UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

KINGSTON TECHNOLOGY COMPANY, INC.,
Petitioner,

v.

MEMORY TECHNOLOGIES, LLC,
Patent Owner

Case No.: To Be Assigned
U.S. Patent No. 7,827,370

PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT NO. 7,827,370

Mail Stop "**Patent Board**"
Patent Trial and Appeal Board
U.S. Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes and Codes

Rules and Regulations

Code of Federal Regulations

EXHIBIT LIST

Exhibit No.	***Description***
1001	U.S. Patent No. 7,827,370
1002	File History for U.S. Patent No. 7,827,370
1003	U.S. Patent App. Pub. No. 2004/0083346 to Chevallier *et al*.
1004	U.S. Patent No. 6,279,114 to Toombs *et al*.
1005	U.S. Patent No. 6,262,918 to Estakhri *et al*.
1006	Declaration of Dr. R. Jacob Baker
1007	U.S. Patent App. No. 10/279,470 to Chevallier *et al*.
1008	Third Joint Claim Construction and Prehearing Statement (N.D. Cal. Patent L.R. 4-3), filed in the related matter on Nov. 16, 2018

I. INTRODUCTION AND STATEMENT OF RELIEF REQUESTED (37 C.F.R. §42.22(a))

Kingston Technology Company, Inc. ("Petitioner" or "Kingston") hereby petitions to institute an *inter partes* review of Claims 1-3, 5-7, 12-15, 19, and 25 (the "Challenged Claims") of U.S. Patent No. 7,827,370 (the "'370 Patent," Ex. 1001), and cancel those claims as unpatentable. The '370 Patent concerns write-protecting a peripheral memory card.

The prior art presented in this Petition—Chevallier (Ex. 1003), Toombs (Ex. 1004), and Estakhri (Ex. 1005)—disclose each and every limitation of the Challenged Claims. Chevallier and Estakhri were not considered during original prosecution of the '370 Patent, and the applicant admitted that Toombs discloses "that an entire card may be write protected by setting write protect bits in a CSD register" and that "addressed portions of memory can be write protected." However, the applicant argued such write protection was not permanent, as claimed, "because Toombs describes removing/cancelling the write protection via a clear command." Chevallier expressly discloses permanent write protection.

Therefore, as discussed in detail below, Chevallier—alone or in combination with Toombs and/or Estakhri—anticipates and/or renders obvious the Challenged Claims of the '370 Patent under 35 U.S.C. §§ 102 and 103. Accordingly, there is a reasonable likelihood that Petitioner will prevail with respect to at least one

challenged claim, and Petitioner respectfully requests that the Board institute a trial for *inter partes* review and cancel all Challenged Claims as unpatentable.

II. MANDATORY NOTICES

A. Real Party-In-Interest (37 C.F.R. §42.8(b)(1))

Petitioner Kingston Technology Company, Inc., is a real party-in-interest. Petitioner's parent company, Kingston Technology Corporation ("Kingston Holding"), is a holding company without any employees or operations. However, because Kingston Holding is a co-defendant in the related matter identified below, is the sole owner of Petitioner, and shares some directors, Petitioner identifies Kingston Holding as an additional real party-in-interest.

B. Identification of Related Matters (37 C.F.R. §42.8(b)(2))

Patent Owner Memory Technologies, LLC ("MTL") has asserted the Challenged Claims of the '370 Patent, as well as claims from seven other patents, against Kingston and Kingston Holding in a co-pending litigation, *Memory Technologies, LLC v. Kingston Technology Corporation et al*., 8:18-cv-00171-JLS-JDE (C.D. Cal.). MTL's Complaint was filed on January 31, 2018, and served on Kingston, at the earliest, on February 1, 2018.

In addition to this Petition, Kingston has or will be filing petitions for *inter partes* review of the other seven patents that MTL has asserted against it.

C. Counsel and Service Information (37 C.F.R. §§42.8(b)(3) & (b)(4))

Petitioner designates the following Lead and Backup Counsel. Concurrently filed with this Petition is a Power of Attorney for appointing the following Lead and Backup Counsel, per 37 C.F.R. § 42.10(b). Service via hand-delivery may be made at the postal mailing addresses below. Petitioner consents to electronic service by e-mail at the following address: **kingston-370ipr@pillsburylaw.com**.

Lead Counsel	Back-Up Counsel
Robert C.F. Pérez (Reg. No. 39,328) PILLSBURY WINTHROP SHAW PITTMAN LLP 1650 Tysons Boulevard, 14th Floor McLean, VA 22101 Telephone: 703.770.7900 Facsimile: 703.770.7901	**Christopher Kao**, Kingston's counsel in the co-pending litigation (*Pro hac vice* motion to be filed) PILLSBURY WINTHROP SHAW PITTMAN LLP Four Embarcadero Center, 22nd Floor San Francisco, CA 94111 Telephone: 415.983.1000 Facsimile: 415.983.1200 **Brock S. Weber**, Kingston's counsel in the co-pending litigation (*Pro hac vice* motion to be filed) PILLSBURY WINTHROP SHAW PITTMAN LLP Four Embarcadero Center, 22nd Floor San Francisco, CA 94111 Telephone: 415.983.1000 Facsimile: 415.983.1200

D. Payment of fees (37 C.F.R. §42.103)

Petitioner authorizes the Patent and Trademark Office to charge Deposit Account No. 033975 for the petition fee and for any other required fees.

III. REQUIREMENTS FOR *INTER PARTES* REVIEW

This Petition complies with all statutory requirements under the AIA and 37 C.F.R. §§ 42.104, 42.105, and 42.15, and should be accorded a filing date as the date of filing of this Petition pursuant to 37 C.F.R. § 42.106.

A. Prior Art Relied Upon

Exhibit 1003—United States Patent Application Publication No. 2004/0083346 to Chevallier *et al*. ("Chevallier"), titled "Permanent Memory Block Protection in a Flash Memory Device," filed October 24, 2002 and published April 29, 2004. Chevallier is prior art under at least pre-AIA 35 U.S.C. §§ 102(a) and (e). Chevallier was not considered during the prosecution of the '370 Patent.

Exhibit 1004—United States Patent No. 6,279,114 to Toombs *et al*. ("Toombs"), titled "Voltage Negotiation in a Single Host Multiple Cards System," filed November 4, 1998 and issued and published on August 21, 2001. Toombs is prior art under at least pre-AIA 35 U.S.C. §§ 102(a), (b), and (e). Toombs was cited by the Patent Office during prosecution of the '370 Patent.

Exhibit 1005—United States Patent No. 6,262,918 to Estakhri *et al*. ("Estakhri"), titled "Space Management for Managing High Capacity Nonvolatile

Memory," filed June 30, 2000 and issued and published on July 17, 2001. Estakhri is prior art under at least pre-AIA 35 U.S.C. §§ 102(a), (b), and (e). Estakhri was not considered during the prosecution of the '370 Patent.

B. Identification of Challenge

Pursuant to 37 C.F.R. §42.104(b), Petitioner shows the following grounds:

1. Claims 1-3, 5-6, 12-15, and 25 are anticipated under 35 U.S.C. §§ 102(a) and (e) by Chevallier;
2. Claims 1-3, 5-6, 12-15, and 25 are rendered obvious under 35 U.S.C. § 103 by Chevallier;
3. Claims 1-3, 5-7, 12-15, 19, and 25 (*i.e.*, all Challenged Claims) are rendered obvious under 35 U.S.C. § 103 by Chevallier in view of Toombs; and
4. Claim 25 is rendered obvious under 35 U.S.C. § 103 by Chevallier in view of Toombs and Estakhri.

The Declaration of R. Jacob Baker, Ph.D., P.E., filed herewith (Ex. 1006, "Baker Decl."), supports the challenge in this Petition that Claims 1-3, 5-7, 12-15, 19, and 25 are invalid as anticipated and obvious.

IV. BACKGROUND OF THE TECHNOLOGY

Memory cards, such as PC cards, compact flash ("CF") cards, secure digital ("SD") cards, or multimedia cards ("MMC"), are electronic data storage devices

used in various portable electronic devices such as digital cameras, mobile phones, laptop computers, tablets, and video game consoles (known as "host" devices). Ex. 1006, ¶74. Data is stored on a memory device by recording the data in bits in memory cells. *Id*., ¶75. This data can be read by sensing the values of the bits. *Id*.

Memory devices are typically based on a block architecture in which the memory is divided into blocks of memory. Ex. 1006, ¶87. This allows file systems to erase certain blocks of memory instead of the entire device. Ex. 1003, ¶0005. Memory sectors, memory blocks, and memory groups are units used to describe portions of a memory. Ex. 1004, 27:37-42, FIG. 66.

MMCs can utilize one or more memory technologies such as ROM (read only memory), OTP (one-time programmable), MTP (multi-time programmable), or Flash. *Id*., 7:5-8, FIG. 4. An example MMC is shown in the figure below.

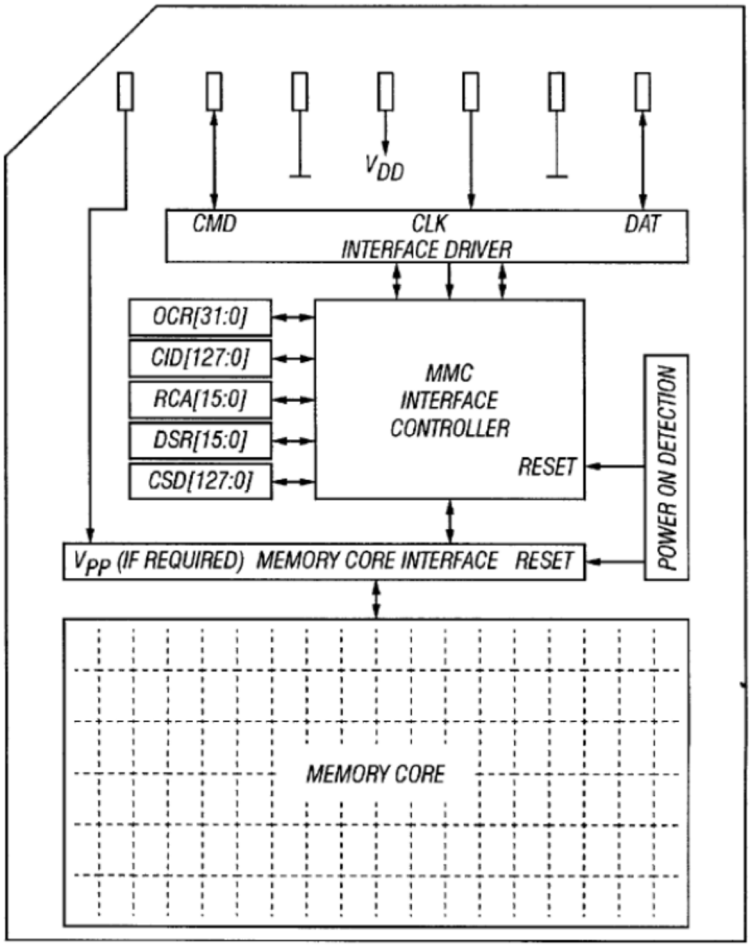

FIG. 14

Id., FIG. 14. As illustrated, a MMC communicates with a host device by a CMD bus line for commands and responses and a DAT bus line for transmission of data. *Id*., 7:57-65. The MMC includes a command set for controlling operations on the MMC such as data read/write or obtaining card information. *Id*., FIGs. 38-44. Each command is identified by a command number. For example, CMD 28 of Fig. 42 identifies the "SET_WRITE_PROT" command. *Id*., FIG. 42.

