UNITED STATES PATENT AND TRADEMARK OFFICE

**UNITED STATES DEPARTMENT OF COMMERCE**
**United States Patent and Trademark Office**
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 15/268,541 | 09/17/2016 | Jianqing Wu | UP168989 | 8440 |

30795 7590 06/29/2020

AZ PATENT LAW FIRM
P.O. Box 689
Beltsville, MD 20704

| EXAMINER | |
|---|---|
| WILCOX, JAMES J | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2439 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 06/29/2020 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE PATENT TRIAL AND APPEAL BOARD

---

*Ex parte* JIANQING WU

---

Appeal 2019-002042
Application 15/268,541
Technology Center 2400

---

Before CARL W. WHITEHEAD JR., MICHAEL M. BARRY, and PHILLIP A. BENNETT, *Administrative Patent Judges.*

BENNETT, *Administrative Patent Judge.*

## DECISION ON APPEAL

## STATEMENT OF THE CASE

Pursuant to 35 U.S.C. § 134(a), Appellant[1] appeals from the Examiner's decision to reject claims 24–43. Claim 1–23 have been cancelled. We have jurisdiction under 35 U.S.C. § 6(b).

We reverse.

---

[1] We use the word "Appellant" to refer to "applicant" as defined in 37 C.F.R. § 1.42(a). Appellant identifies the real party in interest as Jianqing Wu, who is the sole inventor and current sole owner of the application on appeal. Appeal Br. 2.

## CLAIMED SUBJECT MATTER

The claims are directed to an encryption synchronization method. Appellant's claimed method seeks to increase data security for server-based data storage by storing encryption keys exclusively with the client device, such that the server does maintain access to the encryption keys. By storing encryption keys exclusively on the client device, hackers are unable to obtain access to encrypted stored data even if they are able to compromise the storage server. Spec. 6, ll.15–7, ll. 2.

The claimed process employs an "encrypted mark," which is an item of data that is known and identifiable to the client user in order to authenticate a client to the server. As explained in the Specification, "[a]n encryption mark is used for testing if the user knows the common encryption key." Spec. 25, ll. 7–8. The encrypted mark can be a specific image, a sound file, or simply written expression such as, for example, "Encryption Key is OK." Spec. 25, ll. 16–25.

Claim 24 recites a process of a client setting up the encrypted mark by selecting the mark and encrypting it using an encryption algorithm and encryption key selected by the client. The encrypted mark is sent to the server where it is stored in its encrypted form. When a client seeks to authenticate to the server, the client device does so by retrieving the encrypted mark from the server and supplying an encryption key to the server, which is used to decrypt the encrypted mark. The resultant decrypted mark is then compared to the original, unencrypted mark that was used to create the encrypted mark. If the decrypted mark and the original, unencrypted mark match, the match confirms that the client submitted the

correct encryption key and correct encryption algorithm, and the client is authenticated to the server.

Claim 24 is reproduced below:

> 24. A method for encryption synchronization and/or user authentication, the method being used in a system comprising at least one server and at least one client computer, both the at least one server and the at least one client computer being connected to a network or the Internet, the method comprising the steps of:
>
> setting up an encrypted mark, wherein the setup step further comprises the operational steps of (1) selecting a suitable mark, (2) providing an encryption key, (3) sending the mark and the encryption key to one of the at least one server, (4) encrypting the mark with an encryption algorithm and the encryption key on the server, and (5) saving the encrypted mark in a designed storage location or a database on the server or the operational steps of (1) selecting a suitable mark, (2) providing an encryption key, (3) encrypting the mark with an encryption algorithm and the encryption key on the client computer, (4) sending the encrypted mark to the server, and (5) saving the encrypted mark in a designed storage location or a database on the server; and
>
> determining if an encryption algorithm as a current encryption algorithm and an encryption key as a current encryption key are the same as or compatible with the encryption algorithm and the encryption key used to create the encrypted mark, wherein the determining step comprises retrieving the encrypted mark from the server, getting an encryption key stored on the client computer or entered by a user, decrypting the encrypted mark using the encryption key on the server to generate a resulted mark, and comparing the resulted mark with the mark used to create the encrypted mark, wherein, upon receiving a confirmation of the user or a confirmation of the client computer, or upon a determination by the server, the server accepts the current encryption algorithm and the current encryption key as same as the encryption algorithm and the encryption key used to create the encrypted mark, and/or authenticates the user.

