UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
**United States Patent and Trademark Office**
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 13/831,545 | 03/14/2013 | Paul Carl Kocher | 27170.26 (L0026) | 9883 |

108736 7590 12/23/2019
LOWENSTEIN SANDLER LLP / Rambus
Patent Docket Administrator
One Lowenstein Drive
Roseland, NJ 07068

| EXAMINER | |
|---|---|
| NGUYEN, THUONG | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2449 | |

| NOTIFICATION DATE | DELIVERY MODE |
|---|---|
| 12/23/2019 | ELECTRONIC |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patents@lowenstein.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

*Ex parte* PAUL CARL KOCHER, BENJAMIN CHE-MING JUN, and
ANDREW JOHN LEISERSON

Appeal 2018-006630
Application 13/831,545[1]
Technology Center 2400

Before JOSEPH L. DIXON, HUNG H. BUI, and
JON M. JURGOVAN, *Administrative Patent Judges*.

JURGOVAN, *Administrative Patent Judge*.

## DECISION ON APPEAL

Appellant seeks review under 35 U.S.C. § 134(a) from a Final Rejection of claims 1–13, which are all the claims pending in the application. We have jurisdiction under 35 U.S.C. § 6(b).

We AFFIRM IN PART.[2]

[1] We use the word "Appellant" to refer to "applicant(s)" as defined in 37 C.F.R. § 1.42. The real party in interest is Cryptography Research. (Appeal Br. 3.)

[2] Our Decision refers to the Specification ("Spec.") filed March 14, 2013, the Final Office Action ("Final Act.") mailed September 12, 2017, the Appeal Brief ("Appeal Br.") filed February 12, 2018, the Examiner's Answer ("Ans.") mailed April 13, 2018, and the Reply Brief ("Reply Br.")

## CLAIMED INVENTION

The claims are directed to a method and integrated circuit for "providing secure feature and key management" using "a secure memory to store a secret key, and a security manager core, coupled to the secure memory, to receive a digitally signed command, verify a signature associated with the command using the secret key, and configure operation of the integrated circuit using the command." (Abstract.)

Claims 1 and 10 are independent. Claim 1, reproduced below, is illustrative of the claimed subject matter:

> 1. A method comprising:
>
> receiving, by a security manager core of an integrated circuit, a digitally signed message comprising a signature and a feature update information comprising a command that, when executed by the security manager core enables the security manager core to update a functionality of a hardware feature of the integrated circuit to be at least one of locked, unlocked, or modified;
>
> obtaining, by the security manager core, a secret key from a secure memory of the integrated circuit;
>
> verifying, by the security manager core, the signature of the digitally signed message using the secret key; and
>
> executing, by the security manager core, the command to update the functionality of the hardware feature when the signature is verified, wherein the executing the command comprises:
>
> > sending, by the security manager core, a first signal to the hardware feature to lock the functionality of the hardware feature when the feature update information specifies the functionality is to be locked;
> >
> > sending, by the security manager core, a second signal to the hardware feature to unlock the functionality of the hardware feature when the feature update

filed June 12, 2018.

> information specifies the functionality is to be unlocked; and
>
> sending, by the security manager core, a third signal to the hardware feature to modify the functionality of the hardware feature when the feature update information specifies the functionality is to be modified.

(Appeal Br. 40–43 (Claims App.).)

## REJECTIONS & REFERENCES

(1) Claims 1–13 stand rejected under 35 U.S.C. § 101 as directed to non-statutory subject matter. (Final Act. 2–5.)

(2) Claims 1–7, 10, 11, and 13 stand rejected under 35 U.S.C. § 103(a) based on McLellan (US 2009/0187771 A1, published July 23, 2009), Case et al. (US 2010/0199077 A1, published Aug. 5, 2010) ("Case"), and Kocher et al. (US 2008/0037781 A1, published Feb. 14, 2008) ("Kocher '781"). (Final Act. 6–12.)

(3) Claims 8, 9, and 12 stand rejected under 35 U.S.C. § 103(a) based on McLellan, Case, Kocher '781, and Kocher et al. (US 2004/0133794 A1, published July 8, 2004) ("Kocher '794"). (Final Act. 12–15.)

## ANALYSIS

### *Rejection of Claims 1–13 under 35 U.S.C. § 101*

Patent eligibility is a question of law that is reviewable *de novo*. *Dealertrack, Inc. v. Huber*, 674 F.3d 1315, 1333 (Fed. Cir. 2012). Accordingly, we review the Examiner's § 101 determinations concerning patent eligibility under this standard.

