.C. § 312(a)(3)].”). In addition, the argument is inconsistent with Petitioner's anticipation ground because it offers no explanation of a legitimate reason for looking beyond the four corners of Sprunk.

*d. Claim 18*

Claim 18 recites that “the decorrelation means comprises a clock calibration circuit for eliminating timing pulses that are below a predetermined length.” Ex. 1001, col. 12, ll. 54–56. The Petition identifies a “minimum delay circuit,” disclosed by Sprunk that sets a maximum clock rate, thereby preventing the production of clock pulses above a certain length. Pet. 33–34 (citing Ex. 1004, col. 4, ll. 30–35). To support its position that claim 18 is anticipated, Petitioner characterizes such prevention as “eliminat[ing] the production of any clock pulses that are too short.” *Id.* In replying to Patent Owner’s response that pulses that are never generated cannot be “eliminated,” Petitioner contends that “[t]he ’833 Patent performs the claimed elimination exactly the same way as Sprunk – by assuring that its clock, FRC, only generates pulses having a minimum pulse width  $T_m$ .” Reply 10.

We agree with Patent Owner that the claim requirement of “eliminating” certain timing pulses is not coextensive with never generating those timing pulses. PO Resp. 22–24. Petitioner provides insufficient argument and evidence in its Petition to support a construction of

“eliminating” so broad that it encompasses the circumstance of never generating timing pulses below a predetermined length.<sup>8</sup>

We conclude that Petitioner does not demonstrate, by a preponderance of the evidence that claim 18 is anticipated by Sprunk.

*e. Claim 19*

Claim 19 recites that “the random number generator includes counters which may or may not be looped, and which are initialized to a random value.” Ex. 1001, col. 12, ll. 58–60. In addressing this limitation, Petitioner observes that Sprunk discloses a random number generator consisting of LFSRGs, and contends that a person of ordinary skill in the art “would understand that a LFSRG is simply a form of a counter.” Pet. 34 (citing Ex. 1003 ¶ 116). Petitioner further addresses initialization to a random value by quoting disclosure from Sprunk that the initial state of the LFSRGs are a function of, or identical to, unit dependent random key registers, thereby making a sufficient showing. *Id.* Patent Owner does not challenge Petitioner’s analysis with respect to this claim in its Response.

We conclude that Petitioner demonstrates, by a preponderance of the evidence that claim 19 is anticipated by Sprunk.

---

<sup>8</sup> At the oral hearing, Patent Owner disagreed with Petitioner’s characterization of the ’833 patent, contending that “in order to eliminate, you have to have something to eliminate to begin with.” Tr. 57:2–4. Patent Owner directed us to column 9, lines 9 through 36, of the ’833 patent, as well as Figure 3A and its corresponding discussion. *Id.* at 74:10–18. We have reviewed these sections of the ’833 patent, and find them consistent with Patent Owner’s position.

*f. Claim 20*

Claim 20 recites that “the random number generator uses an algorithm of the cryptographic type or a hash function initialed to the initialization random value.” Ex. 1001, col. 12, ll. 62–64. As Petitioner contends, Sprunk expressly teaches that its S-Box is of a cryptographic type and can be embodied “algorithmically.” Pet. 35 (citing Ex. 1004, col. 5, ll. 7–18). Furthermore, as noted in the analysis of claim 19, Sprunk expressly teaches that its random number generator is initialized to the initialization random value. *See id.*

Patent Owner disputes this understanding of Sprunk, contending that “S-box substitution is different from the required cryptographic algorithm,” and relies on testimony to that effect by Dr. Koç. PO Resp. 25 (citing Ex. 2001 ¶ 128). Patent Owner’s argument is not persuasive. When asked under cross-examination to explain the difference between S-Box substitution and an “algorithm of the cryptographic type” recited in claim 20, Dr. Koç responded that Sprunk’s S-Box provides “very poor crypto.” Ex. 1010, 115:11–13. We agree with Petitioner that Dr. Koç’s testimony on this point is consistent with Sprunk disclosing *poor* cryptography, rather than failing to disclose a cryptographic algorithm at all. Reply. 11–12. The claim imposes no restriction on the sophistication of the “algorithm of the cryptographic type,” and Sprunk thus meets the limitation.

Accordingly, we conclude that Petitioner demonstrates, by a preponderance of the evidence that claim 20 is anticipated by Sprunk.

*g. Claim 23*

Claim 23 recites that “the electrical signals are timing, synchronization and status signals.” Ex. 1001, col. 13, ll. 6–7. Petitioner observes that Sprunk teaches that its microprocessor is timed, synchronized to a clock. Pet. 35–36 (citing Ex. 1004, col. 7, ll. 25–28). In addition, Petitioner notes that Patent Owner has admitted in the related litigation that a clock in a microprocessor reads on the “timing” and “synchronization” signals, and that a secure microprocessor chip inherently contains a status register that reads on recited “status signal.” *Id.* (citing Ex. 1007, 60).

We are not persuaded by Patent Owner’s response that “Sprunk has only a single clock” and that “[w]ithout an additional clock, there can be no decorrelating of timing signals.” PO Resp. 25–26 (citing Ex. 2001 ¶¶ 136, 137). As we discuss *supra*, in Section II.C.1.a, Patent Owner provides insufficient reasons to support its position that the claims require two clocks, and we discern no language in claim 23 that imposes such a requirement.

We conclude that Petitioner demonstrates, by a preponderance of the evidence that claim 23 is anticipated by Sprunk.