Appeal Br. 46–47 (Claims Appendix).

REFERENCES

The prior art relied upon by the Examiner is:

| Name | Reference | Date |
|---|---|---|
| Wu | US 9,449,183 B2 | Sept. 20, 2016 |
| Levi | US 2007/0208803 A1 | Sept. 6, 2007 |
| Pritikin | US 2008/0082821 A1 | Apr. 3, 2008 |
| Schneider | US 2010/0223456 A1 | Sept. 2, 2010 |

REJECTIONS

Claims 24–43 of the instant application are rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1–23 of Wu. Final Act. 7.

Claim(s) 24, 26–32 and 35–42 stand rejected under 35 U.S.C. § 102(b) as being anticipated by Pritikin. Final Act. 9.

Claims 25 and 43 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Pritikin and Schneider. Final Act. 23.

Claims 33 and 34[2] stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Pritikin and Levi. Final Act. 25.

[2] The statement of the rejection does not list claims 33 and 34, however the body of the rejection addresses both claims. Accordingly, we consider the omission of claim 33 and 34 from the statement of the rejection to be a typographical error.

## ISSUES

*First Issue:* Has the Examiner erred in rejecting the claims for double patenting?

*Second Issue:* Has the Examiner erred in finding Pritikin anticipates claim 1?

## ANALYSIS

### *First Issue*

The Examiner rejects the pending claims for obviousness-type double patenting based on Appellant's previously issued U.S. Patent No. 9,449,183 B2 ("the '183 patent"), the parent of the instant application. The Examiner finds "[c]laims 24–43 of the instant application contain substantially similar features of claims 1–23 of US Patent No: 9,449,183 B2 and as such a[re] obvious variants of claims 1-23 of the patent." Final Act. 7.

Appellant asserts the double patenting rejection is in error because the pending claims are not obvious variants of the previously issued claims, and in fact are substantially different. Appeal Br. 30 ("However, the subject claimed in the parent and the subject which is claimed now are like a new car and a special carburetor.").

We agree the Examiner has not established double patenting in this instance. Under the policy of the Office:

> Any obviousness-type double patenting rejection should make clear
>
> (A) The differences between the inventions defined by the conflicting claims — a claim in the patent compared to a claim in the application; and
>
> (B) The reasons why a person of ordinary skill in the art would conclude that the invention defined in the claim at issue is

> anticipated by, or would have been an obvious variation of, the invention defined in a claim in the patent.

MPEP § 804(II)(B)(1).

Here, the Examiner has not provided sufficient analysis setting forth the reasons the pending claims would have been obvious over the claims of the '183 patent. Final Act. 7–8. The Examiner does not meaningfully compare the limitations of the two patents, and instead makes a generalized assertion that there are certain similarities between them. *Id.* The burden is on the Examiner in the first instance to set forth sufficient evidence and reasoning in support of the double patenting rejection. That burden has not been met, and we do not sustain the double patenting rejection.

*Second Issue*

The Examiner rejects claim 24 as being anticipated by Pritikin. The Examiner finds all of the limitations disclosed in Pritikin. Final Act. 9–11 (citing Pritikin, Figs. 2A–4, ¶¶ 13–17, 26, 40–44). Appellant generally contends the process described by Pritikin differs fundamentally from the claimed process because Pritikin discloses storing the same encryption key on both the client and the server. Appeal Br. 12–14. More specifically, Appellant argues several limitations are not disclosed in Pritikin, including the limitation "getting an encryption key stored on the client computer or entered by a user, decrypting the encrypted mark using the encryption key on the server to generate a resulted mark, and comparing the resulted mark with the mark used to create the encrypted mark." *Id.* Appellant asserts that any comparison made by Pritikin is a comparison of encrypted cipher text generated by encrypting data with a shared encryption key. Appeal Br. 14 (citing Pritikin ¶ 31); Reply Br. 6 (citing Pritikin ¶ 41). We agree with Appellant.