Patentable subject matter is defined by 35 U.S.C. § 101, as follows:

> [w]hoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

In interpreting this statute, the Supreme Court emphasizes that patent protection should not preempt "the basic tools of scientific and technological work." *Gottschalk v. Benson*, 409 U.S. 63, 67 (1972) ("*Benson*"); *Mayo Collaborative Servs. v. Prometheus Labs., Inc.*, 566 U.S. 66, 71 (2012) ("*Mayo*"); *Alice Corp. v. CLS Bank Int'l*, 573 U.S. 208, 216 (2014) ("*Alice*"). The rationale is that patents directed to basic building blocks of technology would not "promote the progress of science" under the U.S. Constitution, Article I, Section 8, Clause 8, but instead would impede it. Accordingly, laws of nature, natural phenomena, and abstract ideas, are not patent-eligible subject matter. *Thales Visionix Inc. v. United States*, 850 F.3d 1343, 1346 (Fed. Cir. 2017) (citing *Alice*, 573 U.S. at 216).

The Supreme Court set forth a two-part test for subject matter eligibility in *Alice* (573 U.S. at 217–18). The first step is to determine whether the claim is directed to a patent-ineligible concept. *Id.* (citing *Mayo*, 566 U.S. at 76–77). If so, then the eligibility analysis proceeds to the second step of the *Alice*/*Mayo* test in which we "examine the elements of the claim to determine whether it contains an 'inventive concept' sufficient to 'transform' the claimed abstract idea into a patent-eligible application." *Alice*, 573 U.S. at 221 (internal quotation marks omitted) (quoting *Mayo*, 566 U.S. at 72, 79). There is no need to proceed to the second step, however, if the first step of the *Alice/Mayo* test yields a determination that the claim is directed to patent-eligible subject matter.

### *USPTO Step 1–Categories of Invention in 35 U.S.C. § 101*

The Patent Office has recently revised its guidance for how to apply the *Alice/Mayo* test in the *2019 Revised Patent Subject Matter Eligibility Guidance,* 84 Fed. Reg. 50–57 (Jan. 7, 2019) ("2019 Revised Guidance"). Applying Step 1 of the Revised Guidance (which is unchanged from the prior guidance) to the present case, we determine independent claim 1 recites a "method," and independent claim 10 recites an "integrated circuit," which are a form of "process" and "machine," respectively, thereby falling within one of the categories enumerated under § 101 and satisfying Step 1 of the Revised Guidance.

### *Alice/Mayo—Step 1 (Abstract Idea)*
### *USPTO Step 2A–Prongs 1 and 2*

### *USPTO Step 2A—Prong 1 (Does the Claim Recite a Judicial Exception?)*

We proceed to apply Step 2A, Prong 1 of the Revised Guidance to determine if the claims are "directed to" a judicial exception. This prong of the analysis is part of the first step of the *Alice/Mayo* test.

The first Prong of Step 2A under the Revised Guidance is to determine whether the claims recite a judicial exception including (a) mathematical concepts; (b) certain methods of organizing human activity; and (c) mental processes. 2019 Revised Guidance, 84 Fed. Reg. at 51–52. Here, the Examiner determines that claims 1 and 10 are directed to "the abstract idea of 1) **collecting and comparing known information** . . . and 2) **data recognition and storage**." (Final Act. 4; *see also* Ans. 4–5 (citing *CyberSource Corp. v. Retail Decisions, Inc.*, 654 F.3d 1366 (Fed. Cir. 2011); *Cyberfone Sys., LLC v. CNN Interactive Grp., Inc.*, 558 F. App'x 988

(Fed. Cir. 2014); *SmartGene, Inc. v. Advanced Biological Labs., SA*, 555 F. App'x 950 (Fed. Cir. 2014); *Smart Systems Innovations v. Chicago Transit Auth.*, 873 F.3d 1364 (Fed. Cir. 2017)).)

We are not persuaded by the Examiner's findings, as we are unable to agree that the Examiner has adequately found the concept of claims 1 and 10 to be similar to other concepts (e.g., data collection, recognition, and storage) found to be abstract ideas by our reviewing courts. (*See* Appeal Br. 6–9; Reply Br. 5–6.) Appellant's claims 1 and 10 recite a method and an integrated circuit for commanding a hardware feature of the integrated circuit to change functionality to locked, unlocked, or modified. Here, we are unable to determine from the Examiner's analysis whether such technique for updating a functionality of a hardware feature of an integrated circuit to be locked, unlocked, or modified describes subject matter that is a mathematical concept, a method of organizing human activity, or a mental process (i.e., one of the three types of abstract ideas identified by the Revised Guidance).