As illustrated above, the MMC includes an interface controller coupled to the MMC's memory core. Ex. 1006, ¶83. The interface controller also couples to

a group of registers (*e.g.*, OCR, CID, CSD, RCA, DSR) that can store information about the memory card. Ex. 1004, 9:45-59. For example, the CSD (Card Specific Data) register stores card information such as data format, data transfer speed, *etc*. *Id*., 10:22-33, FIGs. 17A-B. The CSD also contains entries that influence the effect of commands executed by the memory card. For example, the WP_GRP_ENABLE bit of the CSD register controls whether groups of memory in the memory core are protected by execution of a SET_WRITE_PROT command. *Id*., 30:1-12, Fig. 17B. As another example, the WP_GRP_SIZE CSD register bit defines the size of the group to be protected by the SET_WRITE_PROT command. *Id*. CSD register entries may be R=readable, W=writable once, or E=erasable (multiple writable). *Id*., 10:29-31.

As of July 2004, the MMC standard allowed permanent (and temporary) write protection of an entire memory card by setting the PERM_WRITE_PROTECT (or TMP_WRITE_PROTECT) bit in the CSD register. *Id*., 12:56-67. The MMC standard also allowed write protecting memory groups of a memory card using the SET_WRITE_PROT command, which could be cleared by a CLR_WRITE_PROT command. *Id*., 30:9-12.

V. OVERVIEW OF THE '370 PATENT

The '370 Patent relates to permanently write protecting a memory card. The '370 Patent notes that it is desirable for some data to be protected from accidental

or conscious deletion by a user while other data is alterable. Ex. 1001, 1:31-49. According to the '370 Patent, at the time of the invention, "[t]he MMC specification offers one solution to this kind of problem." *Id*., 1:56-57. The MMC specification provides for write protecting a portion of a MMC using a specific command called SET_WRITE_PROT. *Id*., 1:60-62. However, the '370 Patent asserts that command does not result in permanent write protection because the write protection can be cancelled using another command called (CLR_WRITE_PROT). *Id*., 1:63-66.

The '370 Patent recognizes that at the time of the invention the MMC specification did provide permanent write protection (*i.e*., write protection that was not changeable) by setting a permanent write protection bit called PERM_WRITE_PROTECT in the CSD (Card Specific Data) register of the memory card. *Id*., 1:66-2:2. However, the '370 Patent asserts such permanent protection could only be applied to the entire card. The '370 Patent instead purports to disclose "permanently write protecting a portion of a multimedia card." *Id*., 2:7-8. Specifically, the '370 Patent discloses "identifying a bit in a specific data register of the memory [and] setting said bit to have a certain predefined value that causes write protection command to mean permanent write protection of part of the memory." *Id*., 2:12-18. The '370 Patent discloses that after this bit is set,

the command is executed to cause a part of the memory to be permanently write protected. *Id*., 2:19-21.

In one embodiment, the '370 Patent discloses defining the PERM_WRITE_PROTECT bit of the CSD "in such way that setting of this bit does not as such protect the whole card," but rather "indicate[s] that all the write protect groups protected with SET_WRITE_PROT command . . . are permanently write protected and cannot be un-protected using CLR_WRITE_PROTECT command." *Id*., 2:55-62. The segment size of the memory to be protected "is defined in the units of WP_GRP_SIZE groups as known to those skilled in the art." *Id*., 2:62-64. Part of the CSD fields corresponding to this embodiment is shown in Table 1:

TABLE 1

permanent write protection of write protect groups	PERM_WRITE_PROTECT	1	R/W	[13:13]

In another embodiment, one of the unused CSD bits (*e.g*., called PARTIAL_PERM_WP) may be defined to "indicate that a portion of the multimedia card [] is permanently write protected." *Id*., 3:9-12. The PARTIAL_PERM_WP bit "should be re-programmable" and "could be cleared automatically when SET_WRITE_PROTECT command [] is received." Part of the CSD fields according to this embodiment is shown in Table 2:

TABLE 2

permanent write protection of write protect groups	PARTIAL_PERM_WP	1	R/W/E	[17:17]

Id., Table 2.

VI. SUMMARY OF THE PROSECUTION HISTORY

On August 18, 2010, the Patent Office issued a Notice of Allowance stating that "[t]he primary reasons for allowance of [the] independent claims . . . is the inclusion in the claims of 'setting at least one bit in a data register configured to indicate that permanent write protection of the at least one part of the memory is allowed in order to redefine the command to allow permanent write protection that cannot be un-protected by a command, of the at least one part of the memory.'" Ex. 1002, 24.

During prosecution, the applicant acknowledged that the Toombs Publication (U.S. Pub. 2001/0016887, Ex. 1004) cited by the Patent Office "described that an entire card may be write protected by setting write protect bits in a CSD register" and disclosed that "addressed portions of memory can be write protected." Ex. 1002, 24. However, the applicant argued such write protection was not permanent "because Toombs describes removing/cancelling the write protection via a clear command." *Id*.

VII. SUMMARY OF THE PRIOR ART

A. Chevallier

Chevallier describes temporarily or permanently protecting memory blocks against write and erase operations. Ex. 1003, Abstract, ¶0008; Ex. 1006, ¶137. For example, Chevallier discloses a flash memory device having a temporary lock function that temporarily locks memory blocks in response to a lock command. Ex. 1003, ¶¶0008, 0016; Ex. 1006, ¶137. The temporary lock function can be cleared, allowing memory blocks that were protected by the temporary function to be erased or reprogrammed. Ex. 1003, ¶0016; Ex. 1006, ¶137.

Chevallier also discloses a secure function that permanently locks memory blocks in response to a secure command. Ex. 1003, ¶¶0007, 0008, 0016, 0018, 0036; Ex. 1006, ¶138. The memory blocks protected by the secure function are permanently secured against write and erase operations. Ex. 1003, ¶¶0016, 0036; Ex. 1006, ¶138. Notably, Chevallier discloses that the secure command and the lock command can be the same command. Ex. 1003, ¶¶0008, 0020; Ex. 1006, ¶138. The secure function can be enabled and disabled by setting a secure function bit in a register. Ex. 1003, ¶0038; Ex. 1006, ¶138. The value of the bit controls whether a lock command will result in temporary write protection or in permanent write protection. Ex. 1003, Claims 18-19; Ex. 1006 ¶138.

B. Toombs

Toombs describes write protecting at least portions of groups of a memory of a MultiMediaCard ("MMC"). Ex. 1004, 29:40-42; Ex. 1006, ¶142. Toombs discloses that the MMC may include a number of data registers used to store information about the card, such as card / content specific information and configuration parameters. Ex. 1004, 9:51-60; Ex. 1006, ¶142. For example, Toombs discloses a card specific data register (CSD) that contains information about the memory card's characteristics. Ex. 1004, 10:21-26; Ex. 1006, ¶142.

Toombs discloses permanently write protecting the memory card by setting a non-erasable PERM_WRITE_PROTECT field in the CSD register. Ex. 1004, 12:56-67, 30:1-3; Ex. 1006, ¶143. Toombs also discloses permanently write protecting the memory card by setting an erasable TMP_WRITE_PROTECT field in the CSD. Ex. 1004, 12:56-67, 30:1-3; Ex. 1006, ¶143.

Lastly, Toombs discloses enabling write protection of memory groups (*i.e.*, less than the whole card) by setting a WP_GRP_ENABLE bit in the CSD. Ex. 1006, ¶143. The size of each memory group to be write protected is defined by the WP_GRP_SIZE field in the CSD. *Id*. The addressed group(s) are then write protected by executing a SET_WRITE_PROT command. Ex. 1004, 30:3-10; Ex. 1006, ¶143.

C. Estakhri

Estakhri discloses a flash memory device having a microprocessor circuit and a volatile storage unit for executing operations on non-volatile memory. Ex. 1005, Fig. 1; Ex. 1006, ¶146. The volatile storage unit stores firmware that is executed by the microprocessor. Ex. 1005, 4:54-59; Ex. 1006, ¶146.

VIII. CLAIM CONSTRUCTION

The Patent Office has adopted a rule by which claims are construed in accordance with "the standard used in federal courts, in other words, the claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. 282(b), which is articulated in *Phillips v. AWH Corp*., 415 F.3d 1303 (Fed. Cir. 2005)." This rule reflects that the PTAB in an AIA proceeding will apply the same standard applied in federal courts to construe patent claims. For example, claim construction begins with the language of the claims. *Phillips,* 415 F.3d at 1312-14. The "words of a claim are generally given their ordinary and customary meaning," which is "the meaning that the term would have to a person of ordinary skill in the art in question at the time of the invention, *i.e.,* as of the effective filing date of the patent application." *Id.* at 1312-13. The specification is "the single best guide to the meaning of a disputed term and . . . acts as a dictionary when it expressly defines terms used in the claims or when it defines terms by implication." *Id.* at 1321 (internal quotation marks

omitted). Although the prosecution history "often lacks the clarity of the specification and thus is less useful for claim construction purposes," it is another source of intrinsic evidence that can "inform the meaning of the claim language by demonstrating how the inventor understood the invention and whether the inventor limited the invention in the course of prosecution, making the claim scope narrower than it would otherwise be." *Id.* at 1317. Extrinsic evidence, such as expert testimony and dictionaries, may be useful in educating the court regarding the field of the invention or helping determine what a person of ordinary skill in the art would understand claim terms to mean. *Id.* at 1318-19. However, extrinsic evidence in general is viewed as less reliable than intrinsic evidence. *Id*.

All claim terms of Challenged Claims of the '370 Patent have been accorded their plain and ordinary meaning as understood by a person having ordinary skill in the art at the time of the alleged invention (a "POSA") and consistent with the intrinsic record. Petitioner's interpretation of the claim terms in the '370 Patent is further explained for each claim limitation in relation to the prior art discussed in the proposed grounds for invalidity, below, in Grounds 1-4.

Under the *Phillips* standard and for clarity, Petitioner provides the following specific constructions.[1]

A. "a data register"

Challenged Claims 1, 5, 12, 14, and 25 all recite a "data register." A POSA would have recognized that the plain and ordinary meaning of this phrase is "a portion of memory containing information about a memory card." Ex. 1006, ¶¶116-18. Indeed, Patent Owner has agreed to this construction in the co-pending related litigation, which is also governed under the *Phillips* standard. Ex. 1008, 1-2 (showing that the agreed construction of "data register" is "a portion of memory containing information about a memory card").

The intrinsic evidence also supports this construction. The specification refers primarily to a particular kind of data register, the "CSD (Card Specific Data) register." Ex. 1001, 1:59-60. The CSD consists of fields which have bit strings of varying length. *Id*., 2:50-54. According to the specification, a "CSD provides

[1] Petitioner reserves the right to address any claim construction positions taken by the Patent Owner in its Preliminary Response, if any, including under 37 C.F.R. § 42.108(c). Petitioner further reserves its ability to show that claims of the '370 Patent are invalid under 35 U.S.C. §112 in the co-pending litigation, despite offering explicit and implicit claim constructions herein.

information on how to access the card contents" (*Id*., 2:49), contains information about the size of memory groups to be write protected (*Id*., 1:58-60), contains a bit enabling permanent write protection on some or all of the memory card (*Id*., 2:65-3:7; 3:38-47), and contains information identifying the type of memory technology on a card and the address space of that memory (*Id*., 5:8-13). In sum, the '370 Patent discloses that a CSD contains information about the memory card. Ex. 1006, ¶117.

