IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF DELAWARE

MEDIA CONTENT PROTECTION LLC, Plaintiff, v. REALTEK SEMICONDUCTOR CORP., Defendant.	C.A. No.: 20-CV-1247-CFC **JURY TRIAL DEMANDED** **REDACTED PUBLIC VERSION**

SECOND AMENDED COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Media Content Protection LLC ("MCP" or "Plaintiff") brings this action for patent infringement under 35 U.S.C. § 271 against Realtek Semiconductor Corp. ("Realtek" or "Defendant"), and alleges as follows:

THE PARTIES

1. Plaintiff Media Content Protection LLC ("MCP") is a limited liability company duly organized and existing under the laws of the State of Delaware with its principal place of business at 533 Congress Street, Portland, ME 04101.

2. Defendant Realtek Semiconductor Corp. is a corporation duly organized and existing under the laws of Taiwan with a principal place of business located at No. 2 Innovation Road II, Hsinchu Science Park, Hsinchu 300, Taiwan.

3. According to its website, Realtek "is a world-leading IC provider that designs and develops a wide range of IC products for connected media, communications network, computer peripheral, and multimedia applications" including "LCD Monitor/ATV/DTV Controllers, and Digital Home Center Controllers." News Release, *Realtek Wins Three Awards at COMPUTEX TAIPEI*

2022, including a Best Choice of the Year Award (May 24, 2022), https://www.realtek.com/en/press-room/news-releases/item/realtek-wins-three-awards-at-computex-taipei-2022-including-a-best-choice-of-the-year-award-2 (last visited October 10, 2022).

4. On information and belief, Realtek has regularly attended and participated in the International Consumer Electronics Show ("CES") in Las Vegas, Nevada, which bills itself as "the most influential tech event in the world." For example, at the 2019 CES, Realtek exhibited and demonstrated "a full range of connectivity, multimedia, and consumer electronics solutions" including the "4K Android Smart TV SoC with Advanced Picture/Audio Quality (RTD2851/RTD2873)." *Realtek to Demonstrate Full Range of Connectivity, Multimedia, and Consumer Electronics Solutions at 2019 CES* (Jan. 7, 2019), https://www.realtek.com/en/press-room/news-releases/item/realtek-to-demonstrate-full-range-of-connectivity-multimedia-and-consumer-electronics-solutions-at-2019-ces. Upon information and belief, at least in order to exhibit and demonstrate the RTD2851/RTD2873 SoCs, Realtek imported the devices into the United States.

5. According to Realtek, it is "headquartered in Taiwan and it has sales or R&D teams in China, Singapore, *the United States*, Japan, and South Korea." *Realtek 2020 Annual Report* at 4 (Apr. 28, 2021) (emphasis added), https://www.realtek.com/images/ar/-__.pdf. As part of its 2020 Annual Report's description of Realtek's "Communications Network Products" and "Multimedia Products" industries, and market overview, Realtek stated that:

> Fierce competition among suppliers of LCD TV Controllers in recent years has led key suppliers to gradually downsize, merge, or leave the market. ***Realtek, however, continues to develop new products..., as well as a new generation of Integrated 4K Smart LCD TV Controllers*** that support HDR . . . . Realtek provides an

> 8K TV decoder solution for customers to have a seamless transition to 8K TV without changing the original TV architecture, and more competitive products for LCD television manufacturers. . . .
>
> [T]he market for UHD televisions is rising and UHD HDR video content is becoming widespread . . . . Realtek is therefore developing highly integrated multimedia controllers with new features and a high cost-performance ratio . . . . Sales of LCD televisions in 2021 are expected to be at about the same level as those in 2020. ***Key growth will come from*** Central and South America, ***North America***, China, and Southeast Asia.

Id. at 78, 84–85 (emphases added).

6. Defendant, either itself and/or through the activities of its subsidiaries, affiliates, or intermediaries (including distributors, retailers, and others), makes, uses, sells, offers for sale, and/or imports throughout the United States, including within the District of Delaware (this "District"), products, such as digital video-capable integrated circuits and associated firmware that infringe the Asserted Patent, defined below. Defendant makes, uses, sells, offers to sell, and/or imports digital video-capable integrated circuits, that it or its customers incorporate into digital video-capable devices that are made, used, sold, offered for sale, and/or imported throughout the United States, including within this District. These digital video-capable devices may include, but are not limited to, televisions, monitors, displays, projectors, video adapters, and/or video hubs.

THE ASSERTED PATENT

U.S. Patent No. 10,298,564

8. United States Patent No. 10,298,564 (the "'564 Patent") is entitled "Secure Authenticated Distance Measurement" and issued on May 21, 2019 to inventor Franciscus L. A. J. Kamperman. The '564 Patent issued from United States Patent Application No. 16/117,019 filed on August 30, 2018. A copy of the '564 Patent is attached hereto as Exhibit A.

9. By way of assignment, MCP owns all rights, title, and interest to the '564 Patent (the "Asserted Patent").

10. The Asserted Patent is valid and enforceable.

JURISDICTION AND VENUE

11. This is a civil action for patent infringement arising under the Patent Act, 35 U.S.C. § 1 *et seq*.

12. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

13. This Court has personal jurisdiction over Realtek pursuant to due process and/or the Delaware long-arm statute, because (1) Defendant has conducted and continues to conduct business in the United States and this District and (2) Defendant has committed and continues to commit acts of patent infringement in the United States and this District, including inducing others to commit acts of patent infringement in the United States and this District.

14. Realtek has conducted and continues to conduct business in the United States and the District of Delaware. Further, Realtek, directly or through subsidiaries or intermediaries (including distributors, retailers, and others), ships, distributes, makes, uses, offers for sale, sells, imports, and/or advertises (including by providing interactive web pages) its products and/or services in the United States and the District of Delaware and/or contributes to and actively induces its customers to ship, distribute, make, use, offer for sale, sell, import, and/or advertise (including the through interactive web pages) infringing products and/or services in the United States and the District of Delaware.

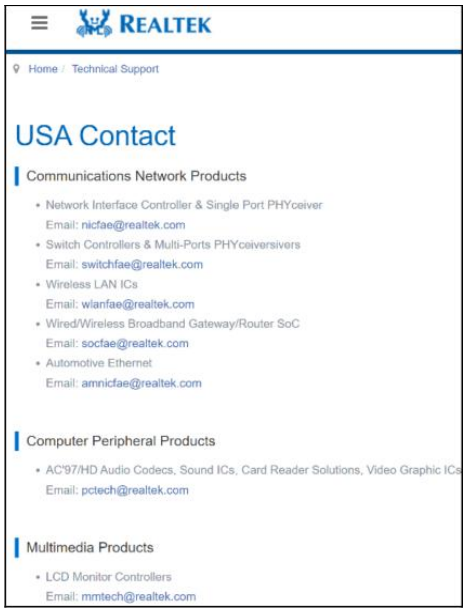
15. Realtek has committed acts of patent infringement within the United States and the District of Delaware. Realtek, directly and through subsidiaries or intermediaries (including distributors, retailers, and others), has purposefully and voluntarily placed one or more of its infringing products and/or services, as

described below, into the stream of commerce with the expectation that those products will be purchased and used by consumers in the District of Delaware. On information and belief, Realtek has not made any efforts to ensure that its products or advertising do not reach consumers in Delaware. On information and belief, these infringing products and/or services have been and continue to be purchased and used by consumers in the District of Delaware.

16. According to its website, Realtek has authorized distributors for the sale and supply of its products in the United States.[1] Specifically, Realtek's United States distributors include Future Electronics and WPG Americas, Inc.[2]

17. Additionally, according to Realtek's 2021 ESG Report, "Realtek . . . has ***overseas subsidiary*** [sic] at key locations around the world, including . . . ***the United States*** . . . in order to provide customers comprehensive products, services, and solutions with timely and professional support."[3]

[1] https://www.realtek.com/en/contact-us-en/cu-3-en-2/category/42-12-en-3 (accessed Oct. 8, 2022).
[2] *Id.*
[3] Realtek 2021 ESG Report at 23, (available at: https://www.realtek.com/images/csr/Realtek_2021_ESG_Report_EN.pdf) (accessed Oct. 8, 2022).