### *USPTO Step 2A—Prong 2 (Integration into Practical Application)*

Even if Appellant's claims were considered to recite an abstract idea, we are persuaded by Appellant's arguments that the claims *integrate* an abstract idea *into a practical application* under the second Prong of Step 2A. (2019 Revised Guidance, 84 Fed. Reg. at 54–55; *see* Appeal Br. 9–14; Reply Br. 5–7.) Particularly, we agree with Appellant the claims *integrate* an abstract idea *into a practical application* of locking, unlocking, and modifying hardware features of integrated circuits (ICs) by a command executed by an IC's security manager core to control one or more configurable features of the IC to be locked, unlocked, or otherwise modified. (Appeal Br. 11, 13.) Claim 1 (and similarly, claim 10) recites a combination of additional elements including "*executing, by the security manager core, the command to update the functionality of the hardware feature when the signature is verified*," the command's execution comprising (1) sending, by the security manager core, a first signal to the hardware feature to lock the functionality of the hardware feature when the feature update information specifies the functionality is to be locked, (2) sending, by the security manager core, a second signal to the hardware feature to unlock the functionality of the hardware feature when the feature update information specifies the functionality is to be unlocked, and (3) sending, by the security manager core, a third signal to the hardware feature to modify the functionality of the hardware feature when the feature update information specifies the functionality is to be modified. The claim's additional elements provide a practical application of enabling an adaptive change in the functionality of an IC's circuitry. (*See* Spec. ¶¶ 29, 35, 39, 60, 84, 96.)

As the Specification explains, the claimed technique and security manager core provide:

> configurable ICs, such that *some aspects of the chip may be configured (e.g., for specific applications or to enable/disable particular features) after manufacture*. . . . *Among other things, the SM [(security manager)] core [in an IC] allows one or more configurable features ("Features") of the IC to be locked or unlocked (or otherwise configured, e.g., such as tuning a PLL to adjust a CPU's performance or delivering a secret key for use by the Feature) depending on the desired configuration and security needs.* An SM-enabled IC includes, for example, one (or possibly more) SM cores, and one (or more) secure persistent memories. . . .

> *Even after a product is sold to end user 130, it is also possible to further configure or enable features in a SM-enabled IC.* For example, end user 130 and/or the product, may coordinate with product vendor 125, device administrator 127, security service 120, a delegate authority, a root authority, or some combination thereof, to enable Features in a SM-enabled IC. For example, this process may involve transmitting a request over a network (e.g. by using a radio in the product to transmit a request message via a cellular data network) and receiving (e.g., by using a radio in the product to receive a message from a cellular data network) a chip-specific message that authorizes the requested configuration changes.

(*See* Spec. ¶¶ 29, 39 (emphases added).) Other updates of hardware features to locked, unlocked, or modified include "enabl[ing] a special audio component of the SM-enabled IC," enabling a GPS radio, and configuring a desired operating frequency in a specific IC product. (*See* Spec. ¶¶ 60, 82, 149, 151, Fig. 2B.) Thus, Appellant's claims 1 and 10 provide an improvement in integrated circuit technology by enabling adaptive changes in the functionality of IC circuitry, whereby chip functionality may be configured (even after chip manufacture) for specific applications or to enable/disable particular features. (Appeal Br. 11–14.) We agree with Appellant that claims 1 and 10 integrate the control and activation of circuitry features into a process rooted in computer and integrated circuit technologies. (*See* Appeal Br. 7, 9–14; *DDR Holdings, LLC v. Hotels.com, L.P.*, 773 F.3d 1245, 1257–58 (Fed. Cir. 2014) (holding patent-eligible a claim that "address[es] a business challenge (retaining website visitors)" by enabling visitors "to purchase products from the third-party merchant without actually entering that merchant's website," thus providing a "claimed solution . . . necessarily rooted in computer technology in order to overcome a problem specifically arising in the realm of computer networks”).)

Because claims 1 and 10 integrate the judicial exception into a practical application, we find claims 1 and 10, and their dependent claims 2–9 and 11–13, are not directed to a judicial exception (abstract idea), rather, they are directed to patent-eligible subject matter under § 101. Accordingly, we do not address Step 2B of the Revised Guidance (corresponding to step two of the *Alice/Mayo* test).

For these reasons, we do not sustain the Examiner’s rejection of claims 1–13 as directed to non-statutory subject matter under 35 U.S.C. § 101.