*h. Claim 24*

Claim 24 recites that the integrated circuit “further includes means for phase shifting the timing, synchronization or status signals of the processor.” Ex. 1001, col. 13, ll. 8–10. Petitioner’s contention that this limitation is disclosed by Sprunk’s introduction of tapped series delays (D1, D2, . . . , DN in Figures 6 and 7) is consistent with our adopted construction, which requires shift registers and a multiplexer (or their equivalents) to perform the recited function. See Pet. 36–37. Patent Owner’s response again relies on

its contention that the claims require two clocks, which we reject. PO Resp. 26–29.

We conclude that Petitioner demonstrates, by a preponderance of the evidence that claim 24 is anticipated by Sprunk.

*i. Claim 25*

Claim 25 recites that “the phase shifting means generates a random phase shift of the timing, synchronization or status signals of the processor.” Ex. 1001, col. 14, ll. 2–4. Petitioner adequately addresses this limitation, and supports its anticipation contention, by observing that Sprunk explicitly describes that its phase shifting circuit operates on the clock, i.e. the timing and synchronization signal. Pet. 37–38. For the reasons expressed above, Patent Owner response that Sprunk does not disclose two clocks is unpersuasive.

We conclude that Petitioner demonstrates, by a preponderance of the evidence that claim 25 is anticipated by Sprunk.

*3. Obviousness of Claims 21 and 26 over Sprunk*

Petitioner challenges claims 21 and 26 as unpatentable under 35 U.S.C. § 103(a) over Sprunk. Pet. 58–59. A claim is unpatentable under § 103(a) if the differences between the claimed subject matter and the prior art are “such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.” *KSR Int’l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations, including: (1) the scope and content of

the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of skill in the art; and (4) objective evidence of non-obviousness, i.e., secondary considerations.<sup>9</sup> *Graham v. John Deere Co.*, 383 U.S. 1, 17–18 (1966).

Additionally, the obviousness inquiry typically requires an analysis of “whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue.” *KSR*, 550 U.S. at 418 (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006) (requiring “articulated reasoning with some rational underpinning to support the legal conclusion of obviousness”)); see *In re Warsaw Orthopedic, Inc.*, 832 F.3d 1327, 1333 (Fed. Cir. 2016) (citing *DyStar Textilfarben GmbH & Co. Deutschland KG v. C. H. Patrick Co.*, 464 F.3d 1356, 1360 (Fed. Cir. 2006)).

*a. Claim 21*

Claim 21 depends from claims 4, 17, and 19, each of which we conclude above is anticipated by Sprunk, and recites that “the initialization value for the counters originates from a non-volatile memory.” Ex. 1001, col. 12, ll. 65–67. Petitioner acknowledges that the limitation is not expressly taught by Sprunk, but observes that, in Sprunk, “the random values used to initialize the LFSRGs in the random number generators are ‘unit dependent random keys held in registers.’” Pet. 58 (quoting Ex. 1004, col. 4, ll. 48–53). Petitioner reasons that it would have been obvious to keep the secret unit dependent keys in non-volatile memory to allow them to be

---

<sup>9</sup> The parties do not address secondary considerations, which, accordingly, do not form part of our analysis.

persistent across resets, and supports that reasoning with testimony by Dr. Polish. *Id.* at 58–59 (citing Ex. 1003 ¶ 208).

Patent Owner counters that “making keys persistent across resets would go against Sprunk’s own teachings” because Sprunk teaches that “[t]he predictability of modulation should be independent of any type of reset signal,” and because Sprunk teaches a backup battery that allows reinitialization to be avoided after a reset. PO Resp. 56–57 (citing Ex. 1004, col. 3, ll. 61–65, col. 4, ll. 45–48). Patent Owner supports its position with testimony by Dr. Koç, who opines that a person of ordinary skill in the art “would have found it counter-productive to keep the same secret unit dependent keys in Sprunk in non-volatile memory for the purpose of being persistent across resets.” Ex. 2001 ¶ 307. We agree with Petitioner that Patent Owner’s argument evades the argument made in the Petition, and that the Petition provides sufficient reasoning that a person of ordinary skill in the art “would know to keep the initiation values in the key registers (not the LFSRGs) in non-volatile memory, so that they would be persistent across resets.” Reply 24 (citing Pet. 58–59).

We conclude that Petitioner demonstrates, by a preponderance of the evidence, that claim 21 is unpatentable under 35 U.S.C. § 103(a) over Sprunk.

*b. Claim 26*

Claim 26 depends from claims 4, 23, 24, and 25, each of which we conclude above is anticipated by Sprunk, and recites that “the phase shifting means is connected to an external clock for partially or totally de-synchronizing the operation of the processor from the external clock during

the execution of a program.” Ex. 1001, col. 14, ll. 6–9. Petitioner acknowledges that Sprunk does not expressly teach that its phase-shifting circuit is connected to an external clock, but contends that it would have been obvious to substitute the external clock for the internal clock of Sprunk. Pet. 59–60 (citing Ex. 1003 ¶ 211). As Petitioner asserts, “[t]he random modulation of Sprunk can be performed on any clock source, whether internal or external,” and “[o]nce randomly modulated, the performance of the microprocessor driven by the resultant random clock is the same, whether the original source was an external or internal clock.” *Id.* at 59. We agree with this reasoning, which is supported by the testimony of Dr. Polish. Ex. 1003 ¶ 211.