18. Further targeting the United States market, Realtek specifically provides technical support contact information within the United States. Notably, the United States is one of the only three countries for which Realtek provides specific technical support contact information.[4] Moreover, Realtek sells and supplies certain infringing digital video-capable integrated circuits to companies that are based in and/or specifically target the United States, including at least [redacted], Lenovo Group Ltd. ("Lenovo), and [redacted]. For example, the [redacted] incorporates Realtek's [redacted] integrated circuit and associated firmware and is marketed and sold to consumers in this District, including through

[4] https://www.realtek.com/en/cu-1-en/cu-1-usa-en (accessed Oct. 8, 2022).

BestBuy[5], Amazon[6], Walmart[7], Target[8], etc. As of October 18, 2022, this infringing product is available for purchase by consumers in Delaware via direct shipment or in-store pickup. *See, e.g.*, https://www.bestbuy.com/site/ (last accessed October 18, 2022).

[5] https://www.bestbuy.com/site/ (last accessed October 18, 2022).
[6] https://www.amazon.com/ (last accessed October 18, 2022).
[7] https://www.walmart.com/ (last accessed October 18, 2022).
[8] https://www.target.com/p/ (last accessed October 18, 2022).

19. In addition, Realtek partners with other companies to specifically and intentionally target the United States market. For instance, Realtek has partnered with iWedia, "a provider of software components and solutions for TV devices for major service operators and consumer electronics manufacturers," to provide "power and flexibility to OEMs ***targeting the North America broadcast market*** and the candidate countries."[9] According to Realtek's own news release, "Realtek joined the 2021 Industry Tech Day, an iconic engineering exhibition among Europe and the U.S." The news release further stated:

> Realtek's business covers Asia, Europe, and ***the Americas***, and is ***well-known*** in Europe and the ***U.S.*** Realtek has been invited to participate at '2021 Industry Tech Days', a European and ***American engineering online exhibition***, where we will showcase our innovative IC technologies and applications.[10]

20. Realtek's extensive contacts with, and intentional targeting of, the United States market are further evidenced by Realtek's Annual Report from 2019, which states:

> As technology matures and prices become more affordable, Wi-Fi use is flourishing in the consumer and IoT markets. For example, Wi-Fi has already become a standard feature in smart televisions. ***Realtek performs strongly in major global television markets***. As the television market becomes saturated, Wi-Fi use is trending toward an M- shape, with high-end products using 11ac and gradually adopting 11ax while low-end

[9] iWedia Partners with Realtek to Launch NextGen TV Reference Platform, TVT Staff (June 7, 2022) (emphasis added), https://www.tvtechnology.com/news/iwedia-partners-with-realtek-to-launch-nextgen-tv-reference-platform.

[10] Realtek joined the 2021 Industry Tech Day, an iconic engineering exhibition among Europe and the U.S. (Sept. 6, 2021) (emphases added), https://www.realtek.com/en/press room/news-releases/item/realtek-joined-the-2021-industry-tech-day-an-iconic engineering-exhibition-among-europe-and-the-u-s.

> products continue to use 11n. For all ranges of televisions, ***Realtek offers Wi-Fi solutions with high price-performance ratios that support expansion of this important market***.[11]

22. At a minimum, Realtek knew, should have known, expected, and/or should have expected that by purposefully selling and supplying certain infringing digital video-capable integrated circuits and associated firmware to its major customers—like massive U.S.-based electronics companies such as [redacted] that products incorporating those infringing digital video-capable integrated circuits and associated firmware would be sold to customers in Delaware.

23. In addition to Realtek's participation in Delaware commerce through its business activities, Realtek has also chosen the United States District Court for the District of Delaware as a forum to initiate at least two prior litigations as a plaintiff. (*See Realtek Semiconductor Corp. v. Avago Technologies General IP (Singapore) Pte. Ltd.* D.Del. 1:17-cv-01114-GMS and *Realtek Semiconductor Corp. v. Broadcom Corp.* D.Del. 1:17-cv-01115-GMS). By filing multiple suits in this District, Realtek has voluntarily appeared in this District, sought the protection of its laws, and availed itself of this forum as a plaintiff. Therefore, Realtek has implicitly consented to this Court's personal jurisdiction. At a minimum, Realtek has shown that it is willing to appear in this forum to vindicate its *own* rights.

24. Alternatively, to the extent that Realtek's contacts with Delaware do not support jurisdiction under the Delaware long-arm statute, Realtek is subject to personal jurisdiction pursuant to Rule 4(k)(2) of the Federal Rules of Civil Procedure because (1) MCP's claims arise under federal law, (2) Realtek is not subject to jurisdiction in the courts of general jurisdiction of any state within the United States, and (3) the exercise of jurisdiction satisfies due process requirements. Venue in this District is proper pursuant to 28 U.S.C. §§ 1391(b), (c) and 1400(b) because

[11] Realtek Annual Report 2019 at 67 (Apr. 8, 2020), https://www.realtek.com/images/ar/Annual_Report_2019__20200519.pdf

Defendant is not a resident of the United States and may be sued in any judicial district, and has committed acts of infringement in this District.

25. Defendant has and does conduct business within the State of Delaware including in this District. Defendant, directly or through subsidiaries, affiliates or intermediaries (including distributors, retailers, and others), ships, distributes, makes, uses, offers for sale, imports and/or advertises (including by providing an interactive web page) its products and/or services in the United States and this District, and/or contributes to and actively induces its customers to ship, distribute, make, use, offer for sale, sell, import, and/or advertise (including the provision of interactive web pages) infringing products and/or services in the United States and this District. Defendant, directly or through subsidiaries, affiliates or intermediaries (including distributors, retailers, and others), has purposefully and voluntarily placed one or more of its infringing products, or components thereof as described below, into the stream of commerce with the expectation that those products will be purchased, used, and or incorporated into digital video-capable devices made, used, sold, offered for sale, purchased, and/or imported by customers and/or consumers in this District.

BACKGROUND

26. MCP incorporates the allegations of all of the foregoing paragraphs as if fully restated herein.

27. Koninklijke Philips N.V. (formerly known as Koninklijke Philips Electronics N.V.) ("Philips N.V.") and Philips North America LLC (formerly known as Philips Electronics North America Corporation) ("Philips North America") (collectively, "Philips") is a world-renowned company that engages in research and development in numerous fields. One of these fields pertains to digital video-capable devices for delivering and displaying content to users. Exemplary products in this field include televisions, monitors, displays, projectors, video adapters, and/or video

hubs. The Asserted Patent derives from Philips's efforts in this field and claim protection for, among other things, delivering and displaying content to users.

28. Defendant made, used, sold, offered for sale, imported, tested, designed, and/or marketed in the United States digital video-capable integrated circuits and associated firmware for delivering and displaying content to users that infringe the Asserted Patent. Such digital video-capable integrated circuits and associated firmware are incorporated into digital video-capable devices made, used, sold, offered for sale or imported into the United States by companies, including but not limited to, Lenovo, [redacted], and/or their affiliates, subsidiaries or intermediaries (the "Exemplary Customers").

29. Defendant has actual notice of the Asserted Patent. Defendant received actual notice of the Asserted Patent at least as early as September 16, 2020 by way of a letter to Defendant dated September 16, 2020. That letter included allegations of infringement of the Asserted Patent. Additionally, the filing of this Complaint and the First Amended Complaint also constitutes notice in accordance with 35 U.S.C. § 287.

30. With actual notice of the Asserted Patent, Defendant has directly infringed, and continues to directly infringe the Asserted Patent under 35 U.S.C. § 271(a) and (g) by one or more of making, using, selling and/or offering to sell, in this District and elsewhere in the United States, and importing into this District and elsewhere in the United States, certain infringing digital video-capable integrated circuits that infringe the Asserted Patent (the "Accused Products"), as further described in detail in Count I *infra*.

