

The opinion in support of the decision being entered today was *not* written for publication and is *not* binding precedent of the Board.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte SARVER PATEL

Appeal 2007-0246
Application 09/854,251
Technology Center 2100

Decided: March 27, 2007

Before KENNETH W. HAIRSTON, JOSEPH L. DIXON, and JAY P.
LUCAS, *Administrative Patent Judges*.
DIXON, *Administrative Patent Judge*.

DECISION ON APPEAL

This is a decision on appeal under 35 U.S.C. § 134 from the Examiner's final rejection of claims 1-4, 7-11, 14, 16, and 19-21.

We AFFIRM.

BACKGROUND

Appellant's invention relates to a message authentication system and method using a single iteration of a keyed compression function when a message fits within the input block. For larger messages, the method and system additionally uses a nested hash function. An understanding of the invention can be derived from a reading of exemplary claim 1, which is reproduced below.

1. A method of processing a message for authentication, said method comprising:

determining whether said message fits within an input block of a compression function;

performing a single iteration of the compression function using a key and said message as inputs when said message fits within an input block of said compression function and using a result from said compression function without further iteration thereof to produce a message authentication code; and

using a hash function nested within a keyed hash function to process said message when said message does not fit within an input block of said compression function and using a result from said keyed hash function to produce a message authentication code. .

PRIOR ART

The prior art reference of record relied upon by the Examiner in rejecting the appealed claims is:

Appeal 2007-0246
Application 09/854,251

Bellare et al., “Keying Hash Functions for Message Authentication”, Preliminary Version: *Advances in Cryptology – Crypto 96 Proceedings, Lecture Notes in Computer Science*, Vol. 1109, Springer-Verlag, (June 1996), pp. 1-19.

REJECTION

Claims 1-4, 7-11, 14, 16, and 19-21 stand rejected under 35 U.S.C. 102 as being anticipated by Bellare.

Rather than reiterate the conflicting viewpoints advanced by the Examiner and the Appellant regarding the above-noted rejection, we make reference to the Examiner's Answer (mailed Jun. 14, 2006) for the reasoning in support of the rejections, and to Appellant's Brief (filed Mar. 20, 2006) for the arguments thereagainst.

OPINION

In reaching our decision in this appeal, we have given careful consideration to Appellant's Specification and claims, to the applied prior art reference, and to the respective positions articulated by Appellant and the Examiner. As a consequence of our review, we make the determinations that follow.

35 U.S.C. § 102

A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference. *Verdegaal Bros. Inc. v. Union Oil Co.*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). The inquiry as to whether a reference anticipates a claim must focus on what subject matter is encompassed by the claim and what subject matter is described by the reference. As set forth by

the court in *Kalman v. Kimberly-Clark Corp.*, 713 F.2d 760, 772, 218 USPQ 781, 789 (Fed. Cir. 1983), it is only necessary for the claims to “‘read on’ something disclosed in the reference, i.e., all limitations of the claim are found in the reference, or ‘fully met’ by it.” While all elements of the claimed invention must appear in a single reference, additional references may be used to interpret the anticipating reference and to shed light on its meaning, particularly to those skilled in the art at the relevant time. *See Studiengesellschaft Kohle v. Dart Indus., Inc.*, 726 F.2d 724, 726-727, 220 USPQ 841, 842-843 (Fed. Cir. 1984).

The Examiner maintains that Bellare teaches the claimed invention as recited in independent claim 1. The Examiner has identified that various pages of Bellare teach the recited limitations of independent claim 1 (Br. 3-4 and 6-7). We find that the Examiner has established a prima facie case of anticipation of the claimed invention. Therefore, we look to Appellant’s Brief to show error in this prima facie case.

Appellant contends that the Examiner erred in finding anticipation by Bellare, but Appellant does not address the merits of the specific teachings recited in Bellare. Rather, Appellant contends that the totality of the merits of teachings of Bellare are encapsulated within Appellant’s discussions of the NMAC and HMAC in the background of the instant Specification. We cannot agree with Appellant, and we find that Appellant’s arguments to the Appellant’s Admitted Prior Art (AAPA) do not address the merits of the instant rejection under review based upon the teachings of Bellare.

We find that Appellant’s arguments to AAPA Figures 6-8 at page 5-7 of the Brief do not identify how the applied prior art reference to Bellare does not teach the claimed invention. The Examiner identifies specific

sections and pages of Bellare at pages 6-8 of the Answer to further illustrate the manner in which the prior art is applied. We find that Appellant does not specifically address the merits of the instant rejection. Since we find that the Examiner had met the initial burden thereby shifting the burden of persuasion to Appellant, and Appellant did not clearly and specifically address those identified teaching in the applied prior art, we will sustain the rejection of independent claim 1 and those claims grouped therewith by Appellant.

We find the same deficiency in the arguments presented by Appellant with respect to independent claims 7 and 19, and we will sustain the rejection of independent claims 7 and 19 and those claims grouped therewith by Appellant. Since Appellant has not shown error in the prima facie case of anticipation, we sustain the rejection of all claims under 35 U.S.C. § 102.

CONCLUSION

To summarize, we have sustained the rejection of claims 1-4, 7-11, 14, 16, and 19-21 stand under 35 U.S.C. § 102.

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

Appeal 2007-0246
Application 09/854,251

AFFIRMED

JLD

ELD

Docket Administrator (Room 3C-512)
Lucent Technologies Inc.,
600 Mountain Avenue
P.O. Box 636
Murray Hill NJ 07974-0636