Therefore, a POSA would have recognized that "a data register" is "a portion of memory containing information about a memory card." Ex. 1006, ¶118.

B. "redefine the command to allow permanent write protection"

Challenged Claims 1, 12, and 25 each recite this element. A POSA would have recognized this phrase to mean to "cause a command that would not result in permanent write protection to result in permanent write protection." Ex. 1006, ¶¶122-23. Here, again, Patent Owner has agreed to this construction in the co-pending related litigation. Ex. 1008, 1-2 (showing that the agreed construction of this phrase is to "cause a command that would not result in permanent write protection to result in permanent write protection").

The intrinsic record also supports this construction. The '370 Patent explains that the MMC specification provides the command SET_WRITE_PROT, which write protects an addressed write-protect group. Ex. 1001, 1:60-62.

However, the specification states that the drawback of using the command is that "it does not allow the portion of the MMC to be permanently write protected" because "[t]he write protection can be cancelled using CLR_WRITE_PROTECT command to the addressed write-protect group." *Id*., 1:63-66. The specification proposes to define a bit that, if set, will "indicate that all the write-protect groups protected with SET_WRITE_PROT command 5 (CMD 28) are permanently write protected and cannot be un-protected using CLR_WRITE_PROTECT command 5 (CMD29)." *Id*., 2:59-63, 3:27-31. In other words, the SET_WRITE_PROT command does not result in permanent write protection unless the defined bit is set. Ex. 1006, ¶123.

Thus, a POSA would understand from the specification that "redefine the command to allow permanent write protection" means to "cause a command that would not result in permanent write protection to result in permanent write protection." *Id*.

C. "wherein said at least one bit has a certain predefined value"

Dependent Claim 2 recites, "wherein said at least one bit has a certain predefined value." A POSA would have recognized this phrase to mean that the bit is set to a value associated with permanent write protection. *Id*. ¶¶,124-26. Here, again, Patent Owner has agreed to this construction in the co-pending related

litigation. Ex. 1008, 1-2 (showing that the agreed construction of this phrase is "wherein the bit is set to a value associated with permanent write protection").

Indeed, the specification discloses "setting said bit to have a certain predefined value that causes write protection command to mean permanent write protection." Ex. 1001, 2:12-16. Thus, the specification makes clear that the "predefined value" refers to the value of the bit after it has been set. Ex. 1006, ¶125. For example, the specification discloses embodiments where a bit is defined so that, when set, a command will result in permanent write protection of addressed memory segments. Ex. 1001, 2:55-62 (defining the PERM_WRITE_PROTECT bit of the CSD such that setting the bit protects groups protected with the SET_WRITE_PROT command), 3:9-30 (defining an unused CSD bit so that, when the bit is set, specified memory groups become permanently write protected), 3:52-57 (defining a PARTIAL_PERM_WP bit such that setting the bit makes write protection permanent). Ex. 1006, ¶125.

D. "wherein said at least one bit is reprogrammable"

Dependent Claim 3 recites, "wherein said at least one bit is reprogrammable." A POSA would have understood that the specification contemplates that a bit set to allow permanent write protection when a command is executed may have its value changed so that permanent write protection does not always occur. Ex. 1006, ¶129. Thus, a POSA would have recognized that phrase

to mean that the value of the at least one bit is changeable. *Id*., ¶¶127-29. Here, again, Patent Owner has agreed to this construction in the co-pending related litigation. Ex. 1008, 1-2 (showing that the agreed construction of this phrase is "wherein the at least one bit can be changed").

The specification states that in one embodiment of the invention, an unused bit in a data register can be defined "to indicate that a portion of the multimedia card 1 is permanently write protected." Ex. 1001, 3:8-12. The specification refers to that bit as "PARTIAL_PERM_WP." The specification describes how that bit can be set so that "groups protected with SET_WRITE_PROTECT command 5 (CMD28) become permanently write protected." The specification then explains the value of that bit can be changed. *Id*., 3:31-36; Ex. 1006, ¶128. In addition, the specification in Table 2 identifies the PARTIAL_PERM_WP bit as "R/W/E," which a POSA would understand refers to the bit as being readable, writable, and erasable (*i.e*., capable of being written multiple times, such that it is changeable). Ex. 1001, 3:43-48; Ex. 1004, 10:21-33; Ex. 1006, ¶128.

E. "memory group"

Challenged Claims 5, 6, and 13-15 recite a "memory group." A POSA would have recognized "memory group" to mean "a segment of memory." Ex. 1006, ¶¶130-32. Patent Owner also agreed to this construction in the co-pending

related litigation. Ex. 1008, 1-2 (showing that the agreed construction of this phrase is "a segment of memory").

The specification consistently discusses performing operations on segments of memory. Ex. 1006, ¶131. For example, the specification states that "the segment to be protected is defined in the units of WP_GRP_SIZE groups as specified in the CSD register. The write protection of the addressed write-protect group is then done using the SET_WRITE_PROT command." Ex. 1001, 1:58-62, 2:60-67 (reiterating that the segment size to be protected by the SET_WRITE_PROT command is identified in the unit of WP_GRP_SIZE groups), 3:61-63 ("The segments of the card that can be write protected are defined using WP_GRP_SIZE bits of CSD 2 as usual.").

The prosecution history further confirms that a "memory group" is "a segment of memory." Ex. 1006, ¶132. During prosecution, the applicant contrasted the recited "memory group" with the entire memory card, and equated the recited "memory group" with Toombs Publication's disclosure of a write-protected portion of memory. Ex. 1002, 39.

IX. A PERSON OF ORDINARY SKILL IN THE ART

A POSA with respect to the technology described in the '370 Patent would be a person with a bachelor's degree in electrical engineering or a closely related field, and two to three years of experience in the field of memory device circuit

design. Ex. 1006, ¶71. However, a higher level of education could make up for less experience, and vice versa. *Id*.

X. GROUND 1: CLAIMS 1-3, 5-6, 12-15, AND 25 ARE ANTICIPATED UNDER 35 U.S.C. §§ 102(a) AND (e) BY CHEVALLIER.

As described below, Chevallier anticipates Claims 1-3, 5-6, 12-15, and 25 of the '370 Patent under 35 U.S.C. § 102.

A. Independent Claim 1

1. A method comprising: write protecting at least one part of a memory by a command;

Chevallier discloses write protecting memory blocks of a flash memory "against unintended write operations." Ex. 1003, ¶0006. Chevallier discloses "memory blocks that are lockable in response to a lock command [corresponding to a lock function]." *Id*., ¶0008. Specifically, Chevallier discloses that "some of the memory blocks have already been temporarily locked with a lock command written to a lock command register." *Id*., ¶0036. Chevallier's disclosure of temporarily locking memory blocks with a lock command discloses "write protecting at least one part of a memory by a command," as recited in Claim 1. Ex. 1006, ¶¶147-49.

2. setting at least one bit in a data register configured to indicate that permanent write protection of the at least one part of the memory is allowed in order to redefine the command to allow permanent write protection, that cannot be un-protected by a command, of the at least one part of the memory;

Chevallier discloses a secure function that permanently secures "memory blocks specified in [a] control data word" "against write and erase operations." Ex. 1003, ¶0036. Chevallier's secure function is permanent because, while the "temporary lock function control can be cleared and the memory blocks erased or reprogrammed," "[t]he permanent secure function . . . cannot be cleared once it is set." Ex. 1003, ¶0016; Ex. 1006, ¶¶150-52.

Chevallier discloses that "the secure function is enabled by a nonvolatile secure function bit" (Ex. 1003, claim 19), which is "part of a control register in the memory device." Ex. 1003, ¶0039; Ex. 1006, ¶152. Chevallier discloses "writing a data word that has a '1' in a secure function bit position to [a] control register [to] enable the [secure] function" (*i.e.*, the permanent write protection function). Ex. 1003, ¶0039. Figure 5 of Chevallier illustrates a method for setting the secure function bit in order to enable the secure function and thus allow permanent write protection:

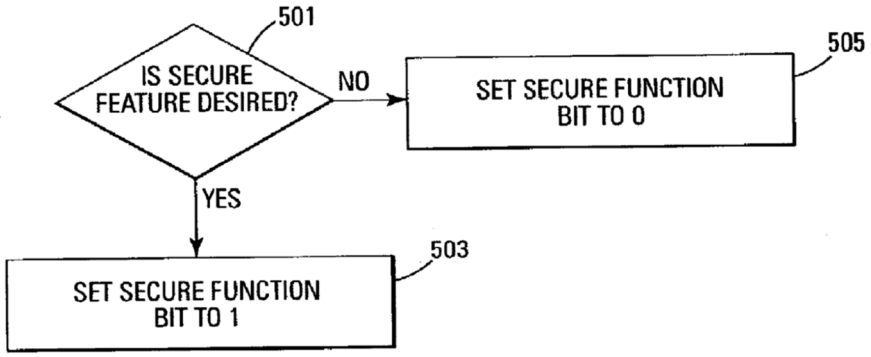

Fig. 5

Ex. 1003, FIG. 5, ¶0038; Ex. 1006, ¶¶151-52.

Chevallier also discloses "***to redefine the command to allow permanent write protection, that cannot be un-protected by a command***, of the at least one part of the memory." Ex. 1006, ¶¶153-57. As explained in Section VIII.B, "redefine the command to allow permanent write protection" would be interpreted by a POSA to mean to "cause a command that would not result in permanent write protection to result in permanent write protection."

Chevallier differentiates between the "regular (temporary) lock function and [the] permanent secure function of the memory device." Ex. 1003, ¶0016; Ex. 1006, ¶156. The "temporary lock function control can be cleared and the memory blocks erased or reprogrammed," while "[t]he permanent secure function of the present invention cannot be cleared once it is set." Ex. 1003, ¶0016. "If the secure command is written to the [memory device] along with the control data word, . . . those memory blocks specified in the control data word ***are permanently secured***

against write and erase operations." *Id*., ¶0036, Claim 18. Chevallier describes that "[t]he permanent secure function of the present invention is an added level of security in addition to the temporary block locking function of the prior art. The secure function overrides the temporary locking function." *Id*., ¶0029.

Chevallier discloses that, in one embodiment, the "secure command . . . is the same as the lock command." *Id*., ¶¶0008, 0020. Chevallier describes that, when serving as a lock command, this "same" command locks (*i.e*., temporarily write protects) a plurality of memory blocks of the memory device. Ex. 1003, ¶0008, Claim 18; Ex. 1006, ¶154. In this case, the "temporary lock function control can be cleared and the memory blocks erased or reprogrammed." Ex. 1003, ¶0016. However, Chevallier discloses that when the secure function bit is set, the "same" command "initiates the secure function" which permanently secures "memory blocks specified in [a] control data word" "against write and erase operations." Ex. 1003, ¶¶0008, 0033, 0036; Ex. 1006, ¶154.

Claims 18 and 19 of Chevallier disclose the "lock" command functioning as a "secure" command after enabling the secure function by the secure function bit. Ex. 1003, Claims 18-19; Ex. 1006, ¶155. In particular, Claim 18 recites "a plurality of lockable memory blocks" that are "temporarily lockable in response to a lock command." Ex. 1003, Claim 18. Claim 18 discloses the method involves "enabling a secure function," which Claim 19 discloses "is enabled by a non-

volatile secure function bit." *Id*., Claims 18-19. Claim 18 further discloses "submitting the lock command to the memory device to activate the secure function." *Id*., Claim 18.