31. The Accused Products include, but are not limited to, all digital video-capable integrated circuits and associated firmware designed to facilitate digital video-capable playback supporting the HDCP 2.0 protocol and above that Defendant, either itself and/or through the activities of its subsidiaries, affiliates, or

intermediaries (including distributors, retailers, and others), makes, uses, sells, offers for sale, and/or imports throughout the United States, including, but not limited to, the following products and/or product lines, their associated firmware/software, and/or any development boards or printed circuit board assemblies containing the same: RTD2795Y, LGE0551-AS1, RTD2873SAJ, "Integrated High Resolution 5K3K/4K2K/QHD LCD Controller with HDR, DP1.4, HDMI2.0, and HDCP2.2", "Integrated High Resolution 4K2K 144Hz/QHD165Hz Gaming LCD Display Controller with Realtek Owl Sight Technology, DSC, HDR, DP1.4, HDMI2.0, ad HDCP2.3", "High Resolution 4K2K 144Hz/QHD 165Hz Gaming LCD Controller with Realtek Owl Sight Technology, DSC, HDR, DP1.4, HDMI2.0, and HDCP2.3", "Ultra-low Power High Resolution 5K3K/4K2K LCD Controllers with HDR, DP1.4, HDMI2.0, and HDCP2.2."[12] This list of Defendant's currently known digital video-capable integrated circuits and associated firmware is exemplary and, on information and belief, many other of Defendant's digital video-capable integrated circuits and associated firmware infringe the Asserted Patent.

32. Defendant has also indirectly infringed, and continues to indirectly infringe the Asserted Patent under 35 U.S.C. § 271(b) and (c). Defendant knew and intended to induce and contribute to the infringement of the Asserted Patent. The Accused Products have no substantial non-infringing use, are a material part of the invention of the Asserted Patent, especially made or especially adapted for use in an infringement of the Asserted Patent, and not a staple article or commodity of commerce suitable for substantial non-infringing use.

33. After receiving actual notice of the Asserted Patent, Defendant proceeded to actively induce, and materially contribute to, its customers' infringement of the Asserted Patent by making, using, selling, offering for sale,

[12] Realtek Semiconductor Corp. 2019 Annual Report at 62, 73, retrieved from https://www.realtek.com/images/ar/Annual_Report_2019__20200519.pdf.

marketing, advertising, and/or importing digital video-capable integrated circuits with associated firmware that are incorporated into Defendants' digital video-capable devices that infringe the Asserted Patent, and instructing customers to infringe the Asserted Patent.

34. For example, Defendants specifically intended and advertised that their digital video-capable integrated circuits and associated firmware for use within digital video-capable devices such as smart televisions.[13] Such digital video-capable integrated circuits and associated firmware are advertised as providing supporting "HDMI 2.0/ HDCP-2.2" interfaces. Further, on information and belief, Realtek presents and demonstrates infringing uses such infringing digital video-capable integrated circuits and associated firmware to customers at trade shows such as Consumer Electronics Solutions ("CES") in Las Vegas, Nevada. Thus, Defendants induce their customers to infringe the Asserted Patent by advertising and/or instructing their customers regarding infringing uses of the Accused Products. On information and belief, Defendants did so with the specific intent to bring about infringement in the United States knowing that, among others, at least the Exemplary Customers would incorporate Defendants' digital-video capable integrated circuits and associated firmware in digital-video capable devices made, used, sold, offered for sale or imported into the United States.

35. As another example, Defendants contribute to the same infringement by selling digital video-capable integrated circuits and associated firmware to customers who incorporate said digital video-capable integrated circuits and associated firmware into their infringing digital video-capable devices. On information and belief, Defendants had knowledge that digital video-capable

[13] https://www.realtek.com/en/press-room/news-releases/item/realtek-to-demonstrate-full-range-of-connectivity-multimedia-and-consumer-electronics-solutions-at-2016-ces.

integrated circuits and associated firmware were especially made or especially adapted for use in an infringement of the Asserted Patent by practicing the HDCP 2.0 protocol or above, and were not a staple article or commodity of commerce suitable for substantial non-infringing use.

36. Thus, Defendant has indirectly infringed, and continues to indirectly infringe, the Asserted Patent under 35 U.S.C. § 271(b) by actively inducing its customers to infringe the Asserted Patent by making, using, selling, offering for sale, marketing, advertising, and/or importing the Accused Products to its customers and by instructing customers to infringe the Asserted Patent, as described in detail in Count I *infra*. Additionally, Defendant has indirectly infringed, and continue to indirectly infringe the Asserted Patent under 35 U.S.C. § 271(c) by materially contributing to their own customers' infringement of the Asserted Patent by making, using, selling, offering for sale, advertising, marketing, and/or importing the Accused Products to its customers and instructing customers to infringe the Asserted Patent, as described in detail in Count I *infra*.

37. Defendant's acts of infringement have caused damage to MCP. MCP is entitled to recover from Defendant the damages incurred by MCP as a result of Defendant's wrongful acts.

COUNT I

Defendant's Infringement of the '564 Patent

38. MCP incorporates the allegations of all of the foregoing paragraphs as if fully restated herein.

39. Defendant has directly infringed, and continues to directly infringe, the '564 Patent by making, using, selling, offering for sale, or importing throughout the United States products and/or methods covered by one or more claims of the '564 Patent including, but not limited to, digital video-capable integrated circuits and associated firmware for inclusion in digital video-capable devices. The products that

infringe one or more claims of the '564 Patent include, but are not limited to, at least the Accused Products. Further discovery may reveal additional infringing products and/or models.

40. For example and without limitation, the Accused Products infringe claim 1 of the '564 Patent.

41. Attached hereto as Exhibit B, and incorporated into this Second Amended Complaint, is a claim chart showing where in the Realtek [redacted] integrated circuit and associated firmware integrated in the [redacted] each limitation of claims 1-11, 14-23, 25, 28, are met. This claim chart is exemplary and, on information and belief, many other products provided by Defendant infringe the '564 Patent.

42. Defendant has, and continues to, indirectly infringe the '564 Patent by actively inducing and contributing to the infringement of the '564 Patent by others, such as customers, resellers, and retailers. These others include, but are not limited to, Best Buy Co., Inc. and its affiliates, who, for example, sell, offer for sale, and/or import throughout the United States, including within this District, the Accused Products.

43. Defendant specifically intended others, such as customers, resellers, and retailers, to infringe the '564 Patent and knew that these others perform acts that constituted direct infringement. For example, Exhibit B shows that an exemplary product, the Realtek [redacted] integrated circuit and associated firmware integrated in the [redacted] which is sold by Best Buy Co., Inc., infringes the '564 Patent. Defendant designed the Accused Products such that they would each infringe the '564 Patent as described in Exhibit B if made, used, sold, offered for sale, or imported throughout the United States. Defendant provided, directly or

indirectly, Accused Products to others, such as, but not limited to, customers, knowing and intending that those others would use, sell, offer for sale, and/or import the Accused Products throughout the United States, thereby directly infringing one or more claims of the '564 Patent.

44. In addition, upon information and belief, Defendant provides instructions, user guides, and/or other documentation to the infringing others regarding the use and operation of the Accused Products. When others follow such instructions, user guides, and/or other documentation, they directly infringe one or more claims of the '564 Patent. By providing such instructions, user guides, and/or other documentation, Defendant knows and intend that others will follow those instructions, user guides, and other documentation, and thereby directly infringe one or more claims of the '564 Patent. Thus, Defendant knows that their actions actively induce infringement.

45. The Accused Products have no substantial non-infringing uses and are a material part of the invention. As described in Exhibit B, any manufacture, use, sale offer for sale or importation throughout the United States of an Accused Product, or incorporation of any of the Accused Products in digital video-capable devices infringes the '564 Patent. Thus, the Accused Products have no substantial non-infringing uses.

46. MCP is entitled to recover damages under 35 U.S.C. § 284 to adequately compensate for Defendant's infringement of the '564 Patent.

DAMAGES

47. Defendant has refused to compensate MCP for its infringement of the Asserted Patent. MCP is entitled to monetary damages adequate to compensate MCP for Defendant's infringement in an amount no less than a reasonable royalty for the use made of the patented inventions by Defendant. The precise amount of damages will be determined through discovery in this action and proven at trial.

MARKING

48. MCP and its licensees of the Asserted Patent have complied with 35 U.S.C. § 287, and relative to its licensees, MCP has taken reasonable steps to ensure compliance with marking.