Anticipation is a test of strict identity. *Trintec Indus., Inc. v. Top-U.S.A. Corp.*, 295 F.3d 1292, 1296 (Fed. Cir. 2002). That is, to meet the strict identity test for anticipation, all elements must be disclosed in exactly the same way as they are arranged or combined in the claim. *Therasense, Inc. v. Becton, Dickinson & Co.*, 593 F.3d 1325, 1332 (Fed. Cir. 2010). In this instance, the Examiner's findings fail to meet this exacting requirement.

Pritikin describes a bi-directionally authenticated connection protocol for securely transmitting sensitive data. Pritikin ¶ 14. Pritikin discloses that a server sends a challenge to a client in an effort to ascertain the identity of the client. Pritikin ¶ 30. The client device encrypts the challenge using a secret key and sends the encrypted challenge back to the server as a challenge response. Pritikin ¶ 31. Pritikin further describes the "server may perform the same encryption algorithm on the first challenge and may compare the result to the first response. If the first response matches the encrypted first challenge, then the client has been authenticated." *Id.* (reference numerals omitted). Thus, Pritikin describes comparing *encrypted* data to authenticate a client. The disputed limitation, however, requires that unencrypted data be the subject of comparison: "decrypting the encrypted mark using the encryption key . . . to generate a resulted mark, and comparing the resulted mark with the mark used to create the encrypted mark." Accordingly, Pritikin's comparison is not the same as what is claimed.

In the remaining paragraphs of Pritikin cited by the Examiner, Pritikin discloses an alternate embodiment in which a client device submits a username and password to a server for authentication purposes. Ans. 3–4 (citing Pritikin ¶¶ 40–44). In the embodiment, the client adds a nonce to the

password and encrypts the password/nonce combination and sends it as a challenge to the server. Pritikin ¶ 41. The server receives the encrypted password/nonce combination and decrypts the combination using "a secret key or stored password." *Id.* However, there is no indication the key used by the server to decrypt the password/nonce combination is "an encryption key stored on the client computer or entered by a user" as claimed. Rather, the key used to decrypt the password/nonce combination appears to be one that is already stored on the server—with no indication of how it got there. Accordingly, the decrypting performed by the server is not performed using "an encryption key stored on the client computer or entered by user," as recited in claim 24, and the alternate embodiment cited by the Examiner is not the same as what is claimed.

Because Pritikin does not identically disclose each element recited in claim 24, we do not sustain the anticipation rejection of claim 24 under 35 U.S.C. § 102(b). For the same reasons, we also do not sustain the rejection of independent claims 31 and 38, which, although not identical in scope to claim 24, recite limitations commensurate to those discussed above. We also do not sustain the rejections of the remaining claims, which are dependent and stand together with their respective base claims.

## CONCLUSION

We reverse the Examiner's rejections.

## DECISION SUMMARY

| **Claims Rejected** | **35 U.S.C. §** | **Reference(s)/Basis** | **Affirmed** | **Reversed** |
|---|---|---|---|---|
| 24–43 | n/a | Double Patenting | | 24–43 |

| | | | | |
|---|---|---|---|---|
| 24, 26–32 35–42 | 102(b) | Pritikin | | 24, 26–32, 35–42 |
| 25, 43 | 103(a) | Pritikin, Schneider | | 25, 43 |
| 33, 34 | 103(a) | Pritikin, Levi | | 33, 34 |
| **Overall Outcome** | | | | 24–43 |

TIME PERIOD FOR RESPONSE

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a). *See* 37 C.F.R. § 1.136(a)(1)(iv).

REVERSED