### *Rejection of Claims 1–3, 5, 8, 10, and 11 under 35 U.S.C. § 103(a)*

With respect to independent claim 1, Appellant contends McLellan, Case, and Kocher ’781 do not teach or suggest the claimed “security manager core” of an integrated circuit receiving “a digitally signed message that has *a command that, when executed by the security manager enables the security manager to update a functionality of a hardware feature* of the integrated circuit to be locked, unlocked, or modified,” as required by claim 1. (Reply Br. 9–10; *see also* Appeal Br. 21–22.)

For example, with respect to Case, Appellant argues “nothing in Case teaches that the security controller 212, when executing . . . [a] non-existent command, changes the states of the fuses 254, 256, and 258 of the configuration block 218 to configure the IC device 202”; rather, Case uses the security controller 212 to “control[] access to the components [of IC device 202] based on the states of these fuses (which cannot be undone).” (Reply Br. 9–10; Appeal Br. 22.) Regarding the claimed “digitally signed message comprising a signature and . . . a command” and “executing, by the security manager core, the command to update the functionality of the hardware feature when the signature is verified,” Appellant argues (i) “[n]othing in Case teaches or suggests that the security controller 212 receives *a digitally signed message including a signature and a command*” and (ii) “McLellan does not teach that the alleged re-encrypt command is executed to update the functionality of the hardware feature when the signature is verified.” (Appeal Br. 20–21; Reply Br. 10.) Appellant further argues the combination of McLellan, Case, and Kocher ’781 fails to teach or suggest sending, by a security manager core, a signal to a hardware feature to lock, unlock, or modify the functionality of the hardware feature, as claimed. (Appeal Br. 24–25.) We do not agree.

Instead, we find the Examiner has provided a comprehensive response to Appellant’s arguments supported by a preponderance of evidence. (Ans. 8–9; Final Act. 6–8.) As such, we agree with and adopt the Examiner’s findings and explanations provided with respect to the obviousness rejection of claim 1. (*Id.*)

Particularly, we agree with the Examiner the combination of McLellan, Case, and Kocher ’781 teaches receiving, by a security manager core of an integrated circuit (IC), a digitally signed message having a command that, when executed by the security manager core enables the security manager core to update a functionality of a hardware feature of the IC to be locked, unlocked, or modified, as recited in claim 1. (*Id.*) For additional emphasis, we note that—contrary to Appellant’s argument that

Case does not change the states of fuses (*see* Reply Br. 9–10, Appeal Br. 22)—Case teaches a command whose execution enables an IC controller to change a fuse state, thereby *updating a functionality of a hardware IC feature to be at least one of locked, unlocked, or modified* (as required by claim 1). (*See* Case Fig. 2.) Particularly, paragraph 28 in Case provides that an authenticated "customer can provide a particular command set (as a command file or other data structure) to the authenticated debug controller 210 via the debug interface 216 to direct the authenticated debug controller 210 to blow the permanent debug fuse 258 internally" to configure the IC device 202 to permit open access to the debug interface 216. (*See* Case ¶ 28, Fig. 2.) Thus, Case discloses a command executed by an IC's control portion enables the control portion to *update a functionality of a hardware feature of the IC to be unlocked*—by configuring the IC device 202 to *enable open access to a debug interface* (e.g., to enable hardware evaluation of the IC device).[3] (*See* Case Fig. 2.)

We are also not persuaded by Appellant's argument that the combination of McLellan, Case, and Kocher '781 fails to teach or suggest "a digitally signed message comprising a signature and . . . a command." (Appeal Br. 19–20; Reply Br. 9–10.) As the Examiner finds, McLellan discloses a digitally signed message comprising a signature ("a digital signature" such as "a message authentication code (MAC)," *see* McLellan

[3] Appellant's Specification similarly describes updating a *debug* functionality to be locked, unlocked, or modified by, e.g., "*enabling select modes of operation* (e.g., controlling diagnostic and *debug mode*[])]." (Spec. ¶ 153 (emphasis added); *see also* Spec. ¶ 151 (describing "enabl[ing] or disabl[ing] test modes (e.g., control diagnostic and debug mode). . . . For example, controlling diagnostic and debug mode may temporarily (e.g., until next reset) enable a debug Feature.").)

¶ 4) and a command (to re-encrypt data to off-chip memory and update an address in a boundary register). (Final Act. 6–7 (citing McLellan ¶¶ 4, 18, 32, 38); Ans. 8; *see also* McLellan ¶ 24 (discussing the use of digital MAC signatures in association with encryption).) Kocher ’781 similarly discloses a digitally signed message comprising a signature (“a digital signature. . . . verifiable using the public key,” *see* Kocher ’781 ¶ 94) and a command (“if the signature is valid, unlocks the memory and executes the digitally-signed code,” *id.*). (Ans. 9 (citing Kocher ’781 ¶ 94).) Additionally, Case discloses the “command file” to blow a debug fuse may be a “signed command file” for authenticating a customer, also suggesting “a digitally signed message comprising a signature and . . . a command” as claimed. (*See* Case ¶¶ 23, 28, 31.)