In summary, Chevallier discloses that the lock command (temporary protection) and the secure command (permanent protection) may be the same command. Ex. 1006, ¶¶153-57. Setting the secure function causes the command to operate as the secure command, which, when executed, results in permanent write protection that is "permanently secured against write and erase operations." Ex. 1003, ¶0036; Ex. 1006, ¶¶153-57. Without enabling the secure function bit, the command provides only temporary write protection, not permanent write protection. Ex. 1003, ¶0036; Ex. 1006, ¶¶153-56.

Chevallier also discloses "to allow permanent write protection, that cannot be un-protected by a command, of the at least one part of the memory," as recited in this limitation of Claim 1. Ex. 1006, ¶¶158-60. Specifically, Chevallier discloses that the secure function allows permanent write protection of memory blocks that were previously temporarily write protected by the lock command. *Id*. ¶158. For example, Chevallier discloses that "some of the memory blocks have already been temporarily locked with a lock command written to a lock command register." Ex. 1003, ¶0036. However, "if the secure command is written to the unused address along with the control data word, as described above, the lock

function is overridden by the secure function and those memory blocks specified in the control data word ***are permanently secured against write and erase operations***." *Id*. (emphasis added).

Chevallier details permanently write protecting part of a memory by "set[ting] the command . . . for the secure function" in a first bus cycle and "set[ting] the particular memory blocks to be permanently disabled" in a second bus cycle. Ex. 1003, ¶0018; Ex. 1006, ¶159. This two-bus-cycle process is illustrated by Figure 1:

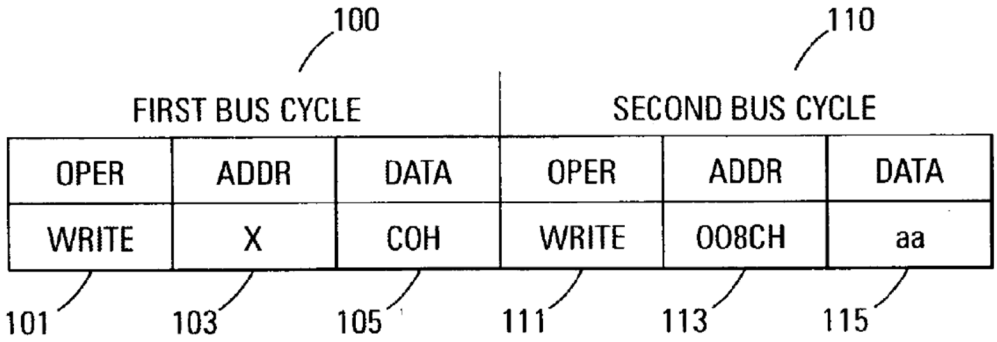

Fig. 1

Ex. 1003 at FIG. 1.

Chevallier discloses that "[t]he second bus cycle (110) performs a write (111) operation of a control data word (115) that indicates the memory block or blocks that are to be secured." Ex. 1003, ¶0021. The memory block or blocks indicated by the control data word constitute "at least one part of the memory," as recited. Ex. 1006, ¶160.

Thus, Chevallier discloses this claim limitation. Ex. 1006, ¶¶150-160.

3. executing the command in order to permanently write protect said at least one part of the memory.

As illustrated by Figure 1, above, Chevallier discloses permanently write protecting part of a memory by "set[ting] the command . . . for the secure function" in a first bus cycle and "set[ting] the particular memory blocks to be permanently disabled" in a second bus cycle. Ex. 1003, ¶0018; Ex. 1006, ¶¶161-63. Chevallier further teaches that "[i]f the secure command is written to the [memory device] along with the control data word, . . . those memory blocks specified in the control data word ***are permanently secured against write and erase operations***." Ex. 1003, ¶0036 (emphasis added), Claim 18.

B. Dependent Claim 2

1. A method according to the claim 1, wherein said at least one bit has a certain predefined value.

As explained in Section VIII.C, a POSA would interpret the phrase "wherein said at least one bit has a certain predefined value" to mean that the bit is set to a value associated with permanent write protection.

Chevallier describes "writing a data word that has a '1' in a secure function bit position to [a] control register [to] enable the [secure] function" (*i.e.*, to enable permanent write protection). Ex. 1003, ¶¶0038-0039, FIG. 5. In other words, when the secure function bit is set to "1," the secure function is enabled and

execution of the secure command permanently write protects part of a memory. Ex. 1006, ¶166. The value "1" of the secure function bit is therefore associated with permanent write protection. Ex. 1003, ¶¶0036, 0038-0039, FIG. 5; Ex. 1006 ¶166.

C. Dependent Claim 3

1. A method according to the claim 1, wherein said at least one bit is reprogrammable.

As explained in Section VIII.D, a POSA would have understood this element to mean that the value of the at least one bit is changeable.

Chevallier describes that the value of the secure function bit can be changed based on whether the secure function is desired. *See, e.g.*, Ex. 1003, ¶0037 ("If a customer desires to use the [secure] function for a particular implementation, the customer or the manufacturer can enable it. If the secure function is not required, the feature does not need to be enabled."), FIG. 5 (disclosing setting the secure bit to "0" if the secure function is not desired and to "1" if the secure function is desired), ¶0039; Ex. 1006, ¶169.

A POSA would recognize that, because Chevallier discloses a method for enabling and disabling the secure function bit by changing the bit's value and further discloses that the secure function can be enabled when a customer desires and disabled when the customer does not desire the function, then Chevallier discloses that the secure function bit is changeable (*i.e.*, so that the secure function

can be enabled or disabled, depending on the situation, to meet the customer's needs). Ex. 1006, ¶169. Thus, the secure function bit is reprogrammable. *Id*.

Further, Claim 19 of Chevallier teaches that "the secure function is enabled by a nonvolatile secure function bit." Ex. 1003, Claim 19. By specifying "nonvolatile," Claim 19 suggests that its antecedent independent claim 18 covers other possible implementations of the secure function. Ex. 1006, ¶170. As a volatile secure function bit is the only possible alternative to a non-volatile secure function bit, a POSA would have understood Claim 18 to encompass and inherently disclose a volatile implementation of the secure function bit. *Id*. A volatile bit only maintains its data when its device is powered; thus, a volatile secure function bit is necessarily changeable. *Id*.

D. Dependent Claim 5

1. A method according to claim 1, wherein said at least one part of the memory comprises at least one memory group having a certain memory size defined in the data register.

As explained in Section VIII.E, a POSA would have recognized "memory group" to mean "a segment of memory." Chevallier discloses all the limitations of Claim 5.

As illustrated by Figure 1, above, Chevallier discloses permanently write protecting part of a memory by "set[ting] the command . . . for the secure function" in a first bus cycle and "set[ting] the particular memory blocks to be permanently

disabled" in a second bus cycle. Ex. 1003, ¶0018; Ex. 1006, ¶173. Chevallier further teaches that, "[i]f the secure command is written to the [memory device] along with the control data word, . . . those memory blocks specified in the control data word are permanently secured against write and erase operations." Ex. 1003, ¶0036. Chevallier's memory blocks are segments of memory. Ex. 1006, ¶173.

Figure 2 illustrates how the control data word is used to "indicate which block or blocks of memory to permanently secure." Ex. 1003, ¶0022.

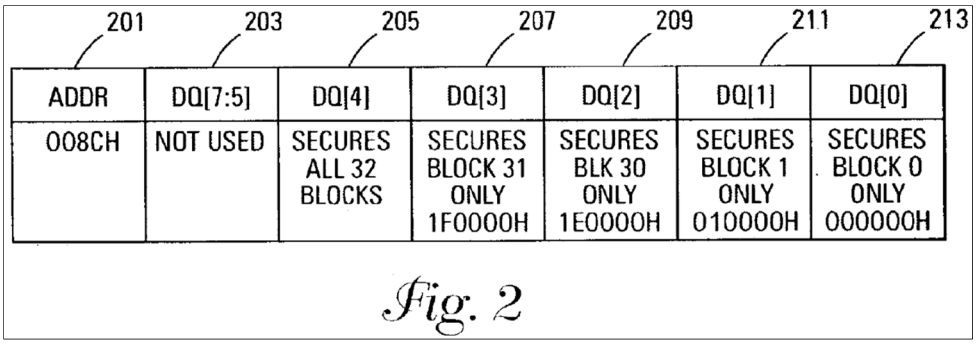

Fig. 2

Specifically, Chevallier discloses one embodiment in which "in order to secure the particular memory block represented by each control bit, a logic 0 is used in that particular control bit location." Ex. 1003, ¶0023. For example, "control bit DQ0 (213) secures memory block 0," while "memory block 1 . . . is represented by bit DQ1 (211)." *Id*., ¶¶0024-25. Memory blocks 30 and 31 may be represented by bit DQ2 (209) and DQ3 (207), respectively. *Id*. Chevallier discloses that "[a]lternate [sic] embodiments represent other memory blocks by the bits of the control data

word." *Id*., ¶0027. For example, Chevallier discloses using the unused control bits DQ5-7 (203) "to represent other memory blocks to secure." *Id*., ¶0026.

Chevallier discloses protecting any number of memory blocks by specifying in the control data word the corresponding combination of control bits. Ex. 1003, ¶0015 ("provid[ing] a permanent disablement of a write or erase operation to one or more memory blocks of a Flash memory device."); ¶0027 ("different combinations of bits in the control data word indicate different memory blocks."). Ex. 1006, ¶177. Thus, by specifying the number of memory blocks to be secured, Chevallier's control data word defines the size of the memory group to be secured. *Id*.

Chevallier teaches writing the control data word to the data register that has the secure function bit. Ex. 1006, ¶178. In particular, it teaches that "[t]he [secure] function bit may be part of a control register in the memory device." Ex. 1003, ¶0039. Chevallier also discloses that "[a]n array of control registers (680) store the secure command and the control data word of the present invention." *Id*., ¶0045. Chevallier's control register(s) can be interpreted to be a "data register" because they are a portion of memory containing information (*e.g*., the secure function bit and the memory blocks (size of memory) to secure) about Chevallier's memory card. *See* Section VIII.A, *supra*; Ex. 1006, ¶178.

Therefore, Chevallier discloses that the size of the permanently write protected part of the memory is defined by the memory blocks specified by the control data word written to the control register, as recited. Ex. 1006, ¶¶172-179.

E. Dependent Claim 6

1. A method according to claim 5, wherein redefining the command allows permanent write protection of each memory group individually.

As explained in Section X.D, immediately above, Chevallier discloses permanently write protecting part of a memory by "set[ting] the command . . . for the secure function" in a first bus cycle and setting a control data word specifying "the particular memory blocks to be permanently disabled" in a second bus cycle. Ex. 1003, ¶0018, ¶0036; Ex. 1006, ¶182. Chevallier further discloses an embodiment that assigns each memory block a control bit that designates whether that memory block will be secured. Ex. 1006, ¶¶182-183. Specifically, "[i]n order to secure the particular memory block represented by each control bit, a logic 0 is used in that particular control bit location." Ex. 1003 ¶0023, FIG. 2. Figure 2 further illustrates that each control bit secures only the individual memory block to which it is assigned. Ex. 1006, ¶¶182-183. Chevallier therefore discloses that each of memory blocks can be individually write protected by specifying the appropriate corresponding control bit in the control data word. *Id*., ¶¶181-84.

F. Independent Claim 12

1. An apparatus comprising: an interface controller arranged to write protect at least one part of a memory of said apparatus by a command;

Chevallier discloses incorporating a flash memory device in portable computers, personal digital assistants (PDAs), digital cameras, and cellular telephones. Ex. 1003, ¶0004. Figure 6 of Chevallier illustrates a memory device 600 interfacing with a host processor 610. A POSA would have considered memory device 600, either with or without host processor 610, to be an apparatus. Ex. 1006, ¶186.

