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.
14/299,390	06/09/2014	John Anderson Fergus Ross	240985-7 (GELC:0061-1)	1062

62204 7590 10/15/2019

GE GLOBAL PATENT OPERATION
GE LICENSING (62204)
901 MAIN AVENUE
NORWALK, CT 06851

EXAMINER
LE, KHOI V

ART UNIT	PAPER NUMBER
2436	

NOTIFICATION DATE	DELIVERY MODE
10/15/2019	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):

docket@fyiplaw.com
rlt@zpspatents.com
sml@zpspatents.com

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

Ex parte JOHN ANDERSON FERGUS ROSS,
MICHAEL JAMES HARTMAN, JOHN ERIK HERSHEY, and
RICHARD LOUIS ZINSER

Appeal 2018-002232
Application 14/299,390
Technology Center 2400

Before MICHAEL J. STRAUSS, AMBER L. HAGY, and
PHILLIP A. BENNETT, *Administrative Patent Judges.*

HAGY, *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 23–27, 29, 30, 32–38, and 45–48, and 50–52. Final Act. 2.[2] 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 the applicant, General Electric Company. Appeal Br. 2.

[2] The Examiner indicates claims 39–44 are allowed, and claim 28 is objected to as dependent on a base claim, but would be allowable if rewritten in independent form. Final Act. 23. Claims 1–22 and 31 were canceled. *Id.* at 2. Claim 49 was also canceled by way of amendment dated Oct. 7, 2016.

CLAIMED SUBJECT MATTER

According to Appellant:

> The present invention relates generally to the field of communication systems, and more particularly, to systems and methods for conducting secure communication between two devices over cable communication networks. To that end, embodiments disclosed [in the Specification] . . . include methods, systems and apparatus that may allow secure communication by exchange of cryptovariables between two devices over the cable communication network along the transmission of intentional noise that may make the recovery of the cryptovariable by an unauthorized third party challenging. The claimed embodiments recite, generally, embodiments for methods, systems and apparatuses that transmit cryptovariables from a first device to a second device and simultaneous transmission of broadband noise from the second device to the first device.

Appeal Br. 3; *see also* Spec. ¶¶ 3–4.

Claims 23, 30, 45, and 52 are independent. Claim 23, reproduced below, is illustrative of the claimed subject matter:

> 23. A method comprising:
>
> transmitting first data comprising a cryptovariable from a first device to a second device over a cable in a cable communication network;
>
> receiving the first data comprising the cryptovariable at the second device;
>
> transmitting second data from the second device over the cable, wherein transmitting the second data from the second device comprises transmitting broadband noise from the second device while the first device transmits the cryptovariable to the second device; and

removing the broadband noise from the first data received at the second device using a division-free duplexing (DFD) technique to recover the cryptovariable.

REFERENCES

The prior art relied upon by the Examiner is:

Name	Reference	Date
Lin et al. ("Lin")	US 7,082,157 B2	July 25, 2006
Kanter et al.	US 2003/0223579 A1	Dec. 4, 2003
Kennedy et al.	US 2009/0110030 A1	Apr. 30, 2009

S. Chen, M. A. Beach, and J. P. McGeehan, *Division-free duplex for wireless applications*, 34 IEEE Electron. Lett. 147–148 (Jan. 1998) ("Chen").

REJECTIONS[3]

Claims 23–27, 30, 32–36, 38, 45–48, and 52 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Kennedy, Kanter, and Chen.

Claims 29, 37, 50, and 51 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Kennedy, Kanter, Chen, and Lin.

OPINION

With regard to claim 23,[4] the Examiner relies on Kennedy as disclosing transmitting multiplexed data streams, which the Examiner finds

[3] The Leahy-Smith America Invents Act ("AIA") included revisions to 35 U.S.C. § 103 that became effective on March 16, 2013. Because the present application was filed before March 16, 2013, the Examiner applies the pre-AIA version of § 103.

[4] Appellant and the Examiner present their arguments as addressed herein based on independent claim 23, which they address collectively with all of the independent claims. Appeal Br. 8–14; Ans. 3–5. We select claim 23 as

teaches transmitting first and second data over a cable in a cable communication network. Final Act. 6. The Examiner states "Kennedy fails to explicitly disclose a cryptovariable; broadband noise; [and] removing the broadband noise from the first data received at the second device . . . to recover the cryptovariable." *Id.* at 7. The Examiner finds Kanter "discloses [a] secure and linear public-key cryptosystem based on parity-check error-correcting, comprising a cryptovariable . . . broadband noise . . . [and] removing the broadband noise from the first data received at the second device . . . to recover the cryptovariable." *Id.* (citing Kanter ¶¶ 114, 136, 209, 249). The Examiner also states "Kennedy and Kanter fail to explicitly disclose using a division-free duplexing (DFD) technique," for which the Examiner relies on Chen. *Id.* at 7–8 (citing Chen, p. 147).

We are persuaded of error in the Examiner's rejection. In particular, we conclude the Examiner's findings are deficient because the Examiner does not explain how the cited art teaches or suggests "transmitting broadband noise *from the second device while* the first device transmits the cryptovariable to the second device . . . ," as recited in independent claim 23 (emphasis added).[5] As Appellant notes, the Examiner relies on Kennedy as generally disclosing simultaneous data transmission between two devices, but acknowledges that Kennedy does not teach transmitting a cryptovariable while a broadband noise is being received. *See id.*; *see also* Final Act. 7.

---

the representative claim, pursuant to our authority under 37 C.F.R. § 41.37(c)(1)(iv).

[5] Appellant's contentions present additional issues. Because the identified issues are dispositive of Appellant's arguments on appeal, we do not reach the additional issues.

