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.
13/301,219	11/21/2011	Lawrence Tang	26141.0014U1	2154

16000 7590 02/01/2019

Comcast
c/o Ballard Spahr LLP
999 Peachtree Street, Suite 1000
Atlanta, GA 30309

EXAMINER
TRAN, TONGOC

ART UNIT	PAPER NUMBER
2434	

NOTIFICATION DATE	DELIVERY MODE
02/01/2019	ELECTRONIC

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.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

USpatentmail@ballardspahr.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte LAWRENCE TANG, KENNETH P. MILLER, and CHRISTOPHER J. BENNETT

Appeal 2018-004968
Application 13/301,219[1]
Technology Center 2400

Before CARLA M. KRIVAK, JASON V. MORGAN, and PHILLIP A. BENNETT, *Administrative Patent Judges*.

BENNETT, *Administrative Patent Judge*.

DECISION ON APPEAL

STATEMENT OF THE CASE

Appellants appeal under 35 U.S.C. § 134(a) from the Examiner's final rejection of claims 1–20. We have jurisdiction under 35 U.S.C. § 6(b).

We affirm.

---

[1] Appellants' Brief ("App. Br.") identifies Comcast Cable Communications, LLC as the real party in interest. App. Br. 1.

CLAIMED SUBJECT MATTER

The claims are directed to authenticating data by generating a nonce based upon a shared key. Spec. ¶ 91. The shared key and nonce may then be transmitted to a recipient device as an encrypted authentication data block while minimizing bandwidth. *Id.* Claims 1, 9, and 17 are independent claims and are reproduced below:

> 1. A method comprising:
>
> processing, by a computing device, a first secret element based upon an intended recipient device to generate a first encrypted secret element;
>
> processing, by the computing device, a second secret element to generate a non-secret element, the second secret element being distinct from the first secret element; and
>
> processing, by the computing device, the first encrypted secret element and the non-secret element to generate an encrypted data block, wherein the encrypted data block comprises the first encrypted secret element and the non-secret element.

App. Br. 12 (Claims Appendix).

> 9. A method comprising:
>
> encrypting, by a computing device, a first shared key based upon a first intended recipient device to generate an encrypted first shared key;
>
> encrypting, by the computing device, a second shared key based upon a second intended recipient device to generate an encrypted second shared key, the second shared key being distinct from the first shared key;
>
> processing, by the computing device, the second shared key to generate a non-secret element; and
>
> processing, by the computing device, the first encrypted shared key, the second encrypted shared key, and the non-secret element to generate an encrypted data block.

App. Br. 13 (Claims Appendix).

17. A method comprising:

processing, by a computing device, a data block to determine a shared key nonce;

processing, by the computing device, the data block to determine a shared key associated with a first identifier, wherein the data block comprises a plurality of encrypted shared keys, and wherein each of the plurality of encrypted shared keys is encrypted based upon a distinct one of a corresponding plurality of intended recipient devices;

generating a first authentication key based upon the shared key;

generating an authentication nonce using the first authentication key; and

comparing the authentication nonce to the shared key nonce to determine authentication.

App. Br. 14 (Claims Appendix).

REFERENCES

The prior art relied upon by the Examiner in rejecting the claims on appeal is:

Kruglick	US 2011/0307953 A1	Dec. 15, 2011
Engels	US 2012/0011360 A1	Jan. 12, 2012
Liu	US 2013/0024689 A1	Jan. 24, 2013
Kocher et al.	US 8,386,800 B2	Feb. 26, 2013

REJECTIONS

Claims 1–17 and 20 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Kocher, Kruglick, and Liu. Final Act. 3–11.

Claims 18 and 19 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Kocher, Kruglick, Liu, and Engels. Final Act. 11–12.

ANALYSIS

We have reviewed the Examiner's rejections in light of Appellants' arguments set forth in the Appeal Brief and the Reply Brief. We are not persuaded by Appellants' arguments. We adopt as our own: (1) the findings and reasons set forth by the Examiner in the action from which this appeal is taken (Final Act. 2–12) and (2) the findings, reasons, and explanations set forth by the Examiner in the Examiner's Answer in response to Appellants' Brief (Ans. 3–24) and concur with the conclusions reached by the Examiner. We highlight the following for emphasis.