PRAYER FOR RELIEF

WHEREFORE, MCP respectfully asks the Court for an order granting the following relief:

a) A judgment that the Asserted Patent is valid and enforceable;

b) A judgment that Defendant has infringed, directly and indirectly, either literally or under the Doctrine of Equivalents, one or more claims of the '564 Patent;

c) A judgment awarding MCP all appropriate damages under 35 U.S.C. § 284 for Defendant's past infringement, and any continuing or future infringement of the Asserted Patent, including pre and post judgment interest, costs, and disbursements pursuant to 35 U.S.C. § 284;

d) An accounting for infringing sales not presented at trial and an award by the Court of additional damages for any such infringing sales;

e) A finding that this case is exceptional within the meaning of 35 U.S.C. § 285 and that MCP be awarded its reasonable attorneys' fees against Defendant incurred in prosecuting this action;

f) An award of reasonable attorneys' fees, costs, and expenses incurred by MCP in connection with prosecuting this action; and

g) Any and all other relief as the Court finds just, equitable, and proper under the circumstances.

DEMAND FOR JURY TRIAL

Pursuant to Fed. R. Civ. P. 38, MCP hereby respectfully demands trial by jury on all claims and issues so triable.

Dated: September 20, 2024

Respectfully submitted,

FARNAN LLP

/s/ Brian E. Farnan

Brian E. Farnan (Bar No. 4089)
Michael J. Farnan (Bar No. 5165)
919 N. Market St., 12th Floor
Wilmington, DE 19801
Phone: (302) 777-0300
Fax: (302) 777-0301
bfarnan@farnanlaw.com
mfarnan@farnanlaw.com

Michael T. Renaud (admitted *pro hac vice*)
Adam S. Rizk (admitted *pro hac vice*)
Catherine Xu (admitted *pro hac vice*)
Timothy J. Rousseau (admitted *pro hac vice*)
Courtney P. Herndon (admitted *pro hac vice*)
Williams S. Dixon (admitted *pro hac vice*)
MINTZ LEVIN COHN FERRIS
GLOVSKY & POPEO PC
One Financial Center
Boston, Massachusetts 02111
Phone: 617) 542-6000
Fax: (617) 542-2241
MTRenaud@mintz.com
ARizk@mintz.com
CXu@mintz.com
TJRousseau@mintz.com
CHerndon@mintz.com
WSDixon@mintz.com

Peter F. Snell (admitted *pro hac vice*)
Brad M. Scheller (admitted *pro hac vice*)
MINTZ LEVIN COHN FERRIS
GLOVSKY & POPEO PC
919 Third Avenue

New York, NY 10022
Phone: (212) 935-3000
Fax: (212) 983-3115
PFSnell@mintz.com
BMScheller@mintz.com

Attorneys for Plaintiff
Media Content Protection LLC

EXHIBIT A

US010298564B2

(12) **United States Patent**
Kamperman

(10) **Patent No.: US 10,298,564 B2**
(45) **Date of Patent: *May 21, 2019**

(54) **SECURE AUTHENTICATED DISTANCE MEASUREMENT**

(71) Applicant: **KONINKLIJKE PHILIPS N.V.**, Eindhoven (NL)

(72) Inventor: **Franciscus L. A. J. Kamperman**, Geldrop (NL)

(73) Assignee: **KONINKLIJKE PHILIPS N.V.**, Eindhoven (NL)

(*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **16/117,019**

(22) Filed: **Aug. 30, 2018**

(65) **Prior Publication Data**

US 2019/0014106 A1 Jan. 10, 2019

Related U.S. Application Data

(63) Continuation of application No. 15/352,646, filed on Nov. 16, 2016, now Pat. No. 10,091,186, which is a (Continued)

(30) **Foreign Application Priority Data**

Jul. 26, 2002 (EP) 02078076

(51) **Int. Cl.**
H04L 29/06 (2006.01)
H04L 9/14 (2006.01)
(Continued)

(52) **U.S. Cl.**
CPC ***H04L 63/0823*** (2013.01); ***G06F 21/10*** (2013.01); ***H04L 9/14*** (2013.01);
(Continued)

(58) **Field of Classification Search**
CPC H04L 63/0823; H04L 9/14; H04L 63/107; H04L 63/062; H04L 43/16;
(Continued)

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,438,824 A 3/1984 Mueller-Scholoer
4,688,036 A 8/1987 Hirano et al.
(Continued)

FOREIGN PATENT DOCUMENTS

EP 1100035 A1 5/2001
JP H04306760 A 10/1992
(Continued)

OTHER PUBLICATIONS

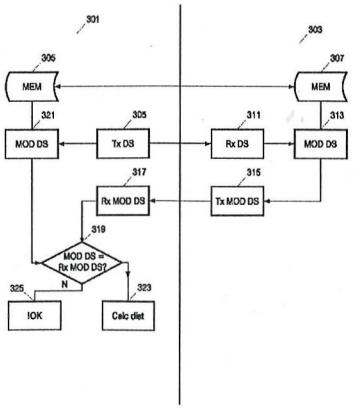
Ikeno et al "Modern Cryptography Theory" Japan, Institute of Electronics, Information and Communication Engineers, Nov. 15, 1997, p. 175-177.
(Continued)

Primary Examiner — Darren B Schwartz

(57) **ABSTRACT**

The invention relates to a method for a first communication device to perform authenticated distance measurement between the first communication device and a second communication device, wherein the first and the second communication device share a common secret and the common secret is used for performing the distance measurement between the first and the second communication device. The invention also relates to a method of determining whether data stored on a first communication device are to be accessed by a second communication device. Moreover, the invention relates to a communication device for performing authenticated distance measurement to a second communication device. The invention also relates to an apparatus for playing back multimedia content comprising a communication device.

53 Claims, 3 Drawing Sheets



Related U.S. Application Data

continuation of application No. 15/229,207, filed on Aug. 5, 2016, now Pat. No. 9,590,977, which is a continuation of application No. 14/538,493, filed on Nov. 11, 2014, now Pat. No. 9,436,809, which is a continuation of application No. 10/521,858, filed as application No. PCT/IB03/02932 on Jun. 27, 2003, now Pat. No. 8,886,939.

(51) **Int. Cl.**

H04L 12/26	(2006.01)
H04L 9/32	(2006.01)
G06F 21/10	(2013.01)
H04L 9/30	(2006.01)
H04W 24/00	(2009.01)
H04W 12/06	(2009.01)

(52) **U.S. Cl.**

CPC ***H04L 9/30*** (2013.01); ***H04L 9/3263*** (2013.01); ***H04L 43/0852*** (2013.01); ***H04L 43/16*** (2013.01); ***H04L 63/062*** (2013.01); ***H04L 63/107*** (2013.01); *G06F 2221/07* (2013.01); *G06F 2221/2111* (2013.01); *H04L 63/0428* (2013.01); *H04L 2463/101* (2013.01); *H04W 12/06* (2013.01); *H04W 24/00* (2013.01)

(58) **Field of Classification Search**

CPC H04L 43/0852; H04L 9/3263; H04L 9/30; H04L 63/0428; H04L 2463/101; G06F 21/10; G06F 2221/07; G06F 2221/2111; H04W 24/00; H04W 12/06