The Examiner's findings in the Final Action combining Kanter with Kennedy do not remedy that deficiency. Although Kanter discusses cryptographic keys and concealment techniques for these keys, the Examiner does not explain how Kanter's concealment technique involves the separate transmission of broadband noise. *See* Final Act. 7. Instead, Kanter's technique relies on random corruption of the data by using a noise signal to alter the statistical features of transmitted information for compression of data. *See* Kanter, ¶¶ 114, 136. As described in Kanter, "[i]n step 202, the public-key [E_k] is corrupted (prior to the publication of the public key) by randomly flipping elements in a fraction, p_q, of the public-key rows, to obtain the corrupted version of the public key, [E_k] (this is an optional step) . . . . The corrupted public key, [E_k], is now utilized to perform all the operations required for encryption." *Id.* ¶¶ 208, 209 (emphasis omitted). Thus, in Kanter, a random process is used to flip bits of the cryptovariable at the sender, and the altered cryptovariable is used for encryption. *See id.* Appellant contends:

> This concealment technique is entirely distinct from the transmission of a broadband noise by a device while receiving . . . a cryptovariable, as recited in the claims. This difference is reflected in the claim recitations, for example, by the fact that the source of the noise is a device that is receiving a cryptovariable. Moreover, in the claims, the cryptovariable is "covered" by the broadband noise, without any corruption to the cryptovariable as occurs in Kanter. In Kanter, the corruption of a cryptographic keys takes place within the sender of the cryptographic key itself.

Appeal Br. 10 (emphasis omitted). As Appellant further contends, "a hypothetical combination of Kanter and Kennedy would, at best, lead to a system distinct from the ones recited in the claims in which a cryptovariable

and a corrupted cryptovariable [are] . . . *sent from the same device*." *Id.* (emphasis added).

In the Answer, the Examiner does not counter Appellant's assertions regarding the deficiencies of Kanter, but asserts (seemingly contradictory to the Examiner's earlier findings) that Kennedy's high bandwidth data transport system *does* include broadband noise. Ans. 4. In particular, the Examiner finds that, in Kennedy's system, "ultra wideband pulses or impulses are transmitted and received near, or in the noise range of the public switched telephone network (PSTN), cable television (CATV) network, and broadband power line (BPL) network, which may also be providing other services such as voice, video, and data, by means other than the ultra wideband pulses or impulses." *Id.* We disagree that this teaching satisfies the "transmitting broadband noise" limitation of the claims. The claims do not require merely the adjacent presence of noise, which appears to be the case in Kennedy's system as described by the Examiner, but they require the *transmission of noise by a second device while it is receiving a cryptovariable from a first device*. The Examiner does not point to a corresponding teaching in Kennedy.

Although the Examiner does not expressly address Kanter in the Answer, the Examiner's findings in the Final Action regarding Kanter do not make up for this deficiency of Kennedy. The Examiner's findings regarding Kanter relate to the use of noise (random variables) to *encrypt data being transmitted*, and the Examiner does not explain how Kanter teaches or suggests the *separate transmission of noise by the second device* (much less the second device simultaneously receiving a cryptovariable from a first device). *See* Final Act. 7; Kanter, ¶¶ 114, 136. That is, the Examiner does

not explain how encrypting a single transmission using noise, as taught in Kanter, would have rendered obvious using two simultaneous transmissions, in which a cryptovariable is sent from a first device to a second device, while broadband noise is transmitted to the first device from the second device, as recited in claim 23. Nor does the Examiner adequately explain how or why an ordinarily skilled artisan would have used Kanter's teachings regarding a single-stream encrypted transmission to modify Kennedy's multiplexed data streams to separately transmit a cryptovariable in one direction and noise in the other direction, as claimed here.

Also seemingly contrary to the Examiner's earlier findings, the Examiner also finds that Kennedy teaches transmitting a cryptovariable because it discloses that a Fast Fourier Transform ("FFT") and an Inverse FFT ("IFFT") are "applied in the transmitting and receiving data," which the Examiner finds corresponds to the disclosure in Appellant's Specification of a "cryptovariable" as an "algorithm or key for performing encryption or decryption of transmitted or received signals." Ans. at 4–5 (citing Spec. ¶ 30). We disagree. As Appellant contends, and we agree, Kennedy's FFT algorithm is not an encryption or decryption technique. *See* Reply Br. 3–4. Rather, although Kennedy discloses that a "FFT algorithm may be used to transform data, data transformed using the FFT algorithm of Kennedy is not concealed or otherwise encrypted in a reasonable sense." *Id.* at 3.

For the foregoing reasons, on this record, we are persuaded of error in the Examiner's 35 U.S.C. § 103(a) rejection of independent claim 23, and we, therefore, do not sustain that rejection. For the same reasons, we are also persuaded of error in the Examiner's rejection of independent claims

30, 45, and 52 on the same basis. The dependent claims stand with their respective independent claims.

CONCLUSION

The Examiner's 35 U.S.C. § 103(a) rejections of claims 23–27, 29, 30, 32–38, 45–48, and 50–52 are REVERSED.

Claims Rejected	35 U.S.C. §	Basis	Affirmed	Reversed
23–27, 30, 32–36, 38, 45–48, and 52	103(a)	Kennedy, Kanter, and Chen		23–27, 30, 32–36, 38, 45–48, and 52
29, 37, 50, and 51	103(a)	Kennedy, Kanter, Chen, and Lin		29, 37, 50, and 51
OVERALL OUTCOME				23–27, 29, 30, 32–38, 45–48, and 50–52

REVERSED