NOTE: This disposition is nonprecedential.

United States Court of Appeals for the Federal Circuit

INTEL CORPORATION,
Appellant

v.

KONINKLIJKE PHILIPS N.V.,
Appellee

2022-2034, 2022-2035

Appeals from the United States Patent and Trademark Office, Patent Trial and Appeal Board in Nos. IPR2021-00327, IPR2021-00370.

Decided: February 22, 2024

CHRISTINA JORDAN MCCULLOUGH, Perkins Coie LLP, Seattle, WA, argued for appellant. Also represented by LORI ANN GORDON, NATHAN K. KELLEY, Washington, DC; TARA LAUREN KURTIS, Chicago, IL.

PETER F. SNELL, Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, PC, New York, NY, argued for appellee. Also represented by WILLIAM MEUNIER, MICHAEL RENAUD, Boston, MA.

Before PROST, TARANTO, and CHEN, *Circuit Judges*.

CHEN, *Circuit Judge*.

Intel Corporation (Intel) filed two petitions for *inter partes* review of several claims of U.S. Patent No. 9,436,809 ('809 patent). These petitions challenged the claims for being unpatentable as obvious over two distinct combinations of references: (1) Menezes[1] in view of Brands-Chaum,[2] and (2) OCPS[3] in view of Brands-Chaum. The Board's final written decisions found that Intel had failed to show by a preponderance of the evidence that the challenged claims were unpatentable. Intel appeals these decisions, and we have jurisdiction under 28 U.S.C. § 1295(a)(4)(A). We *affirm*.

First, we reject Intel's argument that the Board failed to address the unpatentability grounds as articulated in the petitions. According to Intel, rather than considering whether it would have been obvious to incorporate the broad distance-measurement concept allegedly taught in Brands-Chaum into Menezes's or OCPS's authentication protocol, the Board's final written decisions reversed the references—evaluating whether it would have been

---

[1] ALFRED J. MENEZES ET AL., HANDBOOK OF APPLIED CRYPTOGRAPHY (1997).

[2] Stefan Brands & David Chaum, *Distance-Bounding Protocols*, EUROCRYPT '93, 344–59 (1994).

[3] Open Copy Protection System, Philips Research Proposal to Broadcast Protection Discussion Group, Version 1.4 (May 7, 2002); OCPS Compliance and Robustness Rules (May 7, 2002). In this opinion, "OCPS" refers to two separate documents describing the Open Copy Protection System protocol. The parties do not dispute that OCPS can be treated as a single publication, i.e., as a single primary reference.

obvious to modify Brands-Chaum's specific example of a distance-bounding protocol to use Menezes's or OCPS's multi-bit message. We disagree. The Board expressly acknowledged that Intel's proposed combinations involved timing Menezes's and OCPS's multi-bit challenge-response exchanges to calculate a distance between devices or enforce a distance limit. J.A. 17–18, 29; J.A. 47. The Board then found that transmitting multiple bits, instead of a single bit, would have resulted in an inaccurate distance measurement and would have impaired security. J.A. 21, 31; J.A. 57. In other words, the Board correctly understood the proposed combinations and identified deficiencies associated with these combinations. The Board's final written decisions thus squarely addressed the obviousness theories advanced in the petitions.

Second, substantial evidence supports the Board's determination that Brands-Chaum's teachings are incompatible with Menezes's and OCPS's multi-bit exchanges. The Board emphasized that Intel did not reconcile the conflict between Menezes's and OCPS's disclosures directed to multi-bit exchanges and Brands-Chaum's disclosure that an "*essential* element" of its distance-bounding protocol "consists of a *single-bit* challenge and rapid *single-bit* response." J.A. 3212 (emphases added); *see* J.A. 23, 31–32; J.A. 59. The Board further found that timing a multi-bit message would result in unwanted delays and that such delays would impair security, crediting Intel's expert testimony explaining that (1) Brands-Chaum's prover device immediately responds to a challenge so that propagation delay dominates the time being timed by a verifier device, (2) propagation delay has an "iron-clad relationship between distance and time," (3) sending a multi-bit message takes longer than sending a single-bit message, and (4) an unwanted delay of just nanoseconds could cause a message to travel meters. J.A. 21–22, 31–32, 32 n.19; J.A. 57–59, 59 n.13. This amounts to substantial evidence for the Board's determination that transmitting a multi-bit message

would create unwanted delays, which in turn would render the distance measurement inaccurate and impair security. We see no reason on this record to disturb the Board's findings that Brands-Chaum's teachings are incompatible with Menezes's and OCPS's multi-bit authentication protocols.

We have considered Intel's remaining arguments—including Intel's contention that the Board should have found a motivation to combine notwithstanding the delay and security issues associated with timing a multi-bit message—and find them unpersuasive. For the foregoing reasons, we *affirm*.

AFFIRMED