Additionally, we are not persuaded by Appellant’s argument that the combination of McLellan, Case, and Kocher ’781 fails to teach or suggest “executing, by the security manager core, the command to update the functionality of the hardware feature when the signature is verified” as recited in claim 1. (Appeal Br. 21–22; Reply Br. 9–11.) As discussed *supra,* both McLellan and Case teach and suggest executing a command when a signature is verified, and Case also teaches an IC’s control portion executes the command to enable the control portion to update a functionality of a hardware feature to be unlocked (by configuring the IC 202 to enable open access to the debug interface).

We are also unpersuaded by Appellant’s argument that the combination of McLellan, Case, and Kocher ’781 fails to teach or suggest sending, by a security manager core, a signal to a hardware feature to lock, unlock, or modify the functionality of the hardware feature as claimed.

(Appeal Br. 24–25; Reply Br. 11.) As the Examiner finds, Kocher ’781 discloses sending a signal to a hardware feature to unlock a functionality. (Final Act. 8 (citing Kocher ’781 ¶ 94 (“players contain several blocks of nonvolatile memory, which are locked (i.e., read and write permissions are denied) by default. . . . The interpreter verifies the . . . digital signature and, if the signature is valid, unlocks the memory and executes the digitally-signed code”)); Ans. 9.) Additionally, as discussed *supra*, Case discloses sending from the IC’s control portion a signal to blow a debug fuse and enable open access to the debug interface, thereby teaching sending, by a security manager core, a signal to a hardware feature to unlock a functionality of the hardware feature, as claimed. (*See* Case ¶ 28, Fig. 2.)

For these reasons, Appellant has not persuaded us of error in the Examiner’s rejection of claim 1. As such, we sustain the Examiner’s obviousness rejection of claim 1, and dependent claims 2, 3, and 5 for which no separate arguments for patentability are presented. (Appeal Br. 25.)

With respect to independent claim 10, Appellant submits arguments similar to those submitted for claim 1, and further contends the combination of McLellan, Case, and Kocher ’781 fails to teach or suggest “integrated circuit” and “that the hardware feature and the SM core are part of the same integrated circuit”—as required by claim 10, which recites “[a]n integrated circuit comprising . . . a secure memory to store a secret key . . . a security manager (SM) core coupled to the secure memory . . . [and] *a hardware feature of the* integrated circuit.” (Appeal Br. 26.)

Appellant’s arguments are not persuasive. As the Examiner finds (with respect to claims 1 and 10), “Case teaches . . . a security manager core of an integrated circuit.” (Final Act. 7 (citing Case ¶ 23, Fig. 2 (showing an integrated circuit (IC) device 202)); Ans. 8 (again referring to IC device 202).) More particularly, the integrated circuit 202 in Case's Figure 2 includes: "a secure storage element (e.g., a register file, flash memory, etc.) to store one or more root key values **219** specific or unique to the customer" (claimed secure memory to store a secret key), an authenticated debug controller 210 controlling a security controller 212 (claimed security manager core coupled to the secure memory), and a debug hardware feature of the IC (whose functionality may be updated by blowing a debug fuse to unlock, as claimed). (*See* Case ¶¶ 23, 28–29, Fig. 2.)

In light of the above, we sustain the Examiner's § 103(a) rejection of independent claim 10, and dependent claim 11 for which no separate arguments for patentability are presented. (Appeal Br. 33.)

With respect to dependent claim 8 (rejected based on a combination of McLellan, Case, Kocher '781, and Kocher '794), Appellant contends, for the first time in the Reply Brief, that:

> [n]othing in Case or McLellan teaches that to verify the signature the following operations are performed:
>
> obtaining, by the security manager core, delegate permissions and a public key of the delegate authority from a root signed block signed by a root authority;
>
> determining, by the security manager core, that the signature associated with the digitally signed message is valid using the public key of the delegate authority; and
>
> determining, by the security manager core, that the command is permitted using the delegate permissions.

(Reply Br. 14.)[4] This argument, however, is untimely raised and Appellant has not argued good cause for the untimeliness. *See* 37 C.F.R. § 41.41(b)(2).