We have considered Patent Owner’s counterarguments, some of which are derivative of its two-chip theory and its contention that phase shifting requires two clocks. PO Resp. 57–59. For the same reasons expressed above, such arguments are unpersuasive. Patent Owner additionally argues that “[a]ll frequency sources in Sprunk are oscillator-based frequency sources, which are analog circuit elements that do not have an external clock,” contending that “replacing the oscillator-based clock of Sprunk with an external clock . . . would be contrary to Sprunk’s actual teachings.” *Id.* at 59. Patent Owner provides insufficient reasoning why such a conclusion follows. Although not cited by Patent Owner, Dr. Koç makes similar assertions, which we find are not supported by sufficient reasoning. Ex. 2001 ¶ 319; *see, e.g., Tate & Lyle Americas LLC v. Cargill, Inc.*, Case IPR2014-00084, slip op. at 17–18 (PTAB Apr. 1, 2014) (Paper 12) (“We give such conclusory, unsupported assertions by an expert little to no weight”). Furthermore, as Dr. Polish observes, “Sprunk expressly

teaches that: ‘Frequency source 10 can comprise an analog or *digital* circuit.’” Ex. 1011 (quoting Ex. 1004, col. 4, ll. 1–2) (emphasis by Dr. Polish).

We conclude that Petitioner demonstrates, by a preponderance of the evidence, that claim 26 is unpatentable under 35 U.S.C. § 103(a) over Sprunk.

*D. Matsumura*

Matsumura describes an integrated-circuit card in which processing results are returned to a microcomputer “when a given time elapses after reception of a processing command . . . , irrespective of the type of the command . . . thereby preventing the processing result and/or the processing command from being found out by measuring the processing time.” Ex. 1006, abst., col. 2, ll. 29–36. This is accomplished with an interrupt that masks the actual operation of the microcomputer. *Id.* at Fig. 4, col. 3, ll. 51–60, col. 4, ll. 15–22. Figure 4 of Matsumura is reproduced below.

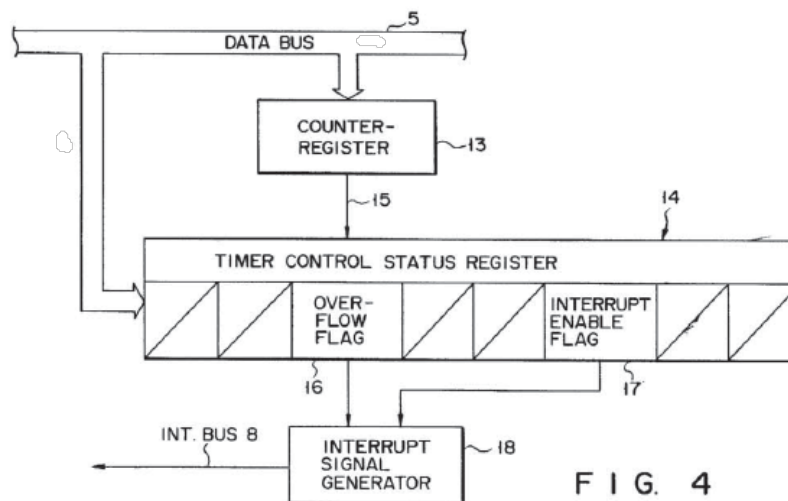


Figure 4 is a block diagram of a microcomputer timer. *Id.* at col. 3, ll. 10–11. When interrupt enable flag 17 and an overflow flag from counter-

register 13 are set, interrupt signal generator 18 generates an interrupt that prevents measuring the processing time. *Id.* at col. 3, ll. 18–19, col. 2, ll. 29–36.

*1. Obviousness of Claims 1–3 and 12–14 Over Sprunk and Matsumura*

Petitioner challenges claims 1–3 and 12–14 under 35 U.S.C. § 103(a) over the combination of Sprunk and Matsumura. Pet. 50–58. In its analysis of these claims, Petitioner contends that it would have been obvious to include the interrupt-generation technique described by Matsumura in the system of Sprunk, and relies on Sprunk for other limitations recited in those claims. Pet. 50–58. In the Institution Decision, we noted that “Petitioner’s articulated reasoning for combining the teachings of the references is generally brief.” Dec. 18. The reasoning provided for claim 2 is typical:

The ’833 Patent further teaches ‘[i]n the case where the secondary program is intended to be combined with a decorrelated clock or interrupt handlers, it is possible in a combination of this type to restrict oneself to one secondary program, thus producing a simpler process.’ Ex. 1001 at 6:44–47. The ’833 Patent thus itself teaches that various security techniques can be combined to provide increased security. See Ex. 1003 at ¶189. Thus, a [person of ordinary skill in the art] would have combined the known interrupt processing of Matsumura into the known device of Sprunk to yield the predictable result of increased security. *Id.* See *KSR Int’l Co. v. Teleflex, Inc.*, 550 U.S. 398, 416 (2007). Therefore, claim 2 would have been obvious to a [person of ordinary skill in the art] based on Sprunk alone or in combination with Matsumura.