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,926,480	A	5/1990	Chaum	
5,126,746	A	6/1992	Gritton	
5,596,641	A	1/1997	Ohashi et al.	
5,602,917	A	2/1997	Mueller	
5,659,617	A	8/1997	Fischer	
5,723,911	A	3/1998	Glehr	
5,778,071	A	7/1998	Caputo et al.	
5,937,065	A	8/1999	Simon et al.	
5,949,877	A	9/1999	Traw et al.	
5,983,347	A	11/1999	Brinkmeyer et al.	
6,085,320	A	7/2000	Kaliski	
6,088,450	A	7/2000	Davis et al.	
6,151,676	A	11/2000	Cuccia et al.	
6,208,239	B1	3/2001	Muller et al.	
6,346,878	B1	2/2002	Pohlman et al.	
6,351,235	B1	2/2002	Stilp	
6,442,690	B1	8/2002	Howard, Jr.	
6,484,948	B1	11/2002	Sonoda	
6,493,825	B1	12/2002	Blumenau et al.	
6,526,598	B1	3/2003	Horn	
6,550,011	B1 *	4/2003	Sims, III	G06F 21/10 365/52
7,200,233	B1	4/2007	Keller et al.	
7,242,766	B1	7/2007	Lyle	
7,516,325	B2	4/2009	Willey	
7,787,865	B2	8/2010	Willey	
7,898,977	B2	3/2011	Roese	
8,068,610	B2	11/2011	Moroney	
8,107,627	B2	1/2012	Epstein	
8,352,582	B2	1/2013	Epstein	
8,997,243	B2	3/2015	Epstein	
2001/0008558	A1	7/2001	Hirafuji	
2001/0043702	A1	11/2001	Elteto et al.	
2001/0044786	A1	11/2001	Ishibashi	
2001/0050990	A1 *	12/2001	Sudia	G06Q 20/02 380/286
2002/0007452	A1 *	1/2002	Traw	G06F 21/10 713/152
2002/0026424	A1	2/2002	Akashi	
2002/0026576	A1	2/2002	Das-Purkayastha et al.	
2002/0035690	A1	3/2002	Nakano	
2002/0061748	A1	5/2002	Nakakita et al.	
2002/0078227	A1	6/2002	Kronenberg	
2002/0166047	A1	11/2002	Kawamoto	
2003/0021418	A1	1/2003	Arakawa et al.	
2003/0030542	A1	2/2003	Von Hoffmann	
2003/0051151	A1	3/2003	Asano	
2003/0065918	A1	4/2003	Willey	
2003/0070092	A1	4/2003	Hawkes et al.	
2003/0112978	A1	6/2003	Rodman et al.	
2003/0174838	A1 *	9/2003	Bremer	H04L 63/0428 380/270
2003/0184431	A1	10/2003	Lundkvist	
2003/0220765	A1	11/2003	Overy et al.	
2004/0015693	A1	1/2004	Kitazumi	
2004/0025018	A1 *	2/2004	Haas	H04L 45/26 713/168
2004/0080426	A1	4/2004	Fraenkel	
2005/0114647	A1	5/2005	Epstein	
2005/0265503	A1	12/2005	Rofheart et al.	
2006/0294362	A1	12/2006	Epstein	

FOREIGN PATENT DOCUMENTS

JP	H0619948	A	1/1994
JP	H08234658	A	9/1996
JP	9170364	A	6/1997
JP	H09170364	A	6/1997
JP	11101035	A	4/1999
JP	11208419	A	8/1999
JP	2000357156	A	12/2000
JP	2001249899	A	9/2001
JP	2001257672	A	9/2001
JP	2002124960		4/2002
JP	2002189966	A	7/2002
WO	9739553	A1	10/1997
WO	9949378		9/1999
WO	0152234	A1	7/2001
WO	0193434	A1	12/2001
WO	0233887	A2	4/2002
WO	0235036	A1	5/2002
WO	02054353	A1	7/2002

OTHER PUBLICATIONS

Modern Cryptography Theory (1986) Chapter 9, ISBN: 4-88552-064-9 (Japanese).

Hayashi et al Encryption and Authentication Program Module , Technical Paper (Japanese) NTT R&D vol. 44, No. 10 Oct. 1, 1995.

Stefan Brands and Devid Chaum "Distance Bounding Protocols" Eurocrypt '93, (1993) p. 344-359.

Tim Kindber & Kan Zhang "Context Authention Using Constrained Channels" pp. 1-8 , Apr. 16, 2001.

Hitachi Ltd., 5C Digital Transmission Content Protection White Paper Rev. 1.0 Jul. 14, 1998, p. 1013.

Boyd et al "Protocols for Authention and Key Establishment" Spring-Verlag, Sep. 17, 2003, p. 116-120, 195, 305.

High Bandwidth Digital Content Protection System Feb. 17, 2000.

High Bandwidth Digital Content Protection System Revision 1.0 Erratum Mar. 1, 2001.

Digital Transmission Content Protection Specification vol. 1 Hitachi Ltd. Revision 1.0 Apr. 12, 1999.

Digital Transmission Content Protection Specification vol. 1 (Informational Version) Hitachi Ltd. Revision 1.2A Feb. 25, 2002.

SmartRight™ Certification for FCC Approval for Use with the Broadcast Flag, Mar. 1, 2004.

SmartRight™ Copy Protection for System for Digital Home Networks, Deployment Process, CPTWG, Nov. 28, 2001.

SmartRight™ Copy Protection System for Digital Home Networks, CPTWG, May 24, 2001.

SmartRight™ Digital Broadcast Content Protection, Presentation to FCC, Apr. 2, 2004 (cited in litigation).

(56) **References Cited**

OTHER PUBLICATIONS

SmartRight™ Technical White Paper, Version 1.7, Jan. 2003 ("White Paper") (cited in litigation).
Internet Security Association and Key Management Protocol (ISAKMP), Request for Comments 2408 ("RFC 2408")—cited in litigation, Nov. 1998.
International Standard ISO/IEC 11770-3 (1st ed.) ("ISO 11770-3") , Nov. 1, 1999.
Scott Crosby, et al., "A Cryptanalysis of the High-bandwidth Digital Content Protection System " Computer and Communications Security, (2001).
SmartRight™ Specifications Sep. 26, 2001.
SmartRight™ Copy Protection System for Digital Home Networks, CPTWG, Jul. 11, 2001.
Bruce Schneier, Applied Cryptography (2d ed. 1996) ("Schneier").
Steven M. Bellovin and Michael Merritt, "Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks", 2002.
RFC 2463 Internet Control Message Protocol Dec. 1998.
RFC2246 the TLS Protocol, Jan. 1999.
Internet Security Association and Key Management Protocol (ISAKMP), Request for Comments 2408 ("RFC 2408") , Nov. 1998.
Declaration of William Rosenblatt, Microsoft Exhibit 1009 , Dec. 8, 2017.
Supplemental Declaration of William Rosenblatt, Microsoft Exhibit 1015 , Apr. 20, 2018.
Petition for Inter Parties Review of USP 8543819 , Dec. 8, 2017.
Patent Owner's Preliminary Response , Mar. 13, 2018.
Petitioners' Reply to Patent Owner's Preliminary Response , Apr. 20, 2018.
Patent Owner's Sur-Reply to Petitioners' Reply , May 4, 2018.
Petition for Inter Parties Review of USP 9436809 , Dec. 8, 2017.
Markman Order Filed Jul. 11, 2017.
Internet Security Association and Key Management Protocol (ISAKMP), Request for Comments 2407 ("RFC 2407") , Nov. 1998.
Internet Security Association and Key Management Protocol (ISAKMP), Request for Comments 2409 ("RFC 2409") , Nov. 1998.