[4] The Appeal Brief merely argued that "[c]laim 8 recites limitatons[sic] similar, although not identical, to those in claim 1" and for "reasons similar

Accordingly, this argument has been waived as it was raised for the first time in the Reply Brief without a showing of good cause. *See* 37 C.F.R. § 41.41(b)(2) (2012); *see also Ex parte Borden*, 93 USPQ2d 1473, 1474 (BPAI 2010) (informative) ("[T]he reply brief [is not] an opportunity to make arguments that could have been made in the principal brief on appeal to rebut the Examiner's rejections, but were not."). Thus, for the same reasons as independent claim 1, we sustain the Examiner's § 103(a) rejection of claim 8 dependent therefrom.

*Rejection of Claim 4 under 35 U.S.C. § 103(a)*

With respect to claim 4, Appellant contends "nothing in . . . paragraph [4] (or elsewhere in McLellan) teaches that the MAC [(message authentication code)] or the underlying encrypted data within the MAC is *delivered from one hardware component to another hardware component*," as "nothing in McLellan teaches that the memory controller 122, in response to verifying MAC, executes a command and that, *as part of executing the command, keys are delivered to the off-chip memory*." (Appeal Br. 33–34 (emphases added); Reply Br. 12.)

We are not persuaded by Appellant's arguments, and agree with the Examiner that McLellan teaches and suggests delivering key(s) between hardware components for encryption operations, digital rights management operations, password management operations, or authentication operations as claimed. (Ans. 9–10.) For example, McLellan suggests key delivery is

to those discussed above with respect to claim 1, it is submitted that claim 8 is patentable over the combination of McLellan, Case, and Kocher '781. Thus, the combination of cited references does not teach or suggest all the features of the dependent claim 8." (Appeal Br. 36.)

performed between on-chip memory system 108 and off-chip memory 120 because registers of memory system 108 control key encryption of data on off-chip memory 120. (*See* McLellan ¶¶ 8 (describing the key update process), 25 (describing the key update process), 35 ("boundary register B is part of element 116 in the memory subsystem 108" and "boundary register B . . . stores the address of the last memory location [of memory 120] that has been subject to the key update process"), 36 ("an address of the memory location [in memory 120] to which the block is to be written is stored in an address register A," where "register A . . . may be implemented in the memory controller **122**"), 48 ("key update . . . occur[s] as a background process in an encrypted off-chip memory"), Figs. 1–2.)

Accordingly, we sustain the Examiner's § 103(a) rejection of claim 4, as Appellant's arguments have not persuaded us of error in the Examiner's rejection.

*Rejection of Claims 6 and 7 under 35 U.S.C. § 103(a)*

Claim 6 recites "the digitally signed message is signed by a root authority, and the secret key is a public key of the root authority," and claim 7 recites "the digitally signed message is signed by a delegate authority." Appellant contends McLellan and Case do not teach "a root authority or a delegate authority that signed the digitally signed message." (Appeal Br. 34.) Appellant argues paragraph 23 of Case only describes the use of a "root key," not "a root authority" (as in claim 6), and McLellan does not teach that a "delegate authority" (as in claim 7) signs the message described in paragraph 4. (Appeal Br. 34–35; Reply Br. 12–14.)

We do not agree. Rather, we agree with the Examiner that McLellan's digital signature/message authentication codes (MACs), generated from encrypted data prior to storage and later from retrieved encrypted data, suggest the existence of an approved signature by a "delegate authority" as recited in claim 7. (Final Act. 11 (citing McLellan ¶ 4); Ans. 10.) Here, claim 7 does not specify what is "a delegate authority" and what is the significance of a signature being "by a delegate authority."[5] For example, the limitation of claim 7 (i.e., the digitally signed message *being signed by a delegate authority*) does not appear to affect or limit any step in the method of base claim 1, and does not appear to change the performance of claim 1's steps. Appellant has not explained why a

[5] The Specification's description of "delegate authority" is also broad. (*See* Spec. ¶ 33 ("The delegate authority may be product vendor 125, IC manufacturer 110, device administrator 127, some other entity, or some combination thereof").)

signature's *author* (e.g., a delegate authority) is a patentable distinction from the prior art.[6]

We also agree with the Examiner that Case's use of a "root key"—that is "specific or unique to the customer" and is used to "sign[] the command file" and enable "authenticat[ing] the source of the command file and thus authoriz[ing] its execution"—suggests a signature by a "root authority" as recited in claim 6. (Final Act. 10 (citing Case ¶ 23, Fig. 2); *see also* Case ¶ 31.)

As Appellant's arguments have not persuaded us of error in the Examiner's rejection of claims 6 and 7, we sustain the Examiner's § 103(a) rejection of claims 6 and 7.