Pet. 55. Patent Owner challenges this reasoning, contending that a person of ordinary skill in the art at the time of filing the application that matured into the ’833 patent would not have been motivated to combine the teachings of

Sprunk and Matsumura because “they teach very different designs.” PO Resp. 30. According to Patent Owner, Sprunk teaches “a packaged closed-end design,” while Matsumura teaches “a design in which the processor produces its results in constant time, which requires changes in the architecture of the processor.” *Id.* In addition, Patent Owner disputes the compatibility of Sprunk with Matsumura as related to the combination because “[u]nder no circumstances . . . will all program sequences in Sprunk complete in exactly the same time duration, which is the premise of Matsumura.” *Id.*

We disagree with Patent Owner’s reasoning in light of the limited purpose for which Petitioner relies on teachings of Matsumura, namely to include the interrupt-generation technique described by Matsumura in the system of Sprunk. The cross-examination testimony of Patent Owner’s expert, Dr. Koç, is consistent with Petitioner’s position that, at the time of filing the ’833 patent, it was conventional practice to include interrupt processing in a microprocessor, as taught by Matsumura. *See* Reply 14 (citing Ex. 1010, Ex. 155:11–13). For such a limited purpose, we find Petitioner’s articulated reasoning for incorporating such interrupt processing in the system of Sprunk sufficiently supported by rational underpinning. As Petitioner’s expert, Dr. Polish, testifies, “Matsumura is doing no more than expressing the state of the art at the time, and many other examples of interrupt processing existed at that time.” Ex. 1011 ¶ 21.

*a. Claim 1*

Independent claim 1 recites a “process” that uses a structure generally corresponding to the structure of the improved integrated circuit of claim 4,

but explicitly reciting that the “main program” has “interrupt sequences.” Ex. 1001, col. 11, ll. 8–26. That process comprises “at least one” of four recited steps, and Petitioner correctly contends that “only one of the method steps need be shown in the prior art.” Pet. 51. Petitioner focuses on step “a),” which recites “triggering the sequencing of one of at least one instruction or at least one operation with the aid of a random-pulse clock.” Ex. 1001, col. 11, ll. 19–21.

For this limitation, Petitioner identifies Sprunk’s disclosure of instructions executed by the microprocessor, driven by random clock pulses: “A clock signal is modulated to provide a substantially random (i.e., completely random or pseudorandom) and unpredictable series of clock pulses for clocking a secure microprocessor. The modulation behavior is designed to resist analysis attempts of a pirate.” Ex. 1004, col. 7, ll. 25–29. As Petitioner observes, “Sprunk explains that ‘[t]he present invention accomplishes this goal by modulating the signal which clocks the processor on a pseudorandom basis to render the time at which each successive clock pulse occurs completely unpredictable.’” Pet. 51–52 (quoting Ex. 1001, col. 3, ll. 42–46).

This showing sufficiently supports Petitioner’s position. For the remaining limitations, Petitioner relies on its analysis, with which we agree, as expressed with respect to claim 4. *Id.* at 50–52. We have considered Patent Owner’s responses, and disagree with them for the following reasons.

*i. Means for Decorrelating*

In arguing that the combination of Sprunk and Matsumura does not teach the “integrated circuit” of claim 1 with the recited “means for

decorrelating execution of the at least one instruction sequence of the program from the internal or external electrical signals of [the] integrated circuit,” Patent Owner repeats its two-chip theory. PO Resp. 31–33. In particular, Patent Owner relies on the same argument made with respect to claim 4 to assert that “Sprunk does not disclose the ‘means for decorrelating’ in a single [integrated circuit] as required,” and asserts that “Petitioner relies on Matsumura to cure these deficiencies.” *Id.* at 32.

We disagree with Patent Owner’s characterization of Petitioner’s obviousness theory. Rather than rely on Matsumura for the “means for decorrelating,” Petitioner takes the position that “Sprunk’s anticipation of the ‘means for decorrelating’ discussed above for claim 4 applies with equal force to the preamble of claim 1.” Pet. 51 (citing Ex. 1004, abst., col. 1, ll. 50–54, col. 2, ll. 7–13, col. 3, ll. 42–46, col. 7, ll. 25–29). For the reasons expressed above, we agree with Petitioner’s position, and find Patent Owner’s reliance on its two-chip theory equally unpersuasive in the context of claim 1.

#### *ii. Main-Program Control*

Patent Owner also repeats (and incorporates by reference) its main-program control argument when addressing claim 1, asserting that “Sprunk simply has no main program control over a decorrelating means, as discussed above with respect to Claim 4 and its dependent claims,” and that “Matsumura fails to remedy the deficiencies of Sprunk.” PO Resp. 34

(citing PO Resp. 16–18<sup>10</sup>; Ex. 1002 ¶¶ 193–94). Our determination, in the context of claim 4, that Patent Owner’s main-program control theory is based on an incorrect reading of the claim applies equally in the context of claim 1.

*iii. “triggering”*

In attacking Petitioner’s showing with respect to claim 1’s recitation of “triggering the sequencing of one of at least one instruction or at least one operation with the aid of a random-pulse clock,” Patent Owner appears to link its argument with its main-program control theory, asserting that “[b]ecause there is no program control in Sprunk, Sprunk’s processor does not go from one instruction to another.” PO Resp. 35 (citing Ex. 2001 ¶ 198). The import of this assertion is not entirely clear, but was explored by Petitioner during cross-examination of Patent Owner’s expert, Dr. Koç. Ex. 1010, 171:10–180:13. Dr. Koç confirmed his opinion that the phrase “triggering the sequencing” in step “a)” of claim 1 requires a jump in the main program. *Id.* at 178:1–3.

But the full discussion during cross-examination confirms that Dr. Koç repeatedly conflated separately recited limitations, namely the “sequencing of at least one instruction” of step “a)” with the “random sequence of instructions” of step “c).” See Reply 16. For example, Dr. Koç testified that “[t]riggering sequencing of one instruction, triggering processing of a random sequence of instructions are related,” and that “(a) is

---

<sup>10</sup> We understand this citation to be what Patent Owner intends. The citation and incorporation by reference of “Section VI.B.2” appears intended to cite and incorporate by reference Section VI.A.2 of the Patent Owner Response.

part of the (c), that is, in the sense that (a) is talking about one operation within what (c) does, what is done in (c), which is processing of random sequence of operation.” Ex. 1010, 178:14–16, 178:20–23.