Claim 1

In rejecting claim 1, the Examiner finds that Kocher teaches "processing . . . a first secret element to generate a first encrypted secret element" because it describes using a shared secret key K_{ROOT} which can be used to generate encrypted information. Final Act. 3–4 (citing Kocher col. 6, ll. 4–18). The Examiner further finds Kocher teaches "processing . . . a second secret element to generate a non-secret element, the second secret element being distinct from the first secret element." Final Act 4 (citing Kocher col. 8, ll. 18–31); Ans. 15–16 (citing Kocher col. 3, ll. 20–24). The Examiner acknowledges that Kocher does not teach "the encrypted data block comprises the first encrypted secret element and the non-secret element," and turns to Kruglick for teaching generating encrypted data blocks comprising a secret node key and a non-secret nonce. Final Act 4 (citing Kruglick ¶ 45); Ans. 17. The Examiner finds "it would have been obvious to implement Kruglick's teaching with Kocher's key to ensure the key is protected." Ans. 17. The Examiner also acknowledges Kocher does not teach that the first secret element is "based upon an intended recipient

device." For this limitation, the Examiner cites Liu, and states that "[i]t would have been obvious to one of ordinary skill in the art at the time the invention was made to implement Liu's feature with Kocher's generation of secret key to enable the client device to decrypt the protected content at the client device." Final Act. 4 (citing Liu ¶ 7).

Appellants argue the cited combination fails to teach the limitation of "the second secret element being distinct from the first secret element." App. Br. 4–5. Specifically, Appellants argue Kocher teaches a system in which both an encrypting device and a decrypting device has access to the same shared key (K_{ROOT}), and as a result, cannot disclose distinct first and second elements. *Id.*

We do not find this argument persuasive.[2] As explained by the Examiner, Kocher teaches that a different key should be used for each segment of data to be encrypted. Ans. 16 (citing Kocher col. 3, ll. 21–25). In so doing, Kocher's encryption technique generates a first encrypted secret element from a first secret element (K_{ROOT}) and a non-secret element (nonce N) by "deriving N from keys." *See* Kocher col. 8, ll. 24–26. Although Appellants argue that "*Kocher* is silent as to any of these keys being 'based upon an intended recipient device'" (Reply Br. 1), this argument is not persuasive because the Examiner cites Liu for this limitation, and not Kocher. *See* Final Act. 4 (citing Liu ¶ 7).

Appellants further argue the cited combination does not teach the limitation "to generate an encrypted data block, wherein the encrypted data block comprises the first encrypted secret element and the non-secret

[2] Appellants present a substantively similar argument with respect to claim 9, which we also do not find persuasive for the same reasons.

element." App. Br. 5–6. Specifically, Appellants argue the Examiner's reliance on Kruglick is misplaced because it "simply discloses encrypting a message that includes two items of information, and fails to disclose generating an encrypted data block that comprises a first encrypted secret element and a non-secret element, as recited in claim 1." App. Br. 6. We disagree.

As the Examiner explains, Kruglick demonstrates that it was known to generate encrypted data blocks comprising a secret node key (i.e., a "first encrypted secret element") and a nonce (i.e., a "non-secret element").[3] Final Act 4 (citing Kruglick ¶ 45); Ans. 17. We agree with the Examiner that Kruglick teaches this feature because Kruglick states that "the secure pairing module 130 can be configured to use the shared signal signature vector to encrypt a node key and a nonce to create a confirmation message to securely exchange a key with another node." Kruglick ¶ 45.

Claim 15

Appellants also present arguments for dependent claim 15, which includes the limitation "wherein the second shared key is associated with a second class of recipient device, different from the first class of recipient devices." App. Br. 7. The Examiner finds Kocher and Liu teach this limitation. Final Act. 9 (citing Kocher col. 11, ll. 1–5); Ans. 20 (citing Liu's use of a key derived from device information such as device serial numbers to allow specific devices to access a specific content).

[3] We note that the Specification indicates that a nonce is a non-secret value. *See* Spec ¶ 64 ("In an aspect, the first shared key nonce **324** can comprise a non-secret value associated with a shared key, such as the first shared key **320** and used to authenticate possession of the shared key.")

Appellants argue Kocher is deficient because "[t]he cited portions of *Kocher* discuss the possibility of using different instances of a message key $K_{MESSAGE}$. These instances of $K_{MESSAGE}$ are based on the same shared key K_{ROOT}, but are not shared themselves." App. Br. 7. Appellants further contend Liu is deficient because it "is silent as to the 'content key' being a 'shared key' as claimed . . . [because] a key based on a 'serial number' would not be associated with a 'class of recipient device[s]' as claimed." Reply Br. 3.