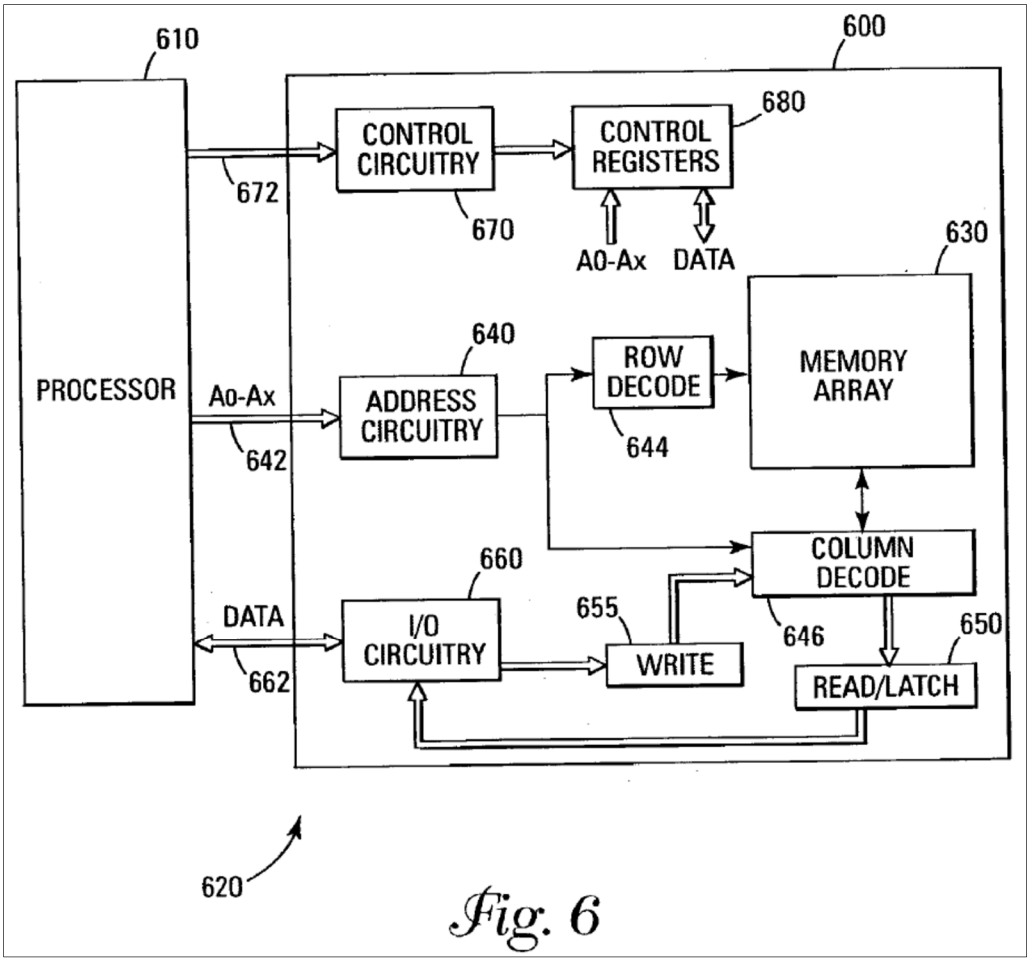

Fig. 6

As illustrated by Figure 6, Chevallier discloses the memory device (600) "includ[ing] an array of memory cells (630)." Ex. 1003, ¶0041. Chevallier also discloses that the memory device (600) includes a "[c]ommand control circuit (670) [that] decodes signals provided on control connections (672) from the processor (610)" and that the "signals are used to control the operations on the memory array (630), including data read, data write, and erase operations." *Id*., ¶0044. Figure 6 of Chevallier illustrates control circuitry 670 interfacing with an array of control registers 680. According to Chevallier, an array of control

registers 680 "store the secure command and the control data word" and can be "programmed with the appropriate secure command and control data word." *Id*., ¶0045. The secure command can be written to the control circuitry of the memory device (*Id*., ¶¶19, 33), and the control data word can be written to an unused memory address in the control register (*Id*., ¶¶21, 34, Claim 12). The secure command and control data word can be written to the same unused address. *Id*., ¶21. The lock command is also written to a control register. *Id*., Claims 4, 9. Lastly, the secure function bit can be stored in the control register and can be changed by writing the appropriate data word to the secure function bit position in the register. *Id*., ¶39; Ex. 1006 ¶188.

The '370 Patent states that its "interface controller" "handles the accesses according to the address sent be [sic] the host 6." Ex. 1001, 5:13-15. A POSA would recognize that an "interface controller" would include Chevallier's command control circuitry; control circuitry, address circuitry, and I/O circuitry interfacing with the host; the processor; or any combination thereof. Ex. 1006, ¶189.

A POSA would therefore understand that Chevallier discloses: (1) control circuitry that writes a lock command and/or secure command to a memory address in a control register; and (2) a processor that writes via control connections a lock command and/or secure command to the control circuitry. Ex. 1006, ¶191. As

explained above in Sections X.A.1 and X.A.2, the lock command and secure command provide temporary and permanent write protection, respectively.

Thus, Chevallier discloses this limitation. *Id*., ¶¶186-91.

2. a data register arranged to define at least one bit to indicate that permanent write protection of the at least one part of the memory is allowed;

As explained above in Section X.A.2, Chevallier's control register is a data register that contains the secure function bit, which enables the secure function and thus indicates that permanent write protection of at least one part of Chevallier's memory is allowed. Ex. 1006, ¶¶151-52,192-95.

3. a controller arranged to set the at least one bit in order to redefine the command to allow permanent write protection that cannot be un-protected by a command, of the at least one part of the memory of said apparatus;

As shown above in Section X.F.1, Chevallier discloses a control circuitry that writes to a control register, and further that the control register stores a secure function bit set by writing the appropriate data word to that bit. Ex. 1006, ¶¶188-89, 191, 197-98. As shown above in Section X.A.2, Chevallier discloses the recited "one bit." *Id*., ¶¶150-60, 199-205.

4. the controller arranged to execute the command in order to permanently write protect said at least one part of the memory.

As shown above in Section X.F.1, Chevallier discloses: (1) control circuitry that writes a secure command to a memory address in a control register; and (2) a

processor that writes via control connections a secure command to the control circuitry. Ex. 1006, ¶¶188-89, 191, 207. As shown above in Section X.A.3, Chevallier discloses that writing the secure command permanently write protects the memory identified by the control data word. *Id*., ¶¶161-63, 208-09.

G. Dependent Claim 13

1. An apparatus according to claim 12, wherein the memory is arranged to comprise at least one memory group.

As shown above in Section X.D, Chevallier's memory is arranged to comprise at least one memory group. Ex. 1006, ¶¶172-79, 211-16.

H. Dependent Claim 14

1. An apparatus according to claim 13, wherein the data register is arranged to define a memory size of the at least one memory group.

As shown above in Section X.D, Chevallier's data register defines the size of Chevallier's memory groups. Ex. 1006, ¶¶172-79, 218-21.

I. Dependent Claim 15

1. An apparatus according to claim 14, wherein the controller is arranged to define the command to allow permanent write protection of the at least one memory group individually.

As shown above in Section X.F.1, Chevallier discloses a control circuitry that writes a control data word to a control register. Ex. 1006, ¶¶188-89, 191, 224. As explained above in Section X.D, the control data word specifies permanent

write protection of memory groups individually or in combination. *Id*., ¶¶172-79, 224-29.

J. Independent Claim 25

1. A memory device having stored thereon instructions that, when executed, perform:

Chevallier discloses a memory device, which is a flash memory device in at least one embodiment (Ex. 1003, ¶0002, FIG. 6), and also discloses commercial devices (portable computers, personal digital assistants (PDAs), digital cameras, and cellular telephones) incorporating memory that could each be considered a "memory device." Ex. 1003, ¶0004; Ex. 1006, ¶239.

Chevallier teaches that "program code, system data such as a basic input/output system (BIOS), and other firmware can typically be stored in Flash memory." Ex. 1003, ¶0004. A POSA would have understood that Chevallier's disclosure of a flash memory device storing program code and firmware teaches "[a] memory device having stored thereon instructions." Ex. 1006, ¶239.

Further, a POSA would have understood that at least part of the program code or firmware stored on the flash memory device would have stored the instructions necessary to perform the functions Chevallier describes corresponding to elements (2)-(4), below. *Id*. In addition, a POSA would have understood that Chevallier's memory device would necessarily have had to execute instructions to perform the functionality Chevallier discloses, and that an operational memory

device would necessarily have stored such instructions, whether a program code, in firmware, or in a state machine implemented as an application-specific integrated circuit (ASIC). *Id*.

2. write protecting at least one part of a memory by a command;

As explained above in Section X.A.1, Chevallier discloses this limitation. Ex. 1006, ¶¶149-56, 158-60, 241.

3. setting at least one bit in a data register configured to indicate that permanent write protection of the at least one part of the memory is allowed in order to redefine the command to allow permanent write protection, that cannot be unprotected by a command, of the at least one part of the memory; and

As explained above in Section X.A.2, Chevallier discloses this limitation. Ex. 1006, ¶¶149-56, 158-60, 242-52.

4. executing the command in order to permanently write protect said at least one part of the memory.

As explained above in Section X.A.3, Chevallier discloses this limitation. Ex. 1006, ¶¶161-63, 253-55.

XI. GROUND 2: CLAIMS 1-3, 5-6, 12-15, AND 25 ARE OBVIOUS UNDER 35 U.S.C. § 103 OVER CHEVALLIER IN VIEW OF THE KNOWLEDGE OF A POSA.

Chevallier anticipates Claims 1-3, 5-6, 12-15, and 25, as shown above in Ground 1 (Section X). In particular, the above analysis shows that there is no meaningful difference between the scope of the prior art and the limitations of

Claims 1-3, 5-6, 12-15, and 25 of the '370 Patent, especially considering the level of skill in the relevant art. Further, Petitioner is unaware of any secondary considerations of non-obviousness that would change this conclusion.[2] Therefore, Chevallier renders Claims 1-3, 5-6, 12-15, and 25 obvious, in addition and in the alternative to anticipating those claims. *See, e.g.*, *Schrader-Bridgeport Int'l, et al. v. Wasica Finance GMBH et al*., Case No. IPR2014-00476, Paper 30 at 23-24 (PTAB July 22, 2015) (finding that a single prior are reference that anticipated challenged claims also rendered those claims obvious, "[b]ecause anticipation is the epitome of obviousness, a disclosure that anticipates under 35 U.S.C. § 102 also renders the claim unpatentable under 35 U.S.C. § 103.") (citing *In re Fracalossi*, 681 F.2d 792, 794 (CCPA 1982); *In re Meyer*, 599 F.2d 1026, 1031 (CCPA 1979); *In re Pearson*, 494 F.2d 1399, 1402 (CCPA 1974)).

A. Independent Claims 1, 12, and 25

To the extent that Chevallier does not explicitly recite that the "secure function bit" is set in order to "redefine" the lock command to become the (permanent) secure command, as recited in Claims 1, 12, and 25, it would be

[2] If Patent Owner alleges that any secondary considerations support the non-obviousness of the Challenged Claims, which is its burden, then Petitioner reserves the right to submit rebuttal evidence and argument under 37 C.F.R. § 42.108(c).

obvious to use the bit in that manner, for example, to eliminate any ambiguity as to whether the command meant "lock" or "secure." Ex. 1006, ¶¶259, 270, 276.