The recitations of steps “a)” and “c)” are distinct, and, as we note above, Petitioner need only demonstrate that one of the steps occurs in the prior art because the claim expressly requires only “that the process comprises *at least one* of the . . . steps.” Ex. 1001, col. 11, ll. 16–17 (emphasis added). We agree with Petitioner that Patent Owner “does not provide any support in claim 1 or the specification . . . for its interpretation that ‘triggering the sequencing’ of step a) requires a jump to different instructions in the main program.” Reply 16–17. For the same reason, we also find Patent Owner’s arguments that the combination of Sprunk and Matsumura do not teach “randomly triggering interrupt sequences” (step “b)”), “triggering the processing of a random sequence of instructions or operations during the execution of a main sequence of instructions or operations” (step “c)”), or “combining at least two of steps a, b, and c” (step “d)”) irrelevant to Petitioner’s argument. See PO Resp. 37–45.

#### iv. “*interrupt sequences*”

Patent Owner also places significant weight on claim 1’s recitation of “a main program having *interrupt sequences*” (emphasis added), drawing a distinction between “*interrupt sequences*” and Matsumura’s disclosure of *interrupts*. PO Resp. 37–44. Patent Owner contends that “[a]n interrupt sequence is a sequence of instructions which are put together not to perform a particular job, but rather to introduce a delay,” and that “[a]n interrupt sequence as *defined and used* in the ’833 Patent has only one purpose: to

introduce a delay.” *Id.* at 37–38 (citing Ex. 2001 ¶ 205) (emphasis added). Although Patent Owner thus asserts that an “interrupt sequence” is “defined” by the ’833 patent, it cites to no support for such a definition other than the testimony of Dr. Koç.

During cross-examination, Dr. Koç acknowledged that there was no such definition in the Specification of the ’833 patent and that the definition was his own. Ex. 1010, 184:11–23. Dr. Koç further acknowledged on cross-examination that one of skill in the art would “interpret interrupt sequence to simply be an interrupt routine,” contrary to Patent Owner’s contention that “Matsumura’s ‘interrupt enable flag’ or ‘interrupt routine’ are not disclosures of ‘interrupt sequences’ either.” Ex. 1010, 205:15–20; PO Resp. 40. Dr. Koç’s cross-examination testimony thus confirms Dr. Polish’s direct testimony drawing an equivalence between Matsumura’s interrupt routines and the claim’s recited “interrupt sequences” as “instruction sequences for handling interrupts.” Ex. 1003 ¶ 168.

Patent Owner’s citation of Figure 8 of the ’833 patent as supporting its distinction between “interrupt sequences” and Matsumura’s “interrupt routines” is also unavailing. See PO Resp. 41–42. Figure 8 shows a secondary program to which operation is rerouted by an interrupt sequence. Ex. 1001, col. 5, ll. 42–43. Patent Owner contends that “[t]he secondary program generates a process with a variable time and can be constituted by a plurality of sequences.” PO Resp. at 42 (citing Ex. 1001, col. 5, ll. 58–63; Ex. 2001 ¶ 216). Although this provides an example of the action of an interrupt sequence in the ’833 patent, Patent Owner’s argument that “Matsumura does not teach any secondary program rerouted to by the interrupt in which the secondary program has a plurality of sequences

generating a variable time” improperly reads a particular embodiment into broader claim language. *Id.*; see *In re Van Geuns*, 988 F.2d 1181, 1184 (Fed. Cir. 1993) (“limitations are not to be read into the claims from the specification”).

*v. Summary*

Having considered Petitioner’s reasoning, as well as Patent Owner’s responses, we conclude that Petitioner demonstrates, by a preponderance of the evidence, that claim 1 is unpatentable under 35 U.S.C. § 103(a) over Sprunk and Matsumura.

*b. Claim 2*

Like independent claim 4, independent claim 2 recites an “integrated circuit,” but includes an explicit recitation of “at least one program interrupt,” as well as requirements that “the program [have] an instruction sequence for authorization, modification, or disablement of the decorrelation means,” and that “authorization includes unmasking the program interrupts.” Ex. 1001, col. 11, ll. 27–40.

In addressing the “modification” instruction sequence, Petitioner observes that Sprunk accomplishes desynchronization by modulating clock 10 with random modulation source 12 to provide random clock CLK to microprocessor 14, and that Sprunk’s program performs the “modification” to the LFSRGs by initializing them with secret keys. Pet. 52–53 (citing Ex. 1004, Fig. 1, col. 4, ll. 5–9, col. 4, ll. 47–53). Such initialization thus “modifies” the decorrelation means, and accordingly meets the claim limitation. In addition, Petitioner addresses the unmasking of program

interrupts by identifying a procedure in Matsumura in which an “interrupt enable flag” is used to enable or disable an internal interrupt. *Id.* (citing Ex. 1006, Fig. 4, col. 3, ll. 26–29). These identifications are sufficient to support Petitioner’s position.

Patent Owner’s responses are unpersuasive. In addition to advancing arguments grounded in the two-chip and main-program control theories that we reject, PO Resp. 31–34, Patent Owner contends that the combination of Sprunk and Matsumura does not teach “the program having an instruction sequence for authorization, modification, or disablement of the decorrelation means, wherein authorization includes unmasking the program interrupts,” *id.* at 45–49.