We are not persuaded by Appellants' arguments. The disputed limitation in claim 15 recites "wherein the second shared key is *associated with* a second class of recipient device, different from the first class of recipient devices." App. Br. 13 (Claims Appendix) (emphasis added). As explained by the Examiner in the Answer, Kocher teaches that different shared keys can be derived from different values. Liu teaches that it was generally known to encrypt a content key based on values derived from recipient device information, and provides a device serial number as a specific example of doing so. Liu ¶ 15. Although Liu does not explicitly teach that a device serial number is indicative of a class of devices, we agree with the Examiner that it would have been obvious to a person of skill in the art to use other values derived from recipient device information, such as a model number indicative of a class of devices, to encrypt a content key. *KSR Int'l v. Teleflex Inc.*, 550 U.S. 398, 418 (2007) ("the [obviousness] analysis need not seek out precise teachings directed to the specific subject matter of the challenged claim, for a court can take account of the inferences and creative steps that a person of ordinary skill in the art would employ"). As such, we agree with the Examiner that the combined teachings of Kocher

and Liu at least suggest the argued limitation in claim 15, and we therefore sustain its rejection.

Claim 17

Independent claim 17 is argued separately by Appellants. Appellants challenge the Examiner's conclusion of obviousness with respect to the limitation of "processing, by the computing device, the data block to determine a shared key associated with a first identifier, wherein the data block comprises a plurality of encrypted shared keys, and wherein each of the plurality of encrypted shared keys is encrypted based upon a distinct one of a corresponding plurality of intended recipient devices." The Examiner relies on the combined teachings of Kocher, Kruglick, and Liu for this limitation. Final Act. 9–11.

Appellants offer three arguments for patentability of claim 17. First, Appellants argue Kruglick is deficient because it "discloses that the confirmation message includes a single key, not a plurality of keys." App. Br. 8. Second, Appellants argue that because Kruglick "teaches that the node key is a signal signature vector, but fails to disclose any encryption applied to the signal signature vector," it does not teach "a data block that comprises a plurality of encrypted shared keys." *Id.* Third, Appellants argue Kruglick "fails to disclose or suggest that each of the plurality of encrypted shared keys is encrypted based upon a distinct one of a corresponding plurality of intended recipient devices." *Id.*

We are not persuaded by Appellants' arguments. With respect to Appellants' argument that Kruglick fails to teach a plurality of encrypted shared keys, we note the Examiner cites Kocher as teaching the plurality of shared keys, and relies on Kruglick as teaching encrypting shared keys.

Final Act. 10 (citing Kocher Fig. 6, item 650 and Fig. 5, 505–508; Kruglick ¶ 45). Thus, the Examiner relies on the combined teachings of the references to show obviousness of this limitation. Appellants' argument attacks Kruglick singly as failing to teach the recited "plurality," but does not address the findings of the Examiner that relies on Kocher as teaching the recited "plurality." As such, this argument is not persuasive of Examiner error.

We also are not persuaded by Appellants' second argument that Kruglick "teaches that the node key is a signal signature vector, but fails to disclose any encryption applied to the signal signature vector" and does not teach "a data block that comprises a plurality of encrypted shared keys." We first note Kruglick teaches that the "shared signal signature vector" is used "to encrypt a node key and a nonce to create a confirmation message." Kruglick ¶ 45. In light of this disclosure, we disagree with Appellant that Kruglick does not disclose encryption applied to the node key to create an encrypted data block. Moreover, as we stated above, the Examiner does not rely on Kruglick as teaching the "plurality," but instead relies on Kocher for this aspect of the claim. Accordingly, we find Appellants' second argument unpersuasive of Examiner error.

Appellants' third argument is unpersuasive because the Examiner relies on Liu, and not Kruglick, for disclosing "based upon a distinct one of a corresponding plurality of intended recipient devices." Final Act. 11 (citing Liu ¶¶ 7, 29). Accordingly, we are not persuaded the Examiner erred in rejecting claim 17, and we sustain its rejection under 35 U.S.C. § 103(a).

Rationale for Combining References

Appellants also attack the combination of Kocher and Kruglick, asserting that the proposed modification of Kocher with the teachings of Kruglick would change the principle of operation of Kocher. Particularly, Appellants argue Kocher teaches the use of a shared key which allows for transmission of encrypted messages without the need to pass a key between devices. Appellants assert Kruglick teaches passing the node key as part of a confirmation message, which undermines Kocher's ability to transmit a message without key exchange. App. Br. 9.

We do not find this argument persuasive. The Examiner relies on Kruglick only to show that it was known to generate encrypted data blocks that include secret and non-secret elements. As the Examiner finds, Kruglick "is used to introduce a well-known feature of keeping a secret information safe." Ans. 23. Moreover, Appellants do not identify any portion of Kocher which disparages or otherwise discredits transmission of encrypted keys between devices. Accordingly, we are not persuaded the Examiner erred in combining Kocher and Kruglick.

DECISION

Because we do not find Appellants arguments persuasive, we affirm the Examiner's rejection of claims 1–20.

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).

AFFIRMED