* cited by examiner

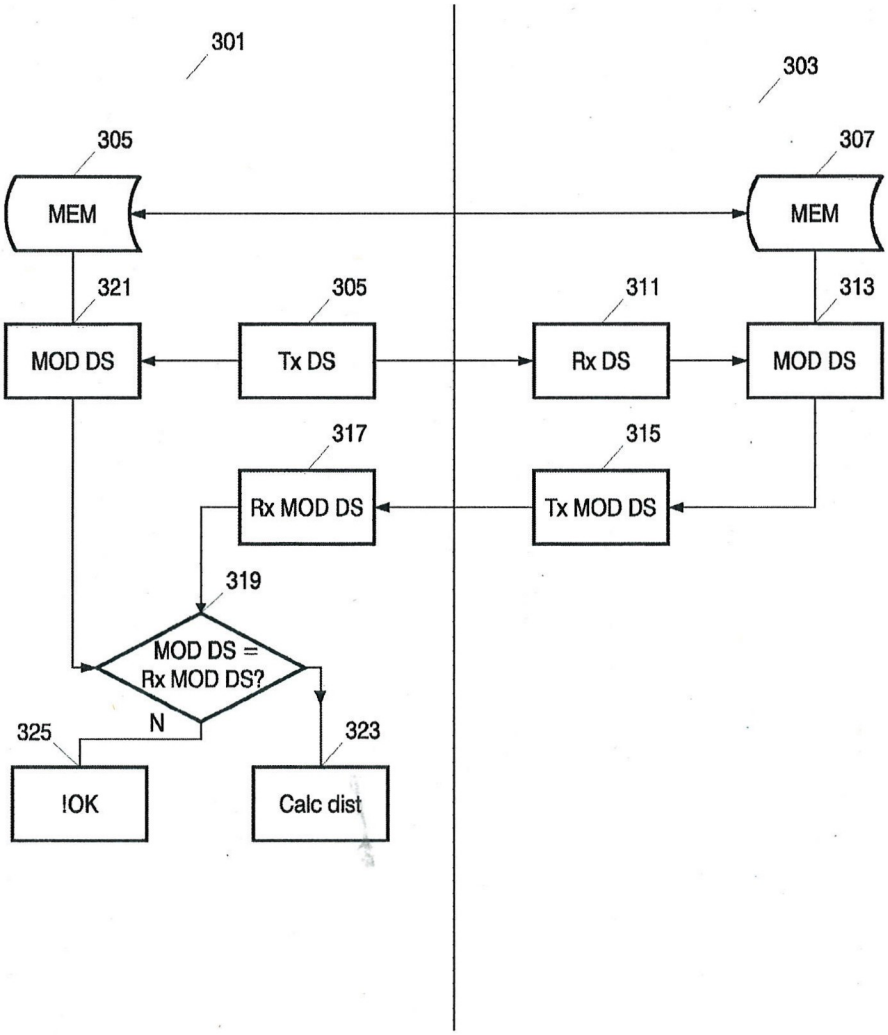


FIG. 3

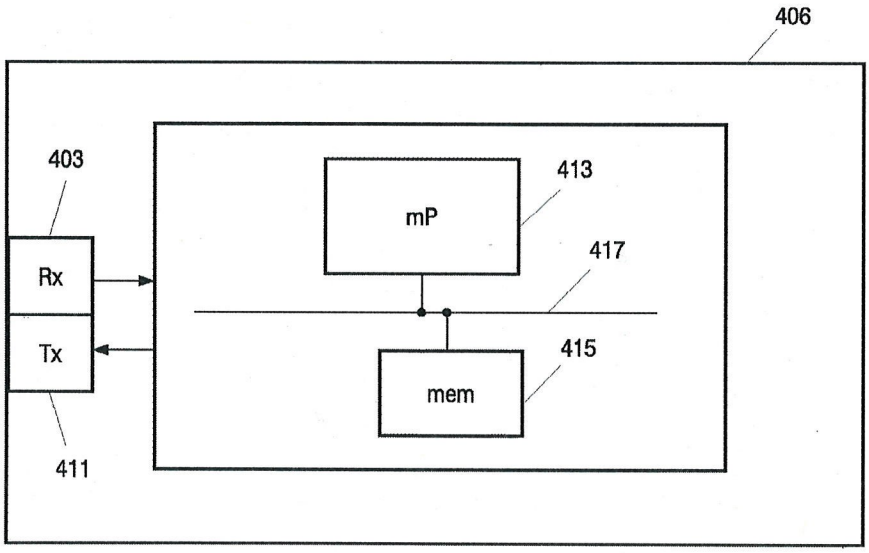


FIG. 4

SECURE AUTHENTICATED DISTANCE MEASUREMENT

This application is a continuation of the patent application entitled "Secure Authenticated Distance Measurement", filed on Nov. 16, 2016 and afforded Ser. No. 15/352,646 which is a continuation of the application filed Aug. 5, 2016 and afforded Ser. No. 15/229,207 which is a continuation of the application filed Nov. 11, 2014 and afforded Ser. No. 14/538,493 which claims priority pursuant to 35 USC 120, priority to and the benefit of the earlier filing date of, that patent application entitled "Secure Authenticated Distance Measurement", filed on Jan. 21, 2005 and afforded Ser. No. 10/521,858 (now U.S. Pat. No. 8,886,939), which claimed priority to and the benefit of the earlier filing date, as a National Stage Filing of that international patent application filed on Jun. 27, 2003 and afforded serial number PCT/IB2003/02932 (WO2004014037), which claimed priority to and the benefit of the earlier filing date of that patent application filed on Jul. 26, 2002 and afforded serial number EP 02078076.3, the contents of all of which are incorporated by reference, herein.

This application is further related to that patent application entitled "Secure authenticated Distance Measurement", filed on Jul. 24, 2009 and afforded Ser. No. 12/508,917 (now U.S. Pat. No. 8,543,819), issued Sep. 24, 2013), which claimed priority to and the benefit of the earlier filing date of that patent application entitled "Secure Authenticated Distance Measurement", filed on Jan. 21, 2005 and afforded Ser. No. 10/521,858 (now U.S. Pat. No. 8,886,939), the contents of which are incorporated by reference herein.

The invention relates to a method for a first communication device to performing authenticated distance measurement between a first communication device and a second communication device. The invention also relates to a method of determining whether data stored on a first communication device is to be accessed by a second communication device. Moreover, the invention relates to a communication device for performing authenticated distance measurement to a second communication device. The invention also relates to an apparatus for playing back multimedia content comprising a communication device.

Digital media have become popular carriers for various types of data information. Computer software and audio information, for instance, are widely available on optical compact disks (CDs) and recently also DVD has gained in distribution share. The CD and the DVD utilize a common standard for the digital recording of data, software, images, and audio. Additional media, such as recordable discs, solid-state memory, and the like, are making considerable gains in the software and data distribution market.

The substantially superior quality of the digital format as compared to the analog format renders the former substantially more prone to unauthorized copying and pirating, further a digital format is both easier and faster to copy. Copying of a digital data stream, whether compressed, uncompressed, encrypted or non-encrypted, typically does not lead to any appreciable loss of quality in the data. Digital copying thus is essentially unlimited in terms of multi-generation copying. Analog data with its signal to noise ratio loss with every sequential copy, on the other hand, is naturally limited in terms of multi-generation and mass copying.

The advent of the recent popularity in the digital format has also brought about a slew of copy protection and DRM systems and methods. These systems and methods use

technologies such as encryption, watermarking and right descriptions (e.g. rules for accessing and copying data).

One way of protecting content in the form of digital data is to ensure that content will only be transferred between devices if

- the receiving device has been authenticated as being a compliant device, and
- the user of the content has the right to transfer (move, copy) that content to another device.

If transfer of content is allowed, this will typically be performed in an encrypted way to make sure that the content cannot be captured illegally in a useful format.

Technology to perform device authentication and encrypted content transfer is available and is called a secure authenticated channel (SAC). Although it might be allowed to make copies of content over a SAC, the content industry is very bullish on content distribution over the Internet. This results in disagreement of the content industry on transferring content over interfaces that match well with the Internet, e.g. Ethernet.

Further, it should be possible for a user visiting his neighbor to watch a movie, which he owns, on the neighbor's big television screen. Typically, the content owner will disallow this, but it might become acceptable if it can be proved that a license holder of that movie (or a device that the license holder owns) is near that television screen.

It is therefore of interest to be able to include an authenticated distance measurement when deciding whether content should be accessed or copied by other devices.

In the article by Stefan Brands and David Chaum, "Distance-Bounding protocols", Eurocrypt '93 (1993), Pages 344-359, integration of distance-bounding protocols with public-key identification schemes is described. Here distance measurement is described based on time measurement using challenge and response bits and with the use of a commitment protocol. This does not allow authenticated device compliancy testing and is not efficient when two devices must also authenticate each other.

It is an object of the invention to obtain a solution to the problem of performing a secure transfer of content within a limited distance.

This is obtained by a method for a first communication device to performing authenticated distance measurement between the first communication device and a second communication device, wherein the first and the second communication device share a common secret and the common secret is used for performing the distance measurement between the first and the second communication device.

Because the common secret is being used for performing the distance measurement, it can be ensured that when measuring the distance from the first communication device to the second communication device, it is the distance between the right devices that is being measured.

The method combines a distance measurement protocol with an authentication protocol. This enables authenticated device compliancy testing and is efficient, because a secure channel is anyhow needed to enable secure communication between devices and a device can first be tested on compliancy before a distance measurement is executed.

In a specific embodiment, the authenticated distance measurement is performed according to the following steps,

- transmitting a first signal from the first communication device to the second communication device at a first time t1, the second communication device being adapted for receiving the first signal, generating a second signal by modifying the received first signal

according to the common secret and transmitting the second signal to the first device,

receiving the second signal at a second time t2,

checking if the second signal has been modified according to the common secret,

determining the distance between the first and the second communication device according to a time difference between t1 and t2.