First, Patent Owner contends that, in the context of claim 2, “modification” does not refer broadly to *any* modification of the decorrelation means (as is implicit in Petitioner’s argument), but refers in more limited fashion “to whether the authorization (or lack of authorization) of the decorrelation means, is modified.” *Id.* at 46–47. Patent Owner further contends that this more limited understanding of “modification” is confirmed by the prosecution history of the ’833 patent because “[t]he language ‘an instruction sequence of the program causes the authorization, modification, or disablement of the decorrelation means’ was added to independent Claim 2 in response to the Examiner’s question regarding how the ‘operation’ of the decorrelation means is ‘authorized.’” *Id.* at 46 (citing Ex. 1002, 229).

We are not persuaded by Patent Owner’s argument that “modification” is properly construed so narrowly. Originally filed claim 21, which issued in amended form as claim 2, recited that “a part of this

program makes it possible *to authorize, modify, or disable* the operation of the decorrelation means.” Ex. 1002, 44 (emphasis added). The recitation of three separate acts was not altered by the incidental changing of the verb forms “authorize,” “modify,” and “disable” to noun forms “authorization,” “modification,” and “disablement” to conform with other amendments to the claims, and Patent Owner provides insufficient reason to interrelate the separately recited “modification” and “authorization.” We discern no compelling basis to do so in light of the prosecution history. In response to the Examiner’s query regarding how the operation of the decorrelation means is authorized, the applicant amended the claim to clarify that the authorization is caused by “an instruction sequence in the program.” *Id.* at 229. Contrary to Patent Owner’s contention, we disagree that this explanation requires that “modification” be construed as narrowly as Patent Owner advocates. Instead, we agree with Petitioner that “there is no support for [Patent Owner’s] interpretation that ‘modification’ refers to the modification of the authorization act.” Reply 21.

Second, the claim’s requirement that “authorization” include “unmasking the program interrupts” was added (in slightly different form that was further amended) at the same time, addressing the Examiner’s concern that the meaning of “authorized” was unclear. Ex. 1002, 229. Patent Owner contends that such unmasking is not met by Matsumura’s “interrupt enable flag” because Matsumura’s security feature is always active and because the flag does not act to “unmask” the program interrupt. Neither of these contentions is persuasive. As Petitioner observes, Matsumura “expressly discloses that its interrupt processing security feature is turned on or off depending on the sensitivity of the commands being

executed.” Reply 21; Ex. 1006, Fig. 5, col. 5, ll. 23–26. In addition, we agree with Petitioner that the function Matsumura assigns to its “interrupt enable flag” is the same as the bit in register 8 of the ’833 patent, which is described as a “mask.” Reply 22; Ex.1001, 5:29–31.

For these reasons, we conclude that Petitioner demonstrates, by a preponderance of the evidence, that claim 2 is unpatentable under 35 U.S.C. § 103(a) over Sprunk and Matsumura.

*c. Claim 3*

Claim 3 depends from claim 2 and recites that “the decorrelation means comprises means for generating one of a timing signal, and a sequence of clock pulses which is dispatched at random times, and used to sequence one of means for randomly generating interrupts and means for triggering the execution of a secondary sequence.” Ex. 1001, col. 11, ll. 41–47.

Petitioner relies on Sprunk for the first portion of this limitation, i.e., “the decorrelation means comprises means for generating one of a timing signal, and a sequence of clock pulses which is dispatched at random times.” Pet. 55–56. As Petitioner observes, Sprunk discloses that “[a] clock signal is modulated to provide a substantially random (i.e., completely random or pseudo random) and unpredictable series of clock pulses for clocking a secure microprocessor.” Ex. 1004, col. 7, ll. 25–29. We agree with Petitioner that this disclosure meets the claim recitation.

Patent Owner’s contrary position, namely that the claim language “require[s] the dispatching to be done under the main program control,” is unpersuasive for reasons similar to those discussed above with respect to

Patent Owner’s main-program control theory. PO Resp. 50. In arguing that certain language in the written description of the ’833 patent requires such main-program control, *id.* (citing Ex. 1001, col. 4, ll. 60–63, col. 7, ll. 22–26), Patent Owner improperly reads a particular embodiment into broader claim language. *See In re Van Geuns*, 988 F.2d at 1184.

Petitioner relies on Matsumura for the second part of claim 3’s limitation, i.e., that the random clock pulses are “used to sequence one of means for randomly generating interrupts and means for triggering the execution of a secondary sequence.” Pet. 56–57. Petitioner observes that Figure 4 of Matsumura discloses a timing circuit for generating an interrupt that “is always functioning to increment its count value by one for every given period while CPU 6 is functioning.” *Id.* at 56 (quoting Ex. 1006, col. 3, ll. 11–14). Supported by testimony of Dr. Polish, Petitioner asserts that a person of skill in the art would understand such disclosure to “indicate[] that the timing circuit operates on the same clock as the CPU,” and reasons that “the same random clock that Sprunk provides to its microprocessor would be applied to the timing circuit of [Matsumura].” *Id.* (citing Ex. 1003 ¶ 193). We agree with this reasoning, which supports the conclusion that “[t]his combination would randomly generate the interrupts in [Matsumura] and provide increased security to thwart the ill-intentioned.” *Id.*

We conclude that Petitioner demonstrates, by a preponderance of the evidence, that claim 3 is unpatentable under 35 U.S.C. § 103(a) over Sprunk and Matsumura.