### *Rejection of Claim 9 under 35 U.S.C. § 103(a)*

With respect to claim 9, Appellant asserts the Office Action cites to non-existent paragraphs in McLellan and fails to establish a *prima facie* obviousness case with respect to claim 9. (Appeal Br. 37.) Thus, Appellant argues the Examiner has not shown where the cited art teaches or suggests "[deriving] . . . a mixed key . . . deriving . . . a transport key using the mixed key . . . decrypting the encrypted payload using the transport key." (*Id.*) We concur with Appellant.

The Examiner has not responded to Appellant's arguments in the Answer. The Examiner, in the Final Action, cites to paragraphs 218 and 234 in McLellan, and paragraph 175 in Kocher '794 (which the Examiner calls

[6] In the event of any further prosecution, we suggest the Examiner consider rejecting dependent claim 7 under (pre-AIA) 35 U.S.C. § 112, fourth paragraph, for failing to further limit the subject matter of claim 1 upon which it depends.

“Kocher”). (Final Act. 14.) However, McLellan does not include paragraphs 218 and 234. Additionally, paragraph 175 in Kocher ’794 merely discusses a “date [that] can also be stored encrypted (e.g., using the value of private data field **428** as a key) to limit read access to the stored date value,” which does not support the Examiner’s findings with respect to claim 9. (*See* Final Act. 14.) As the Examiner has not identified sufficient evidence to support a rejection of claim 9’s “deriving, by the security manager core, a mixed key using a base key accessible to the security manager core,” “deriving, by the security manager core, a transport key using the mixed key,” and “decrypting, by the security manager core, the encrypted payload using the transport key to obtain a decrypted payload,” we do not sustain the Examiner’s obviousness rejection of claim 9.

*Rejection of Claim 12 under 35 U.S.C. § 103(a)*

With respect to claim 12, the Examiner “interpret[s] the crypto oracle 230 [of Kocher ’794] as extractor, interpreter 215 as sub-extractor and processor [210] as [the] hardware feature” recited in the claim. (Ans. 12 (citing Kocher ’794 ¶¶ 10, 95, Fig. 2); *see also* Final Act. 15.)

Appellant contends the cited art does not teach the features of claim 12 requiring “an extractor **coupled** to the SM core” and “**a plurality of sub-extractors coupled to the extractor, wherein each of the plurality of sub-extractors is also coupled to one of the plurality of hardware features**.” (Reply Br. 15; *see also* Appeal Br. 38.) Appellant argues the interpreter 215 of Kocher ’794 is “software executed by the processor 210 and thus cannot be ‘coupled to’ the processor as the alleged hardware feature”; moreover, Kocher ’794 does not teach *multiple* interpreters 215 (e.g., claimed “plurality of sub-extractors") coupled to the crypto oracle 230, with each of the multiple interpreters also coupled to one of a plurality of hardware features, as required by claim 12. (*Id.*) We agree with Appellant.

At the outset, we note Appellant's Specification explains what an *extractor* and *sub-extractors* are. The Specification provides that an *extractor* "is a hardware component that is configured to receive and route information (e.g., keys and feature state) from SM core 305 to the appropriate sub-extractor(s) associated with an intended destination Feature, in a form that is appropriate for the Feature," the *extractor* being produced according to an "extractor hardware definition . . . used in the IC design to route bus outputs from the SM core to the various sub-extractors." (*See* Spec. ¶¶ 86–87, 97.) For example, an *extractor* "may communicate a 128-bit key and target key address to one or more Features . . . via [a] key interface" and "may be configured to decode a target address to identify a particular sub-extractor associated with the destination feature." (*See* Spec. ¶ 98.) The Specification further explains that *sub-extractors* "facilitate the delivery of SM core outputs (such as configuration values and keys) across SM-enabled IC designs," are "generally used for large or complex SM-enabled ICs (including those where top-level ASIC floorplanning and/or routing are challenging) that include multiple Features," and are produced according to "[s]ub-extractor hardware definitions . . . used in the IC design to map the feature space bits from the extractor to named Features and keys, as specified in the one or more configurator input files." (*See* Spec. ¶¶ 87, 96.) The *sub-extractors* deliver inputs to hardware Features, such inputs being "configurable, thereby providing configurability (e.g., via key management and Feature management operations) of the functionality associated with [the] Features." (*See* Spec. ¶ 95.) We have reviewed the Examiner's cited portions of Kocher '794 and do not find they disclose hardware components including an *extractor* coupled to an SM core and *multiple sub-extractors* coupled to the *extractor* and coupled to hardware features as recited in claim 12.