As shown above in Section X.A.1-2, Chevallier describes that a lock command used for temporary write protection and a secure command used for permanent write protection may be the same command. *Id*., ¶¶153-57, 259, 270, 276. A POSA would have understood that when the lock function and the secure function result from the same command, it would be beneficial to unambiguously specify which function results from execution of the command. *Id*., ¶¶259, 270, 276. A POSA would understand that Chevallier's secure function bit, which enables and disables the secure function, could provide the beneficial specificity—if the secure function is not enabled, then the command results in the lock function; if the bit is enabled, then the command results in the secure function. *Id*.

B. Dependent Claim 3

1. "Wherein said at least one bit is reprogrammable"

To the extent that Chevallier does not disclose that the secure function bit was reprogrammable, as recited, it would have been an obvious matter of design choice to implement the register address for the secure function bit to be reprogrammable. Ex. 1006, ¶262. Further, it would have been obvious to try implementing a reprogrammable secure function bit given the small number of options (*i.e*., reprogrammable or not reprogrammable). *Id*., ¶262.

In addition, a POSA would have been motivated to implement the secure function bit to be reprogrammable rather than non-reprogrammable to ensure flexibility of the device. *Id*., ¶263. As shown above in Sections X.A.2 and XI.A, Chevallier discloses that the secure function bit determines whether temporary or permanent write protection occurs. *Id*., ¶263. A POSA would have understood that it is beneficial for a memory device to sometimes apply temporary write protection and other times apply permanent write protection. *Id*., ¶263. Notably, Chevallier discloses providing such flexibility to a user. *Id*., ¶264; *see* Ex. 1003, ¶0037 ("If a customer desires to use the function for a particular implementation, the customer or the manufacturer can enable it. If the secure function is not required, the feature does not need to be enabled."). A POSA would have recognized that by making the secure function bit changeable, a user could enable the secure function when it is desired and disable it when it is not. Ex. 1006, ¶264. In fact, Chevallier provides a method for doing just that. Ex. 1003, FIG. 5, ¶0038; Ex. 1006, ¶264. A POSA would have found it obvious to implement the memory device of Chevallier in a way such that the customer can use the method illustrated by Figure 5 as desired to switch between permanent and temporary write protection. Ex. 1006, ¶264.

In addition, if the secure function bit was made non-reprogrammable, setting the secure function bit would render inaccessible Chevallier's temporary lock function when the lock and secure commands are the same. *Id*., ¶263.

C. Dependent Claims 5 and 14

1. "at least one memory group having a certain memory size defined in the data register"/ "data register…define[s] a memory size"

As shown above in Section X.D, Chevallier discloses a memory based on a block architecture and protecting blocks of the memory specified by a control data word, where the memory blocks are located at particular memory addresses. Ex. 1006, ¶¶172-79, 267, 273. A POSA would have understood that securing specific memory block as Chevallier discloses requires information about the structure of the memory, including the size of each memory block. *Id*., ¶¶267, 273.

In addition, it was known that the size of each memory block may be directly stored in the control register or indirectly indicated by addresses of the memory blocks stored in the control register, and storing memory size information in one memory location versus another memory location was simply a routine design choice. *Id*. It would therefore have been obvious to define the size of the memory group to be secured in a register. *Id*.

D. Dependent Claims 2, 6, 13, and 15

Each of these claims depends from at least one claim that this section shows is obvious over Chevallier in view of the knowledge of a POSA. Section X shows that Chevallier expressly discloses the limitations recited by these claims. Thus, Chevallier renders these claims obvious.

XII. GROUND 3: CLAIMS 1-3, 5-7, 12-15, 19, AND 25 ARE OBVIOUS UNDER 35 U.S.C. § 103 OVER CHEVALLIER IN VIEW OF TOOMBS.

As shown above in Ground 1 (Section X), Chevallier discloses all of the elements of Claims 1-3, 5, 6, 12-15 and 25. In addition, those claims—as well as Claims 7 and 19 (*i.e.*, all Challenged Claims)—are obvious over Chevallier and Toombs, as explained below with reference to particular claim elements.

A. Independent Claim 1

1. "Setting at least one bit in order to redefine the command to allow permanent write protection that cannot be unprotected by a command"

Toombs discloses register fields that provide supplemental information controlling the meaning of particular commands (*i.e.*, redefining those commands). Ex. 1006, ¶280. For example, Toombs discloses a WP_GRP_ENABLE bit in the CSD register that "is used to indicate whether the write protection group is enabled." Ex. 1004, 12:25-28. A SET_WRITE_PROT command can be used to "set[] the write protection of [] addressed write-protect group" only if the WP_GRP_ENABLE bit is set to 1 in the CSD register. *Id.*, 30:3-12. As another

example, a READ_BL_LEN field in the CSD register controls the maximum size of a block of data that can be read using a command READ_SINGLE_BLOCK command. *Id*., 20:5-17.

Toombs also discloses a PERM_WRITE_PROTECT bit that, when set, permanently protects the memory card such that "all write and erase commands for this card are permanently disabled." Ex. 1004, 12:56-61. Toombs' permanent write protection thus cannot be cleared by a command, such as Toombs' CLR_WRITE_PROT command that clears temporary write protection. Ex. 1004, 30:8-12; Ex. 1006, ¶282.

Motivation to Combine and Resulting System / Method

It would have been obvious to a POSA to apply Toombs' technique of using register bits to control a command's functionality to Chevallier's system, wherein a single lock/secure command can have two different functions, in order to control the meaning/functionality of the lock/secure command. Ex. 1006, ¶283; *see* Section X.A.2. A POSA would have understood that it is necessary to unambiguously specify, whenever the command is executed, which of the two functions is to be initiated. *Id*. This would motivate a POSA to combine the teachings of Chevallier and Toombs to solve this problem and use the existing secure function bit in Chevallier to control the meaning of the lock/secure command. *Id*.

It would also have been obvious to a POSA to implement Chevallier's secure function bit and secure/lock command in the memory card of Toombs. Ex. 1006, ¶285. For example, a POSA would have been motivated to introduce the lock/secure function of Chevallier to Toombs in order to provide the memory card of Toombs with the additional functionality of flexibly invoking permanent write protection of Chevallier, and a POSA would have further been motivated to store Chevallier's secure function bit for controlling that command in Toombs' data structure storing information command functionality, *e.g.*, the CSD register, to keep such information organized in one data structure. *Id*.

This combination would also yield a predictable result—*i.e.*, that the command initiates the secure function when the binary secure function bit is set to enable the secure function, and the command initiates the lock function when the secure function bit is set to disable the secure function. *Id*.

2. "a data register"

Toombs discloses that "each of the cards of the MultiMediaCard system comprises a group of registers for storing a variety of status and internal information." Ex. 1004, 9:46-48. This corresponds with the claimed "data register." Toombs discloses an embodiment in which the information is stored in five registers, including OCR, CID, CSD, RCA, and DSR. *Id*., 9:51-53. In particular, Toombs teaches that "[t]he CSD register is responsible for providing

information to the MultiMediaCard host on how to access the card content" and that "the CSD register stores values defining the data format . . . data transfer speed . . . etc." *Id*., 10:24-29. Toombs discloses an embodiment where the CSD register contains information about the card's write protection, including the WP_GRP_ENABLE bit that enables the SET_WRITE_PROT function, and also including the PERM_WRITE_PROTECT and TMP_WRITE_PROTECT bits. *Id*., FIG. 17B, 12:56-67, 30:1-12.

It would also have been obvious to a POSA to implement Chevallier's secure function bit using the CSD of Toombs, as explained immediately above. *See* Section XII.A.1; Ex. 1006, ¶285.

B. Dependent Claim 2

Chevallier discloses all the limitations of Claim 2. *See* Section X.B; Ex. 1006, ¶287.

C. Dependent Claim 3

1. "Wherein said at least one bit is reprogrammable"

Toombs discloses a TMP_WRITE_PROTECT field in the CSD register that "temporarily protects the whole card content against overwriting or erasing (all write and erase commands for this card are permanently disabled)" and that "***can be set and reset***." Ex. 1004, 12:62-66 (emphasis added). Here, setting the TMP_WRITE_PROTECT bit applies temporary write protection because the

TMP_WRITE_PROTECT field can be reset by a user. Ex. 1006, ¶289. This register field is illustrated below:

NAME	FIELD	WIDTH	CELL TYPE	CSD-SLICE
MAX. WRITE CURRENT @V_{DD} MIN	VDD_W_CURR_MIN	3	R	[55:53]
MAX. WRITE CURRENT @V_{DD} MAX	VDD_W_CURR_MAX	3	R	[52:50]
MAX. V_{PP} CURRENT	VPP_CURR	3	R	[49:47]
ERASE SECTOR SIZE	SECTOR_SIZE	5	R	[46:42]
ERASE GROUP SIZE	ERASE_GRP_SIZE	5	R	[41:37]
WRITE PROTECT GROUP SIZE	WP_GRP_SIZE	5	R	[36:32]
WRITE PROTECT GROUP ENABLE	WP_GRP_ENABLE	1	R	[31:31]
MANUFACTURER DEFAULT ECC	DEFAULT_ECC	2	R	[30:29]
STREAM WRITE SPEED FACTOR	R2W_FACTOR	3	R	[28:26]
MAX. WRITE DATA BLOCK LENGTH	WRITE_BL_LEN	4	R	[25:22]
PARTIAL BLOCKS FOR WRITE ALLOWED	WRITE_BL_PARTIAL	1	R	[21:21]
RESERVED	-	5	R	[20:16]
RESERVED	-	3	R/W	[15:13]
COPY FLAG (OTP)	COPY	1	R/W	[12:12]
PERMANENT WRITE PROTECTION	PERM_WRITE_PROTECT	1	R/W	[11:11]
TEMPORARY WRITE PROTECTION	TMP_WRITE_PROTECT	1	R/W/E	[10:10]
ECC CODE	ECC	2	R/W/E	[9:8]
CRC	CRC	7	R/W/E	[7:1]
NOT USED, ALWAYS '1'	-	1	-	[0-0]

FIG. 17B

Ex. 1004, FIG. 17B (highlighting added).

The TMP_WRITE_PROTECT field is marked "R/W/E," which indicates that the field is readable, writable, and erasable (multiple writable). Ex. 1004, 10:29-32. Toombs thus teaches using a reprogrammable register field to enable or disable write protection for an entire memory. *Id*.

Motivation to Combine and Resulting System / Method

It would have been obvious to a POSA to combine the teachings of Toombs and Chevallier to make the secure function bit disclosed by Chevallier erasable. Ex. 1006, ¶291. Such a combination would have been a routine design choice to allow a user to flexibly choose whether to temporarily or permanently write protect part of the memory by controlling the value of the secure function bit. *Id*.

Indeed, Chevallier discloses providing such flexibility to a user. *Id*.; Ex. 1003, ¶0037. In addition, a POSA would have been motivated to introduce the R/W/E feature from Toombs to Chevallier as one way to implement Chevallier's method of Figure 5, *i.e*., to enable and disable the secure function as desired. Ex. 1006, ¶291. Lastly, introducing the known R/W/E feature disclosed in Toombs to the secure function bit of Chevallier would have the predictable result of making Chevallier's secure function bit also R/W/E. *Id*.