*d. Claim 12*

Claim 12 depends from claim 4 and recites that “the main program can enable or disable the decorrelation means.” Ex. 1001, col. 12, ll. 28–30. Petitioner’s and Patent Owner’s analyses of this limitation parallel their analyses of the similar limitation recited in independent claim 2. Pet. 57; PO Resp. 51–54. For the reasons expressed above, we agree with Petitioner’s analysis and disagree with Patent Owner’s analysis.

We conclude that Petitioner demonstrates, by a preponderance of the evidence, that claim 12 is unpatentable under 35 U.S.C. § 103(a) over Sprunk and Matsumura.

*e. Claim 13*

Claim 13 is identical to claim 5, but depends from claim 12 instead of directly from claim 4. For the reasons discussed above in Section II.C.2.a, we agree with Petitioner that Sprunk discloses the limitation. *See* Pet. 58. We have also considered Patent Owner’s arguments, presented together with its arguments addressing claim 3, that the combination of Sprunk and Matsumura does not render obvious “a sequence of timing pulses *which are dispatched* at random times,” but are unpersuaded by those arguments for the reasons discussed above. *See* PO Resp. 49–51 (emphasis omitted).

We conclude that Petitioner demonstrates, by a preponderance of the evidence, that claim 13 is unpatentable under 35 U.S.C. § 103(a) over Sprunk and Matsumura.

*f. Claim 14*

Claim 14 is identical to claim 17, but depends from claim 12 instead of directly from claim 4. For the reasons discussed above in Section II.C.2.c, we agree with Petitioner that Sprunk discloses the limitation. See Pet. 58.

We conclude that Petitioner demonstrates, by a preponderance of the evidence, that claim 14 is unpatentable under 35 U.S.C. § 103(a) over Sprunk and Matsumura.

*E. Griffin*

Griffin “pertains to data processing and is particularly directed to preventing compromise of secure data processing routines by a procedure known as a ‘clock attack,’” i.e., a “procedure by which an attacker gains access to secure data or code . . . by determining the time of execution.” Ex. 1005, col. 1, ll. 11–29. Figure 1 of Griffin is reproduced below.

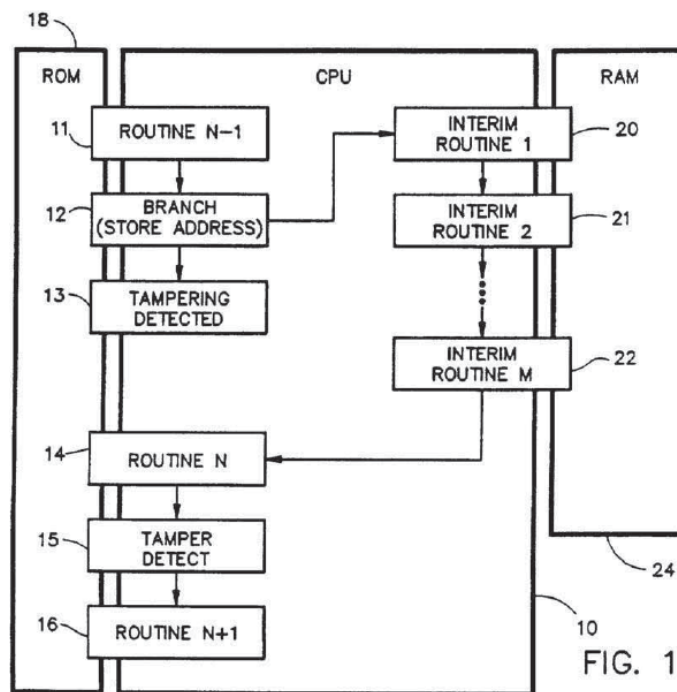


Figure 1 illustrates a data-processing method and system described by Griffin. *Id.* at col. 2, ll. 56–58. Processor 10 executes a group of data processing routines 11, 12, 14, 15, 16 that are “essential sequential subroutines of a repetitive overall larger data processing routine,” in response to code instructions accessed from read-only memory 18. *Id.* at col. 3, ll. 11–27. “[T]o prevent a predetermined protected routine ROUTINE N from being synchronized with the externally observable event that repetitively precedes the protected routine ROUTINE N, the BRANCH routine 12 causes the CPU 10 to branch to the maze of m interim routines INTERIM ROUTINE 1, INTERIM ROUTINE 2, . . . , INTERIM ROUTINE m.” *Id.* at col. 3, ll. 27–34. The total duration of the m interim routines “is a random variable,” and the m interim routines “have different durations.” *Id.* at col. 3, ll. 34–36.

Figure 5 of Griffin is reproduced below.