As the Examiner has not identified sufficient evidence to support the rejection of claim 12, we do not sustain the Examiner's obviousness rejection of claim 12.

### *Rejection of Claim 13 under 35 U.S.C. § 103(a)*

Appellant contends "the Office action has failed to establish how each of these separately claimed features [('crypto module' and 'execution engine' in claim 13)] are taught by the combination of cited references." (Appeal Br. 35.) Particularly, Appellant argues "[t]he execution of a command in response to the digital signature being verified is not taught by McLellan[, r]ather, McLellan teaches that the verification of the digital signature is done to verify whether the 'encrypted data has been modified while stored in the external memory.'" (Appeal Br. 35–36.)

We are not persuaded by Appellant's arguments, and agree with the Examiner that McLellan teaches it was known to use a crypto module to verify a signature of a digitally signed message, as required by claim 13. (Ans. 11 (citing McLellan ¶¶ 4–5); Final Act. 11–12.) For example, McLellan describes authenticating/verifying a message's digital signature to determine whether to accept or reject the message. (*See* McLellan ¶¶ 4 ("a digital signature can allow detection of this type of tampering with encrypted data," the "signature [being] an example of what is more generally referred to herein as a message authentication code (MAC),” where based on the MAC “the processor can determine whether to accept or reject the retrieved encrypted data based on such a determination”), 5 (providing that replay attacks may be prevented by “incorporating a random value or ‘nonce’ into the data prior to encryption, or using one-time encryption keys”).) Additionally, Case’s Figure 2 discloses controllers 210 and 212 of IC 202 verify a response value to a challenge value to authenticate a customer desiring to gain access to a debug interface, also suggesting “a crypto module to verify the signature of the digitally signed message” as claimed. (*See* Case ¶¶ 29 (“the authenticated debug controller **210** conducts a challenge/response process to authenticate a customer desiring to gain access to the debug interface. . . . [and] signals the security controller **212** to set the access level for the IC device **202**”), 30 (“**security controller 212 is configured to enact a particular security level at the IC device 202 based on signaling received from the authenticated debug controller 210**,” for example, “**the IC device 202 may be configured in one of four security** levels [including] . . . Closed: the debug interface **216** is not available (either customer authentication has not taken place or has not been successful)”).)

We also agree with the Examiner that McLellan teaches it was known to execute a command upon verifying a signature, as required by claim 13. (Ans. 11 (citing McLellan ¶¶ 4–5); Final Act. 11–12.) For example, McLellan describes executing a command (regarding encrypted data, e.g., reject the data, or retrieve and accept the encrypted data as valid and decrypt it) based on digital signature (e.g., MAC) verification. (*See* McLellan ¶¶ 3–5.) Additionally, Case discloses executing a command to change a debug fuse state, also suggesting executing a command upon verifying a signature.

(*See* Case ¶ 28 ("permanent debug fuse **258** is protected from being blown without proper authentication," and "**once the customer is authenticated, the customer can provide a particular command set (as a command file or other data structure) to the authenticated debug controller 210** . . . to direct the authenticated debug controller **210** to blow the permanent debug fuse **258** internally"), Fig. 2.)

Appellant's additional argument that the "Office action has failed to establish how" claim 13's "communication module" and "data storage module" are taught by the combination of cited references (*see* Reply Br. 13) does not address the Examiner's findings with respect to these claim limitations. (*See* Final Act. 12 (citing Case Fig. 2).)

Accordingly, we sustain the Examiner's § 103(a) rejection of claim 13, as Appellant's arguments have not persuaded us of error in the Examiner's rejection.

## DECISION SUMMARY

The Examiner's rejection of claims 1–13 under 35 U.S.C. § 101 is REVERSED.

The Examiner's rejection of claims 1–8, 10, 11, 13 under 35 U.S.C. § 103(a) is AFFIRMED.

The Examiner's rejection of claims 9 and 12 under 35 U.S.C. § 103(a) is REVERSED.

In summary:

| **Claims Rejected** | **35 U.S.C. §** | **Basis/Reference(s** | **Affirmed** | **Reversed** |
|---|---|---|---|---|
| 1–13 | 101 | Non-statutory | | 1–13 |
| 1–7, 10, 11, 13 | 103(a) | McLellan, Case, Kocher ’781 | 1–7, 10, 11, 13 | |
| 8, 9, 12 | 103(a) | McLellan, Case, Kocher ’781, Kocher ’794 | 8 | 9, 12 |
| **Overall Outcome** | | | 1–8, 10, 11, 13 | 9, 12 |

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED-IN-PART