Alternatively, a POSA would have been motivated to improve the functionality of permanently write protecting an entire memory using the reprogrammable TMP_WRITE_PROTECT bit, as disclosed in Toombs, by using this bit in conjunction with the control data word, as disclosed in Chevallier. Ex. 1006, ¶292. This control data word may be written in one or more unused addresses in the CSD register or another suitable register. *Id*. Chevallier suggests making this improvement by stating that the block architecture of "[n]ewer

memory devices" "allows the file system to erase blocks of Flash memory instead of the entire device" and that "critical system code can be stored in a lockable block of memory while other blocks are allocated to other portions of code or data." Ex. 1003, ¶0005; Ex. 1006, ¶292. This combination would allow a user to specify a particular portion of the memory (*e.g.*, critical system code, data necessary for the operation of an application, or important records) to permanently write protect while keeping other portions (*e.g.*, system data that can be updated or user files that are overwritten, such as drafts of documents) available for writing. Ex. 1006, ¶292.

D. Dependent Claim 4

1. "Wherein executing the command clears automatically said at least one bit"

Toombs discloses erasing data stored in memory groups by first tagging each group to be erased and then using one command to erase all tagged groups. Ex. 1004, 28:10-25; Ex. 1006, ¶296. According to Toombs "[a]ll tag bits are cleared by each command except a tag or untag command." Ex. 1004, 28:37-39. Toombs therefore discloses setting one or more bits (*e.g.*, group tags) to specify a functionality of a command (*e.g.*, particular memory groups to be erased by the erase command) and executing the command, which automatically clears the one or more bits. Ex. 1006, ¶296. Toombs further discloses "issuing [a] status

command [] to read [] bits" in a status register and that some of the bits are cleared after "reception of a valid command." Ex. 1004, 24:55-25:6.

Motivation to Combine and Resulting System / Method

It would have been obvious to a POSA to combine the feature where a command automatically clears related register bits, as disclosed in Toombs, with the use of the secure function bit to specify the meaning of the lock/secure command, as disclosed in Chevallier, such that executing the secure command automatically clears the secure function bit. Ex. 1006, ¶297. A POSA would have been motivated to do so to avoid inadvertently and permanently securing part of the memory following a permanent secure command (*e.g.*, where the next secure command was intended to only be temporary). *Id*. In fact, Chevallier recognizes that inadvertent securing of blocks is a problem to be avoided. Ex. 1003, ¶0035 ("It is desirable to use a voltage so that the memory blocks cannot be inadvertently secured."); Ex. 1006, ¶297. Toombs also teaches that irreversible write protection is not always desirable, as Toombs discloses both a permanent write protection function and a temporary write protection function. Ex. 1004, 12:56-67; Ex. 1006, ¶297.

E. Dependent Claims 5, 13, and 14

1. "At least one part of the memory comprises a memory group having a certain memory size defined in the data register" / "wherein the memory is arranged to comprise at least one memory group" / "wherein the data register is arranged to define a memory size of the at least one memory group"

The '370 Patent acknowledges that the concept of a "memory group having a certain memory size" is known to a POSA. Ex. 1006, ¶300, 332. The '370 Patent states that "the segment size to be protected is defined in the units of WP_GRP_SIZE groups as specified in the CSD . . . register" and that "[t]he write protection of the addressed write-protect group is then done[.]" Ex. 1001, 1:58-62.

Toombs discloses a MMC card comprising memory groups:

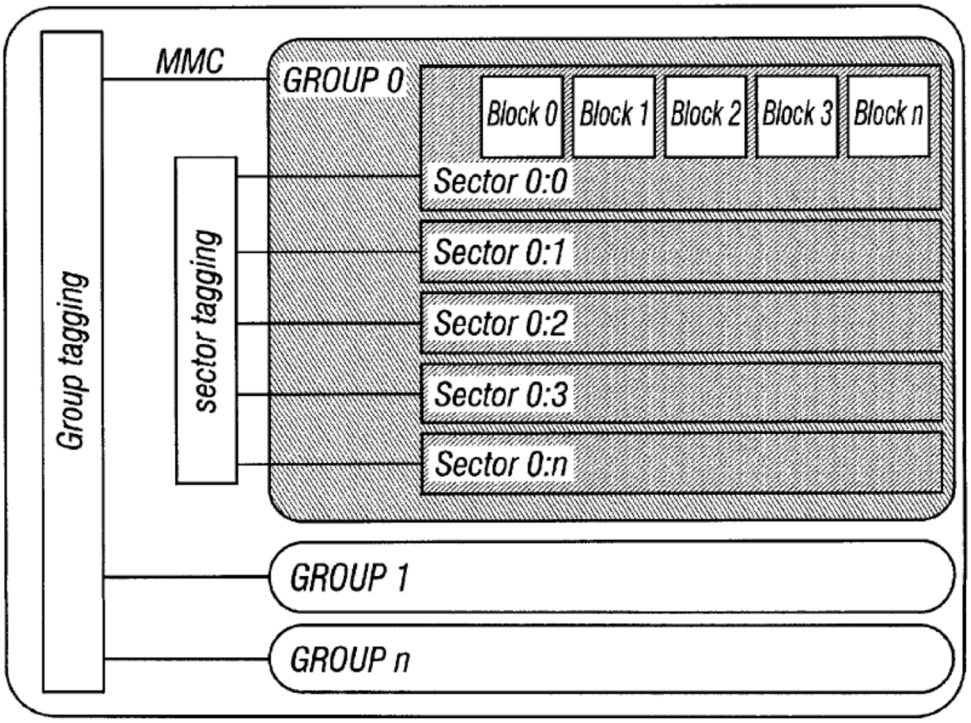

FIG. 66

Ex. 1004, FIG. 66.

According to Toombs, "the MultiMediaCard card is divided into n memory groups." *Id*., 27:37-38. "Each of the memory groups is subdivided into a plurality of sectors." *Id*., 27:38-39. "Further, each of the sector [sic] comprises of a plurality of memory blocks." *Id*., 27:39-40. Toombs further discloses that "the group size is a configurable parameter" and that "[t]he actual size is stored in the CSD register." *Id*., 27:57-60.

Toombs also discloses write protection being "applied to memory groups." *Id*., 29:45-46. Toombs shows a memory hierarchy for a write protection mechanism:

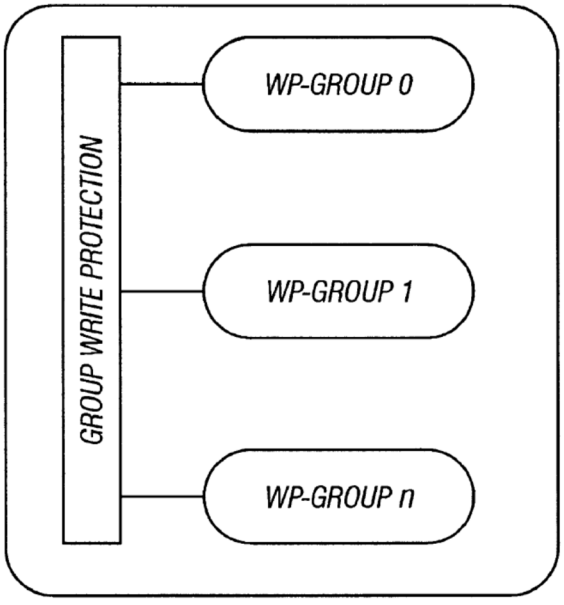

FIG. 69

Id., FIG. 69. Toombs explains: "[t]he WP-Group is the minimal unit which may have individual write protection" and that "[i]ts size is the number of groups which will be write protected by one bit." *Id*., 29:58-60. Toombs further discloses that "[t]he size of a WP-group is a configurable parameter" and that "the actual size [of a WP-group] is stored in the CSD register." *Id*., 29:60-62. According to Toombs, "[f]or cards which support write protection of groups of sectors . . . portions of the data may be protected (in units of WP_GRP_SIZE sectors as specified in the CSD)." *Id*., 30:3-7.

Motivation to Combine and Resulting System / Method

It would have been obvious to a POSA to combine the memory hierarchy of Toombs with the use of register bits to define the meaning of a write protection command of Chevallier to achieve permanent write protection of memory groups. Ex. 1006, ¶305, 335. A POSA would have been motivated to do so because the introduction of Toombs' memory hierarchy to Chevallier would reduce the number of bits in Chevallier's control register required to specify each portion of the memory to protect. *Id*., ¶306, 336. For example, for the memory illustrated by Figure 2 of Chevallier, which comprises thirty-two memory blocks, specifying each part of the memory to write protect would require a control data word comprising at least thirty-two bits, each corresponding to one memory block. *Id*. On the other hand, if for example the thirty-two memory blocks are grouped into

four memory groups each comprising eight memory blocks, the control data word would only need to be four-bits long to specify all possible combinations of the groups. *Id*.

Alternatively, a POSA would have been motivated to improve Toombs' teaching of write protecting memory groups with Chevallier's disclosure of using a register bit to redefine a command so that the command applies permanent write protection to specified memory groups. Ex. 1006, ¶307, 337. The secure function bit, as disclosed by Chevallier, may be placed in one or more unused addresses of the CSD register of Toombs or another suitable register. *Id*. The resulting combination would introduce the permanent write protection of Chevallier to the memory groups and their size definitions specified in the CSD of Toombs. *Id*. In addition, the combination would achieve permanent write protection of specified memory groups rather than of an entire card. *Id*.

Lastly, it would have been obvious to a POSA to store the secure function bit and the size of the memory group to be write protected in the same register. Ex. 1006, ¶308, 338. That data relates to the memory to be write protected, and thus it would be an obvious design choice to store the same type of data in the same register. *Id*. It would also provide the benefit of keeping information about write protection organized in the same data structure. *Id*. In fact, both Chevallier and Toombs suggest storing write-protection information and memory-size information

in the same register (*e.g.*, Ex. 1003, ¶0039, Claim 4; Ex. 1004, FIG. 17B, 2:50-51). Ex. 1006, ¶308, 338.

F. Dependent Claim 6

1. "Wherein redefining the command allows permanent write protection of each memory group individually"

Toombs discloses dividing a memory into memory groups. Section XII.E (immediately above); Ex. 1006, ¶¶301-04, 311. Toombs teaches "a method of providing write protection to any combination of memory groups and sectors in the MultiMediaCard system." Ex. 1004, 1:57-59. Toombs further discloses that "[e]ach WP-group has an additional write protection bit," which "can be programmed via special commands." *Id*., 29:65-67. The "special command[]" is a SET_WRITE_PROT command, which "sets the write protection of the addressed write-protect group." *Id*., 30:9-10. Toombs therefore discloses temporarily write protecting each memory group individually. Ex. 1006, ¶311.

Motivation to Combine and Resulting System / Method

As shown immediately above in Section XII.E, a POSA would have been motivated to improve the system disclosed in Chevallier with the group-based memory hierarchy disclosed in Toombs or to introduce to Toombs' system the ability to permanently write protect individual memory groups. Ex. 1006, ¶¶306, 312. Further, a POSA would have been motivated to combine Chevallier and

Toombs in order to allow a user to selectively identify which memory groups to permanently write protect. *Id*., ¶307, 312.

G. Dependent Claim 7

1. "A method according to claim 1, wherein the memory is included on a multimedia card (MMC)."