When measuring a distance by measuring the time difference between transmitting and receiving a signal and using a secret, shared between the first and the second communication device, for determining whether the returned signal really originated from the second communication device, the distance is measured in a secure authenticated way ensuring that the distance will not be measured to a third communication device (not knowing the secret). Using the shared secret for modifying the signal is a simple way to perform a secure authenticated distance measurement.

In a specific embodiment the first signal is a spread spectrum signal. Thereby a high resolution is obtained and it is possible to cope with bad transmission conditions (e.g. wireless environments with a lot of reflections).

In another embodiment the step of checking if the second signal has been modified according to the common secret is performed by the steps of,

generating a third signal by modifying the first signal according to the common secret,

comparing the third signal with the received second signal.

This method is an easy and simple way of performing the check, but it requires that both the first communication device and the second communication device know how the first signal is being modified using the common secret.

In a specific embodiment the first signal and the common secret are bit words and the second signal comprises information being generated by performing an XOR between the bit words. Thereby, it is a very simple operation that has to be performed, resulting in demand for few resources by both the first and the second communication device when performing the operation.

In an embodiment the common secret has been shared before performing the distance measurement, the sharing being performed by the steps of,

performing an authentication check from the first communication device on the second communication device by checking whether the second communication device is compliant with a set of predefined compliance rules,

if the second communication device is compliant, sharing the common secret by transmitting the secret to the second communication device.

This is a secure way of performing the sharing of the secret, ensuring that only devices being compliant with compliance rules can receive the secret. Further, the shared secret can afterwards be used for generating a SAC channel between the two devices. The secret could be shared using e.g. key transport mechanisms as described in ISO 11770-3. Alternatively, a key agreement protocol could be used, which e.g. is also described in ISO 11770-3.

In another embodiment the authentication check further comprises checking if the identification of the second device is compliant with an expected identification. Thereby, it is ensured that the second device really is the device that it should be. The identity could be obtained by checking a certificate stored in the second device.

The invention also relates to a method of determining whether data stored on a first communication device are to be accessed by a second communication device, the method comprising the step of performing a distance measurement between the first and the second communication device and checking whether the measured distance is within a predefined distance interval, wherein the distance measurement is an authenticated distance measurement according to the above. By using the authenticated distance measurement in connection with sharing data between devices, unauthorized distribution of content can be reduced.

In a specific embodiment the data stored on the first device is sent to the second device if it is determined that the data stored on the first device are to be accessed by the second device.

The invention also relates to a method of determining whether data stored on a first communication device are to be accessed by a second communication device, the method comprising the step of performing a distance measurement between a third communication device and the second communication device and checking whether the measured distance is within a predefined distance interval, wherein the distance measurement is an authenticated distance measurement according to the above. In this embodiment, the distance is not measured between the first communication device, on which the data are stored, and the second communication device. Instead, the distance is measured between a third communication device and the second communication device, where the third communication device could be personal to the owner of the content.

The invention also relates to a communication device for performing authenticated distance measurement to a second communication device, where the communication device shares a common secret with the second communication device and where the communication device comprises means for measuring the distance to the second device using the common secret.

In an embodiment the device comprises:

means for transmitting a first signal to a second communication device at a first time t1, the second communication device being adapted for receiving the first signal, generating a second signal by modifying the received first signal according to the common secret and transmitting the second signal,

means for receiving the second signal at a second time t2,

means for checking if the second signal has been modified according to the common secret, and

means for determining the distance between the first and the second communication device according to a time difference between t1 and t2.

The invention also relates to an apparatus for playing back multimedia content comprising a communication device according to the above.

In the following preferred embodiments of the invention will be described referring to the figures, wherein:

FIG. **1** illustrates authenticated distance measurement being used for content protection,

FIG. **2** is a flow diagram illustrating the method of performing authenticated distance measurement,

FIG. **3** illustrates in further detail the step of performing the authenticated distance measurement shown in FIG. **2**,

FIG. **4** illustrates a communication device for performing authenticated distance measurement.

FIG. **1** illustrates an embodiment where authenticated distance measurement is being used for content protection. In the center of the circle **101** a computer **103** is placed. The computer comprises content, such as multimedia content

being video or audio, stored on e.g. a hard disk, DVD or a CD. The owner of the computer owns the content and therefore the computer is authorized to access and present the multimedia content for the user. When the user wants to make a legal copy of the content to another device via e.g. a SAC, the distance between the other device and the computer **103** is measured and only devices within a predefined distance illustrated by the devices **105**, **107**, **109**, **111**, **113** inside the circle **101** are allowed to receive the content. Whereas the devices **115**, **117**, **119** having a distance to the computer **101** being larger than the predefined distance are not allowed to receive the content.

In the example a device is a computer, but it could e.g. also be a DVD drive, a CD drive or a Video, as long as the device comprises a communication device for performing the distance measurement.

In a specific example the distance might not have to be measured between the computer, on which the data are stored, and the other device, it could also be a third device e.g. a device being personal to the owner of the content which is within the predefined distance.

In FIG. **2** a flow diagram illustrates the general idea of performing authenticated distance measurement between two devices, **201** and **203** each comprising communication devices for performing the authenticated distance measurement. In the example the first device **201** comprises content which the second device **203** has requested. The authenticated distance measurement then is as follows. In step **205** the first device **201** authenticates the second device **203**; this could comprise the steps of checking whether the second device **203** is a compliant device and might also comprise the step of checking whether the second device **203** really is the device identified to the first device **201**. Then in step **207**, the first device **201** exchanges a secret with the second device **203**, which e.g. could be performed by transmitting a random generated bit word to second device **203**. The secret should be shared securely, e.g. according to some key management protocol as described in e.g. ISO 11770.

Then in step **209**, a signal for distance measurement is transmitted to the second device **203**; the second device modifies the received signal according to the secret and retransmits the modified signal back to the first device. The first device **201** measures the round trip time between the signal leaving and the signal returning and checks if the returned signal was modified according to the exchanged secret. The modification of the returned signal according to some secret will most likely be dependent on the transmission system and the signal used for distance measurement, i.e. it will be specific for each communication system (such as 1394, Ethernet, Bluetooth, IEEE 802.11, etc.).

The signal used for the distance measurement may be a normal data bit signal, but also special signals other than for data communication may be used. In an embodiment spread spectrum signals are used to be able to get high resolution and to be able to cope with bad transmission conditions (e.g. wireless environments with a lot of reflections).

In a specific example a direct sequence spread spectrum signal is used for distance measurement; this signal could be modified by XORing the chips (e.g. spreading code consisting of 127 chips) of the direct sequence code by the bits of the secret (e.g. secret consists also of 127 bits). Also, other mathematical operations as XOR could be used.

The authentication **205** and exchange of secret **207** could be performed using the protocols described in some known ISO standards ISO 9798 and ISO 11770. For example the first device **201** could authenticate the second device **203** according to the following communication scenario:

First device→Second device: R_B||Text 1
where R_B is a random number
Second device→First device: CertA||TokenAB
Where CertA is a certificate of A
TokenAB=R_A||R_B||B||Text3||sS_A(R_A||R_B||B||Text2)
R_A is a random number
Indentifier B is an option
sS_A is a signature set by A using private key S_A
If TokenAB is replaced with the token as specified in ISO 11770-3 we at the same time can do secret key exchange. We can use this by substituting Text2 by:
Text2:=eP_B(A||K||Text2)||Text3
Where eP_B is encrypted with Public key B
A is identifier of A
K is a secret to be exchanged

In this case the second device **203** determines the key (i.e. has key control), this is also called a key transport protocol, but also a key agreement protocol could be used. This may be undesirable in which case it can be reversed, such that the first device determines the key. A secret key has now been exchanged according to step **207** in FIG. **2**. Again, the secret key could be exchanged by e.g. a key transport protocol or a key agreement protocol.

After the distance has been measured in a secure authenticated way as described above content, data can be sent between the first and the second device in step **211** in FIG. **2**.

