

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 ALAIN BENAYOUN, JEAN-FRANCOIS LE PENNEC  
and PATRICK MICHEL

---

Appeal No. 2006-3095  
Application No. 09/573,527

---

ON BRIEF

---

Before HAIRSTON, BARRY, and MACDONALD, Administrative Patent Judges.

HAIRSTON, Administrative Patent Judge.

This is an appeal from the final rejection of claims 1 through 24.

Appeal No. 2006-3095  
Application No. 09/573,527

The disclosed invention relates to a method and system for updating a secret encryption key in a data communication system. In a data transmitting node of the data communication system, a next secret encryption key to be used to encrypt a next data transmission is derived from a current value of a secret encryption key and an updated database in the transmitting node. In a data receiving node of the data communication system, a next secret decryption key to be used to decode a next data transmission is derived from the contents of a receiving database in the receiving node.

Claims 1 and 8 are illustrative of the claimed invention, and they read as follows:

1. A method of updating a secret encryption key in a data communication system, said method comprising:

a transmitting node receiving clear data;

updating a sending database, in said transmitting node, utilizing said clear data;

in said transmitting node, encrypting said clear data using a current secret encryption key;

transmitting said encrypted data to a receiving node; and

deriving from said current value of said secret encryption key and said updated database in said transmitting node, a next secret encryption key to be used to encrypt a next data transmission.

Appeal No. 2006-3095  
Application No. 09/573,527

8. A method of updating a secret encryption key in a data communication system, said method comprising:

upon receiving encrypted data in a receiving node, decrypting said encrypted data to obtain decrypted data by using a secret decryption key;

updating a receiving database in said receiving node with said decrypted data to synchronize said receiving database to a sending database; and

deriving, from contents of said receiving database in said receiving node, a next secret decryption key to be used to decode a next data transmission.

The references relied on by the examiner are:

Wood	5,003,596	Mar. 26, 1991
Janson et al. (Janson)	5,729,608	Mar. 17, 1998
Hawthorne	5,832,087	Nov. 03, 1998
Moulart et al. (Moulart)	6,031,912	Feb. 29, 2000
York	6,711,709	Mar. 23, 2004 (filed June 24, 1998)

Claims 1, 2, 4, 5, 8 through 10, 12, 13, 16 through 18, 20, 21 and 24 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Hawthorne in view of Wood.

Claims 3, 11 and 19 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Hawthorne in view of Wood and York.

Claims 6, 14 and 22 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Hawthorne in view of Wood and Janson.

Appeal No. 2006-3095  
Application No. 09/573,527

Claims 7, 15 and 23 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Hawthorne in view of Wood and Moulart.

Reference is made to final rejection, the briefs and the answer for the respective positions of the appellants and the examiner.

OPINION

We have carefully considered the entire record before us, and we will reverse the obviousness rejections of claims 1 through 24.

According to the examiner's reasoning (final rejection, pages 3 and 4), Hawthorne discloses all of the method steps and system structure set forth in claims 1, 9 and 17 with the exception of deriving from the current value of the encryption key and the updated database in the transmitting mode, a next secret encryption key to be used to encrypt a next data transmission. The examiner states (final rejection, page 4) that "Wood teaches deriving from said current value of said secret encryption key and said updated database in said transmitting node, a next secret encryption key to be used to encrypt a next data transmission (column 9, lines 7-26)." Based upon the teachings of Wood, the examiner is of the opinion (final rejection, page 4) that "[i]t would have been obvious to one of ordinary skill in the art at the time the invention was made to derive a new key from the current value and the updated database,

Appeal No. 2006-3095  
Application No. 09/573,527

since Wood states at column 9, lines 7-26 that selecting a different key in each round of communications makes it impossible to search for or solve mathematically for one key used repetitively."

Appellants argue inter alia (reply brief, page 2) that:

The cited text of *Hawthorne* discloses that a new set of look-up tables is generated in accordance with a *new, random session key*, but does not disclose deriving the session key, or performing any other operations, "utilizing said clear data", as claimed. Random keys are not data-dependent. Because the Examiner's combination of *Hawthorne* and *Wood* does not teach or suggest "updating a sending database, in said transmitting node, utilizing said clear data", Appellants respectfully submit that the Examiner's rejection under 35 U.S.C. § 103 is not well founded and should be reversed.

We agree with the appellants' arguments. *Hawthorne* uses "[f]or each fresh transmission (or session) between the unit and a corresponding unit at another station, a new set of look-up tables . . . generated in accordance with a new, random session key" (column 2, lines 27 through 31). Stated differently, *Hawthorne* does not use the clear data at input port 12 (Figure 1) to update a sending database. *Wood* is silent as to updating a sending database using clear data, and using the updated database to derive a next secret encryption key. Thus, the obviousness rejection of claims 1, 9 and 17 is reversed because *Hawthorne* and

Appeal No. 2006-3095  
Application No. 09/573,527

Wood are incapable of deriving "a next secret encryption key" based on an "updated database" as required by the noted claims on appeal.

For all of the reasons expressed supra, the obviousness rejection of claims 2, 4, 5, 10, 12, 13, 18, 20 and 21 is likewise reversed.

Turning next to the obviousness rejection of claims 8, 16 and 24, appellants argue (reply brief, page 3) that the combination of Hawthorne and Woods lacks a teaching of "updating a receiving database in said receiving node with said decrypted data to synchronize said receiving database to a sending database," and "deriving, from contents of said receiving database in said receiving node, a next secret decryption key to be used to decode a next data transmission." We agree with the appellants' arguments. Neither Hawthorne nor Wood is concerned with updating a receiving database with decrypted data that is used to synchronize the receiving database to the sending database, and then using the decrypted data in a receiving database to derive a next secret decryption key as required by the claims on appeal. Accordingly, the obviousness rejection of claims 8, 16 and 24 is reversed.

Appeal No. 2006-3095  
Application No. 09/573,527

The obviousness rejections of claims 3, 6, 7, 11, 14, 15, 19, 22 and 23 are reversed because the teachings of York, Janson and Moulart fail to cure the noted shortcomings in the teachings of Hawthorne and Wood.

DECISION

The decision of the examiner rejecting claims 1 through 24 under 35 U.S.C. § 103(a) is reversed.

Appeal No. 2006-3095  
Application No. 09/573,527

REVERSED

KENNETH W. HAIRSTON )  
Administrative Patent Judge )  
 )  
 )  
 )  
 ) BOARD OF PATENT  
LANCE LEONARD BARRY )  
Administrative Patent Judge ) APPEALS AND  
 )  
 ) INTERFERENCES  
 )  
ALLEN R. MACDONALD )  
Administrative Patent Judge )

KWH/ce

Appeal No. 2006-3095  
Application No. 09/573,527

DILLON & YUDELL LLP  
8911 NORTH CAPITAL OF TEXAS HWY  
SUITE 2110  
AUSTIN, TX 78759