Toombs shows a MMC bus system with MMC cards:

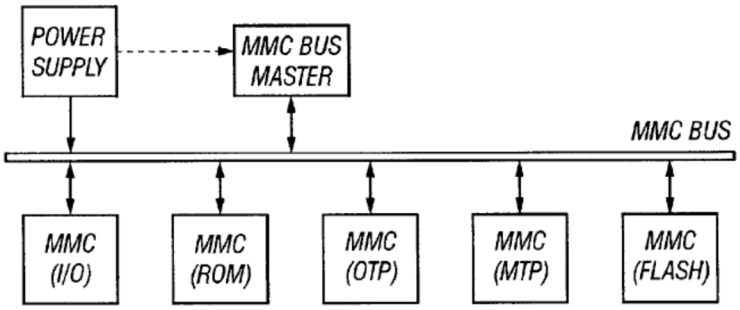

FIG. 4

Ex. 1004, FIG. 4.

According to Toombs, "the MultiMediaCard bus connects the MultiMediaCard cards each comprising various solid-state mass storage devices, or I/O devices." *Id*., 6:61-65. Toombs discloses "allow[ing] the MultiMediaCard card to write protect any combination of groups of the memory." *Id*., 29:40-42.

Chevallier contemplates flash memory devices. Ex. 1003, ¶0002. As Toombs discloses, a MMC can comprise flash memory. Ex. 1006, ¶318.

Motivation to Combine and Resulting System / Method

A POSA would have found it obvious to include the flash memory of Chevallier in a MMC form factor disclosed by Toombs. *Id*. A POSA would be

motivated to include the flash memory in a memory card compliant with the MMC standard since such cards are in demand for various consumer applications such as "PDAs, cameras, smart phones[.]" Ex. 1004, 1:20-23; Ex. 1006, ¶318. Indeed, Chevallier also identifies "[c]ommon uses for Flash memory" including "(PDAs), digital cameras, and cellular telephones." Ex. 1003, ¶0004; Ex. 1006, ¶318. The teachings of Chevallier and Toombs would yield the predictable result of: (1) the flash memory of Toomb's MMC being permanently write protectable; and (2) Chevallier's memory device being part of a MMC. Ex. 1006, ¶318. Moreover, a MMC including flash memory provides the benefit of allowing "software and data [to] be preloaded and changed by the [] host." Ex. 1004, 1:31-33; Ex. 1006, ¶318.

H. Independent Claim 12

Toombs discloses an interface controller that interfaces with an MMC's data registers, memory core, and a host. *Compare* Ex. 1004, Fig. 3 and Ex. 1001, Fig. 1; Ex. 1006, ¶188.

1. "An interface controller arranged to write protect at least one part of a memory of said apparatus by a command"

Toombs' interface controller processes the commands executable on Toombs' MMC (which are sent by a host over a CMD line), including write protect commands. Ex. 1004, Fig. 4 (CMD 28), 23:46-51, 30:8-12 (SET_WRITE_PROT command); Ex. 1006, ¶322.

Motivation to Combine and Resulting System / Method

A POSA would have been motivated to introduce Toombs' interface controller to the memory device of Chevallier in order to have a built-in controller that could interface with a host and execute Chevallier's write protection commands (*i.e*., the lock command and secure command). Ex. 1006, ¶322.

In addition, introducing Toombs' interface controller to Chevallier's memory device would have had the predictable result of a controller that interfaces with a host to process commands for performing functions on an array of memory. Ex. 1003, ¶0044, Fig. 6; Ex. 1006, ¶322.

2. "A controller arranged to set the at least one bit in order to redefine the command to allow permanent write protection that cannot be un-protected by a command, of the at least one part of the memory of said apparatus"

The data registers of Toombs (specifically, the CSD register) contain the bit(s) controlling permanent and temporary write protection of the MMC. Ex. 1004, Figs. 17A-B, 10:1-4, 12:56-67 (PERM_WRITE_PROTECT and TMP_WRITE_PROTECT bits); Ex. 1006, ¶323. A POSA would have recognized that Figure 14 of Toombs illustrates that the MMC interface controller is the only controller that interfaces with the CSD, and thus the interface controller necessarily sets the bits related to write protection. Ex. 1006, ¶324.

Motivation to Combine and Resulting System / Method

A POSA would have been motivated to introduce Toombs' interface controller to the memory device of Chevallier in order to have a built-in controller that could interface with a host and set Chevallier's secure function bit (*i.e.*, execute the steps of Chevallier's method in Figure 5). *Id*., ¶323. In addition, introducing Toombs' interface controller to Chevallier's memory device would have had the predictable result of a controller that interfaces with a host to control operations and settings of a memory array, including setting a secure function bit in a data register. Ex. 1003, ¶¶0039, 0044, Fig. 6; Ex. 1006, ¶323.

3. "Setting at least one bit in order to redefine the command to allow permanent write protection" and/or "a data register"

As shown above for Section XII.A, these limitations would have obvious in view of the Chevallier-Toombs combination. Ex. 1006, ¶¶280-85, 324-27.

I. Dependent Claim 15

1. "Wherein the controller is arranged to define the command to allow permanent write protection of the at least one memory group individually"

As shown above for Sections XII.E and XII.F, these limitations would have obvious in view of the Chevallier-Toombs combination. Ex. 1004, Fig. 4 (CMD 28) (explaining that the SET_WRITE_PROTECT command is defined to protect the memory group(s) identified by the WP_GRP_SIZE bit in the CSD, and explaining rationales for combining Toombs with Chavllier); Section XII.H

(explaining that execution of the SET_WRITE_PROTECT command and interfacing with the CSD functions are performed by Toombs' interface controller); Ex. 1006, ¶341.

In other words, Toombs' interface controller defines the value of the WP_GRP_SIZE bit in the CSD. *Id*. The WP_GRP_SIZE bit is referenced by the SET_WRITE_PROTECT command executed by Toombs' controller, and thus the Toombs' controller defines the SET_WRITE_PROTECT command (via the WP_GRP_SIZE bit) to protect the specified memory group(s), including each WP-group individually. *Id*.

J. Dependent Claim 19

1. "An apparatus according to claim 12, wherein the apparatus is a multimedia card (MMC)."

As shown above for Section XII.G, the Chevallier-Toombs combination renders this Claim obvious. Ex. 1006 ¶¶318, 362-66.

K. Independent Claim 25

1. "A memory device having stored thereon instructions that, when executed, perform [the steps of Claim 25]"

Toombs discloses an MMC card (*e.g*., Fig. 14) that includes firmware that stores information necessary for operation of the card. Ex. 1004, *e.g*., 7:59-61. A POSA would have understood that Toombs disclosure of a firmware teaches "[a] memory device having stored thereon instructions" for performing the functions of

the memory card. Ex. 1006, ¶368. Further, a POSA would have understood that the firmware would have stored the instructions necessary for its MMC card (*e.g.*, the interface controller) to perform operations on the memory block. *Id*.

Motivation to Combine and Resulting System / Method

A POSA would have been motivated to implement the permanent-write-protection method of Chevallier on the MMC card (which includes the firmware) of Toombs in order to enable permanent write protection of segments of memory on the MMC. *Id*. A POSA would have recognized that the MMC would still perform the predictable function of storing the instruction necessary for the interface controller to control operation of the MMC. *Id*.

1. "Setting at least one bit in order to redefine the command to allow permanent write protection" and/or "a data register"

As shown above for Section XII.A, these limitations would have obvious in view of the Chevallier-Toombs combination. Ex. 1006, ¶¶369-72.

XIII. GROUND 4: CLAIM 25 IS OBVIOUS UNDER 35 U.S.C. § 103 OVER THE CHEVALLIER-TOOMBS-ESTAKHRI COMBINATION.

To the extent that Chevallier and/or the Chevallier-Toombs combination do not teach a memory device storing instructions that perform the function of a card controller, it was obvious to introduce that feature to Chevallier and/or the Chevallier-Toombs combination from Estakhri's disclosure of a memory device

having a flash controller (microprocessor circuit) and a storage unit containing the controller's firmware (instructions). Ex. 1005, FIG. 1, 4:54-59; Ex. 1006, ¶377.

Motivation to Combine and Resulting System / Method

A POSA would have understood that Estakhri's storage unit could store the instructions for executing the functionality (including the steps of Claim 25) of Chevallier and/or the Chevallier-Toombs combination, and the microprocessor circuit could execute those functions, providing the predictable and beneficial result of a card controller operable to perform its disclosed functions. Ex. 1006, ¶378; Sections X and XII, *supra*; Ex. 1003, Fig. 6, ¶0004.

XIV. CONCLUSION

For the foregoing reasons, Petitioner respectfully requests that a trial for *inter partes* review of the '370 Patent be instituted and that Claims 1-3, 5-7, 12-15, 19, and 25 be rejected and canceled.

Dated: January 29, 2019

Respectfully submitted,

/Robert C.F. Pérez/

Robert C.F. Pérez (Reg. No. 39,328)
Christopher Kao (*Pro hac vice* to be filed)
Brock S. Weber (*Pro hac vice* to be filed)

Attorneys for Petitioner
Kingston Technology Company, Inc.

PILLSBURY WINTHROP SHAW PITTMAN LLP
1650 Tysons Boulevard, 14th Floor
McLean, VA 22102
Telephone: 703.770.7900
Facsimile: 703.770.7901

CERTIFICATE OF COMPLIANCE

1. The undersigned certifies that this brief complies with the type volume limitations of 37 CFR § 42.24(a)(1)(i). This brief contains 12,383 words (excluding the table of contents, the table of authorities, mandatory notices under 37 CFR § 42.8, the certificate of service, certificate of compliance, and appendix of exhibits), as calculated by the "Word Count" feature of Microsoft Word 2016, the word processing program used to create it.

2. The undersigned further certifies that this brief complies with the typeface requirements of 37 CFR § 42.6(a)(2)(ii) and typestyle requirements of 37 CFR § 42.6(a)(2)(iii). This brief has been prepared in a proportionally spaced typeface using Microsoft Word 2016 in Times New Roman 14-point font.

Dated: January 29, 2019

Respectfully submitted,

/Robert C.F. Pérez/

Robert C.F. Pérez (Reg. No. 39,328)
Christopher Kao (*Pro hac vice* to be filed)
Brock S. Weber (*Pro hac vice* to be filed)

Attorneys for Petitioner
Kingston Technology Company, Inc.

PILLSBURY WINTHROP SHAW PITTMAN LLP
1650 Tysons Boulevard, 14th Floor
McLean, VA 22102
Telephone: 703.770.7900
Facsimile: 703.770.7901

CERTIFICATE OF SERVICE

The undersigned hereby certifies that a true copy of the foregoing **PETITION FOR *INTER PARTES* REVIEW OF U.S. PATENT NO. 7,827,370** and supporting materials (Exhibits 1001 - 1008 and Power of Attorney) have been served in its entirety this 29th of January, 2019, by Federal Express and e-mail on Patent Owner at the correspondence address for the attorney of record for the 7,827,370 Patent shown in USPTO PAIR, as well as on counsel for Patent Owner in the co-pending litigation:

Patent Owner in PAIR (*via FedEx*):

Daniel Hayes
LEE & HAYES, P.C.
601 W. Riverside Avenue, Suite 1400
Spokane, WA 99201

Counsel for Patent Owner in co-pending litigation (*via electronic mail*):

Andrew G. Strickland
Andrew.Strickland@leehayes.com
William B. Dyer III
Bill.Dyer@leehayes.com
LEE & HAYES, P.C.
1175 Peachtree Street
100 Colony Square, Suite 2000
Atlanta, GA 30361

Marc E. Hankin
Marc@HankinPatentLaw.com
Anooj Patel
Anooj@HankinPatentLaw.com
HANKIN PATENT LAW, APC
4299 MacArthur Boulevard,
Suite 100
Newport Beach, CA 92660

/Robert C.F. Pérez/
Robert C.F. Pérez (Reg. No. 39,328)