FIG. **3** illustrates in further detail the step of performing the authenticated distance measurement. As described above the first device **301** and the second device **303** have exchanged a secret; the secret is stored in the memory **305** of the first device and the memory **307** of the second device. In order to perform the distance measurement, a signal is transmitted to the second device via a transmitter **309**. The second device receives the signal via a receiver **311** and **313** modifies the signal by using the locally stored secret. The signal is modified according to rules known by the first device **301** and transmitted back to the first device **301** via a transmitter **315**. The first device **301** receives the modified signal via a receiver **317** and in **319** the received modified signal is compared to a signal, which has been modified locally. The local modification is performed in **321** by using the signal transmitted to the second device in transmitter **309** and then modifying the signal using the locally stored secret similar to the modification rules used by the second device. If the received modified signal and the locally modified signal are identical, then the received signal is authenticated and can be used for determining the distance between the first and the second device. If the two signals are not identical, then the received signal cannot be authenticated and can therefore not be used for measuring the distance as illustrated by **325**. In **323** the distance is calculated between the first and the second device; this could e.g. be performed by measuring the time, when the signal is transmitted by the transmitter **309** from the first device to the second device and measuring when the receiver **317** receives the signal from the second device. The time difference between transmittal time and receive time can then be used for determining the physical distance between the first device and the second device.

In FIG. **4** a communication device for performing authenticated distance measurement is illustrated. The device **401** comprises a receiver **403** and a transmitter **411**. The device further comprises means for performing the steps described above, which could be by executing software using a microprocessor **413** connected to memory **415** via a communication bus **417**. The communication device could then be

placed inside devices such as a DVD, a computer, a CD, a CD recorder, a television and other devices for accessing protected content.

The invention claimed is:

1. A second device for receiving delivery of a protected content from a first device, the second device comprising a processor circuit, the processor circuit arranged to execute instructions, the instructions arranged to:

provide a certificate to the first device prior to receiving a first signal, wherein the first signal is sent by the first device, wherein the certificate is associated with the second device;

receive the first signal when the certificate indicates that the second device is compliant with at least one compliance rule;

create a second signal, wherein the second signal is derived from a secret known by the second device;

provide the second signal to the first device after receiving the first signal, wherein the second signal is received by the first device; and

receive the protected content from the first device when the first device determines that the second signal is derived from the secret and a time between the sending of the first signal and the receiving of the second signal is less than a predetermined time.

2. The second device of claim 1, wherein the secret is securely provided to the second device by the first device.

3. The second device of claim 2, wherein determining that the second signal is derived from the secret comprises:

modifying the first signal, wherein the modifying requires the secret; and

determining that the modified first signal is identical to the second signal.

4. The second device of claim 2, wherein determining that the second signal is derived from the secret comprises:

modifying the first signal; and

determining that the modified first signal is identical to the second signal.

5. The second device of claim 2, wherein the predetermined time is based on a communication system associated with the first device.

6. The second device of claim 2, further comprising instructions arranged to receive the secret from the first device.

7. The second device of claim 2, wherein the second signal comprises the first signal modified by the secret.

8. The second device of claim 2, wherein the secret comprises a random number.

9. The second device of claim 2, wherein the secret is encrypted with a public key.

10. The second device of claim 2, wherein the first signal comprises a random number.

11. The second device of claim 2, wherein the second signal comprises an XOR operation of the first signal with the secret.

12. The second device of claim 2, wherein determining that the second signal is derived from the secret comprises:

modifying the second signal, wherein the modifying requires the secret; and

determining that the modified second signal is identical to the first signal.

13. The second device of claim 2, wherein determining that the second signal is derived from the secret comprises:

modifying the second signal; and

determining that the modified second signal is identical to the first signal.

14. The second device of claim 2, wherein the secret is used for generating a secure channel between the first device and the second device.

15. The second device of claim 1, wherein determining that the second signal is derived from the secret comprises:

modifying the first signal, wherein the modifying requires the secret; and

determining that the modified first signal is identical to the second signal.

16. The second device of claim 1, wherein determining that the second signal is derived from the secret comprises:

modifying the first signal; and

determining that the modified first signal is identical to the second signal.

17. The second device of claim 1, wherein the predetermined time is based on a communication system associated with the first device.

18. The second device of claim 1, further comprising instructions arranged to receive the secret from the first device.

19. The second device of claim 1, wherein the second signal comprises the first signal modified by the secret.

20. The second device of claim 1, wherein the secret comprises a random number.

21. The second device of claim 1, wherein the secret is encrypted with a public key.

22. The second device of claim 1, wherein the first signal comprises a random number.

23. The second device of claim 1, wherein the second signal comprises an XOR operation of the first signal with the secret.

24. The second device of claim 1, further comprising instructions arranged to provide the secret to the first device.

25. The second device of claim 1, wherein the secret is used for generating a secure channel between the first device and the second device.

26. The second device of claim 1, wherein determining that the second signal is derived from the secret comprises:

modifying the second signal, wherein the modifying requires the secret; and

determining that the modified second signal is identical to the first signal.

27. The second device of claim 1, wherein determining that the second signal is derived from the secret comprises:

modifying the second signal; and

determining that the modified second signal is identical to the first signal.

28. The second device of claim 1, wherein the secret is known by the first device.

29. A method of receiving a protected content sent from a first device to a second device, the second device comprising a processor circuit, the processor circuit arranged to execute instructions implementing the method, the method comprising:

providing a certificate to the first device prior to receiving a first signal, wherein the first signal is sent by the first device, wherein the certificate is associated with the second device;

receiving the first signal form the first device when the certificate indicates that the second device is compliant with at least one compliance rule;

creating a second signal, wherein the second signal is derived from a secret known by the second device;

providing the second signal to the first device after receiving the first signal, wherein the second signal is received by the first device;

receiving the protected content from the first device when the first device determines that the second signal is derived from the secret and a time between the sending of the first signal and the receiving of the second signal is less than a predetermined time.

30. The method of claim **29**, wherein the secret is securely provided to the second device by the first device.

31. The method of claim **30**, wherein determining that the second signal is derived from the secret comprises:

modifying the first signal, wherein the modifying requires the secret; and

determining that the modified first signal is identical to the second signal.

32. The method of claim **31**, wherein the second signal comprises an XOR operation of the first signal with the secret.

33. The method of claim **31**, wherein the secret comprises a first random number.

34. The method of claim **33**, wherein the secret is used for generating a secure channel between the first device and the second device.

35. The method of claim **33**, wherein the secret is encrypted with a public key.

36. The method of claim **35**, wherein the first signal comprises a second random number.

37. The method of claim **30**, wherein determining that the second signal is derived from the secret comprises:

modifying the first signal; and

determining that the modified first signal is identical to the second signal.

38. The method of claim **30**, wherein the second signal comprises the first signal modified by the secret.

39. The method of claim **30**, wherein determining that the second signal is derived from the secret comprises:

modifying the second signal, wherein the modifying requires the secret; and

determining that the modified second signal is identical to the first signal.

40. The method of claim **30**, wherein determining that the second signal is derived from the secret comprises:

modifying the second signal, wherein the modifying requires the secret; and

determining that the modified second signal is identical to the first signal.

41. The method of claim **29**, wherein determining that the second signal is derived from the secret comprises:

modifying the first signal, wherein the modifying requires the secret; and

determining that the modified first signal is identical to the second signal.

42. The method of claim **29**, wherein determining that the second signal is derived from the secret comprises:

modifying the first signal; and

determining that the modified first signal is identical to the second signal.

43. The method of claim **29**, wherein the predetermined time is based on a communication system associated with the first device.

44. The method of claim **29**, further comprising receiving the secret from the first device.

45. The method of claim **29**, wherein the second signal comprises the first signal modified by the secret.

46. The method of claim **29**, wherein the secret comprises a random number.

47. The method of claim **29**, wherein the secret is encrypted with a public key.

48. The method of claim **29**, wherein the first signal comprises a random number.

49. The method of claim **29**, wherein the second signal comprises an XOR operation of the first signal with the secret.

50. The method of claim **29**, further comprising providing the secret to the first device.

51. The method of claim **29**, wherein the secret is used for generating a secure channel between the first device and the second device.

52. The method of claim **29**, wherein determining that the second signal is derived from the secret comprises:

modifying the second signal, wherein the modifying requires the secret; and

determining that the modified second signal is identical to the first signal.

53. The method of claim **29**, wherein determining that the second signal is derived from the secret comprises:

modifying the second signal; and

determining that the modified second signal is identical to the first signal.

* * * * *

EXHIBIT B

U.S. Patent No. 10,298,564

LG Product / Realtek Product

REDACTED