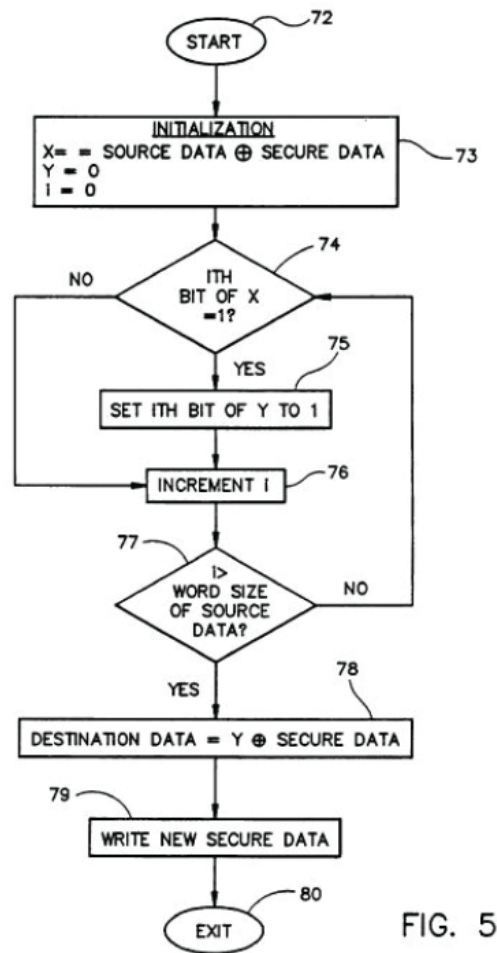


FIG. 5

Figure 5 is a flow diagram for an embodiment of an interim routine that illustrates how it achieves a random duration unknown to an observer. *Id.* at col. 7, ll. 52–53. In this embodiment, a random variable (“secure data”) initializes the random duration for execution of interim routine, with subroutine 75 being executed a number of time that depends on the content of dynamically processed source data and secure data in RAM. *Id.* at col. 8, l. 68–col. 9, l. 5. The random initialization value (“secure data”) is updated during execution of the interim routine:

The randomness of the . . . total duration of the interim routine of FIG. 5 is further compounded by execution of the WRITE NEW SECURE DATE subroutine 79, which changes the secure data in the RAM that is accessed during the INITIALIZATION

subroutine 73, so that each time the interim routine of FIG. 5 is executed, such secure data may be different. The secure data may be provided in the RAM in response to a signal produced by a physically (truly) random phenomena, such as a noisy diode, or in response to a pseudorandom device, such as a pseudorandom number generator.

*Id.* at col. 9, ll. 6–17.

Petitioner challenges claim 22 as unpatentable under 35 U.S.C. § 103(a) over Sprunk and Griffin. Pet. 70–72. Claim 22 depends from claims 4, 17, 19, and 21, each of which we have found unpatentable above, and recites that “the initialization value for the counters is modified during the execution of a program.” Ex. 1001, col. 13, ll. 2–3. Although Sprunk teaches that its initialization values for counters are stored, Petitioner acknowledges that Sprunk does not teach that the value is updated during execution of the program. Pet. 70. For this limitation, Petitioner relies on the teaching of Griffin, contending that a person of ordinary skill in the art “would have combined the random variable update routine of Griffin into the known device of Sprunk to yield the predictable result of increased security that comes from updating the random variable.” *Id.* at 72 (citing Ex. 1003 ¶¶ 260–62; *KSR*, 550 U.S. at 416). The Petition offers no further reasoning for combining the teachings of Sprunk and Griffin, and Petitioner’s Reply only additionally asserts that “both Griffin and Sprunk operate set top boxes [with] the same goal of making observation of the microprocessor more difficult for attackers.” Reply 26 (citing Ex. 1010, 36:15–22 (cross-examination testimony of Dr. Koç agreeing with statement)).

Petitioner provides insufficient reasoning with rational underpinning to support the legal conclusion of obviousness. An allegation that the references both fall within such a broadly characterized field “is not enough for [Petitioner] to meet its burden of presenting a sufficient rationale to support an obviousness conclusion.” *Securus Techs. v. Global Tel\*Link Corp.*, 2017 WL 2992516 at \*5 (Fed. Cir. 2017). “Such short-cut logic would lead to the conclusion that any and all combinations of elements known in this broad field would automatically be obvious, without the need for any further analysis.” *Id.*

Furthermore, as Patent Owner observes, Sprunk and Griffin differ in a relevant way because Sprunk modulates its clock “to provide an unpredictable stream of clock pulses,” Ex. 1004, col. 2, ll. 7–11, while Griffin teaches that its “interim routines should have instructions with parallel clock cycles,” Ex. 1005, col. 5, ll. 54–55. That is, as Dr. Koç testifies, “Griffin relies on stable and always same clock pulses, while Sprunk teaches the exact opposite.” Ex. 2001 ¶ 332. This is a meaningful distinction that Petitioner inadequately addresses, even after it was raised by Patent Owner in its Response.

We conclude that Petitioner does not demonstrate, by a preponderance of the evidence, that claim 22 is unpatentable under 35 U.S.C. § 103(a) over Sprunk and Griffin.

### III. CONCLUSION

For the foregoing reasons, we conclude that Petitioner demonstrates, by a preponderance of the evidence, that claims 4, 5, 17, 19, 20, and 23–25 are anticipated by Sprunk; claims 21 and 26 are unpatentable under 35

U.S.C. § 103(a) over Sprunk; and claims 1–3 and 12–14 are unpatentable under 35 U.S.C. § 103(a) over Sprunk and Matsumura. We also conclude that Petitioner does not demonstrate that claims 7 or 18 are anticipated by Sprunk; or that claim 22 is unpatentable under 35 U.S.C. § 103(a) over Sprunk and Griffin.

#### IV. ORDER

It is

ORDERED that, based on a preponderance of the evidence, claims 1–5, 12–14, 17, 19–21, and 23–26 are held to be unpatentable;

FURTHER ORDERED that, based on a preponderance of the evidence, claims 7, 18, and 22 have not been shown to be unpatentable;

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

IPR2016-01092  
Patent 5,944,833

PETITIONER:

Michael Scheer  
Pejman Sharifi  
Louis Campbell  
WINSTON & STRAWN LLP  
mscheer@michaelscheer.com  
PSharifi@winston.com  
LLcampbell@winston.com

PATENT OWNER:

Peter Schechter  
Tammy Terry  
OSHA LIANG LLP  
schechter@oshaliang.com  
dunn@oshaliang.com