EUROPEAN PATENT OFFICE
U.S. PATENT AND TRADEMARK OFFICE

CPC NOTICE OF CHANGES 435

DATE: AUGUST 1. 2017

PROJECT RP0424

The following classification changes will be effected by this Notice of Changes:

Action	**Subclass**	**Group(s)**
Title wording change:	H04K	1/00
	H04K	1/003
	H04K	1/02
	H04K	3/00
Modified Definitions:	H04K	subclass
	H04K	1/00
	H04K	3/00
Scheme Notes to be deleted:	H04K	3/00

No other subclasses/groups are impacted by this Notice of Changes.

This Notice of Changes includes the following *[Check the ones included]:*

1. CLASSIFICATION SCHEME CHANGES
   - ☒ A. New, Modified or Deleted Group(s)
   - ☐ B. New, Modified or Deleted Warning Notice(s)
   - ☒ C. New, Modified or Deleted Note(s)
   - ☐ D. New, Modified or Deleted Guidance Heading(s)
2. DEFINITIONS (New or Modified)
   - ☒ A. DEFINITIONS (Full definition template)
   - ☐ B. DEFINITIONS (Definitions Quick Fix)
3. ☐ REVISION CONCORDANCE LIST (RCL)
4. ☐ CHANGES TO THE CPC-TO-IPC CONCORDANCE LIST (CICL)
5. ☐ CROSS-REFERENCE LIST (CRL)

CPC NOTICE OF CHANGES 435

DATE: AUGUST 1. 2017

PROJECT RP0424

1. CLASSIFICATION SCHEME CHANGES

A. New, Modified or Deleted Group(s)

SUBCLASS H04K - SECRET COMMUNICATION; JAMMING OF COMMUNICATION

Type*	**Symbol**	**Indent Level Number of dots (e.g. 0, 1, 2)**	**Title (new or modified) "CPC only" text should normally be enclosed in {curly brackets}****	**Transferred to#**
M	H04K 1/00	0	Secret communication	
M	H04K 1/003	1	{by varying carrier frequency at or within predetermined or random intervals (H04K 1/04 takes precedence)}	
M	H04K 1/02	1	by adding a second signal to make the desired signal unintelligible	
M	H04K 3/00	0	Jamming of communication; Counter-measures	

*N = new entries where reclassification into entries is involved; C = entries with modified file scope where reclassification of documents from the entries is involved; Q = new entries which are firstly populated with documents via administrative transfers from deleted (D) entries. Afterwards, the transferred documents into the Q entry will either stay or be moved to more appropriate entries, as determined by intellectual reclassification; E= existing entries with enlarged file scope, which receive documents from C or D entries, e.g. when a limiting reference is removed from the entry title; M = entries with no change to the file scope (no reclassification); D = deleted entries; F = frozen entries will be deleted once reclassification of documents from the entries is completed; U = entries that are unchanged.

NOTES:

- **No {curly brackets} are used for titles in CPC only subclasses, e.g. C12Y, A23Y; 2000 series symbol titles of groups found at the end of schemes (orthogonal codes); or the Y section titles. The {curly brackets} are used for 2000 series symbol titles found interspersed throughout the main trunk schemes (breakdown codes).
- For U groups, the minimum requirement is to include the U group located immediately prior to the N group or N group array, in order to show the N group hierarchy and improve the readability and understanding of the scheme. Always include the symbol, indent level and title of the U group in the table above.
- All entry types should be included in the scheme changes table above for better understanding of the overall scheme change picture. Symbol, indent level, and title are required for all types except "D" which requires only a symbol.
- #"Transferred to" column must be completed for all C, D, F, and Q type entries. F groups will be deleted once reclassification is completed.
- When multiple symbols are included in the "Transferred to" column, avoid using ranges of symbols in order to be as precise as possible.
- For administrative transfer of documents, the following text should be used: "< administrative transfer to XX>" or "<administrative transfer to XX and YY simultaneously>" when administrative transfer of the same documents is to more than one place.
- Administrative transfer to main trunk groups is assumed to be "invention information", unless otherwise indicated, and to 2000 series groups is assumed to be "additional information".

C. New, Modified or Deleted Note(s)

SUBCLASS H04K - SECRET COMMUNICATION; JAMMING OF COMMUNICATION

Type*	Location	Old Note	New/Modified Note
D	H04K 3/00	1. {This group covers: "Jamming", only when it means purposefully trying to interfere with the physical transmission and reception of communication. Provided this condition is met, this group covers devices and methods for: a. jamming of communication: i. jamming by intentionally decreasing the signal to noise ratio ii. deceptive jamming iii. passive jamming iv. destructive jamming b. countermeasures against jamming c. countermeasures against undesired self-jamming resulting from jamming d. countermeasures against surveillance, interception or detection e. other electronic countermeasures using or against electromagnetic or acoustic waves f. signal detection techniques used in relation to i. jamming: for interception and monitoring of the jamming target signal ii. anti-jamming: for jamming detection, iii. anti-surveillance: for surveillance detection g. jamming for testing or assessing countermeasures h. jamming used to prevent: – cellular phone communication i. in a vehicle during motion ii. in particular areas, including prisons, hospitals, planes, petrol stations, theatres iii. to trigger RCIEDs - reception of positioning data using GPS – wireless communication in ad hoc networks or in sensor networks – exchange of data between wirelessly connected devices or device units, on Bluetooth, infrared or near field links – unauthorized access to network, service or information, including: i. access to a WLAN network ii. access to information stored in contactless carriers, including RFID carriers – transmission of an alarm, against burglary or vehicle theft – remote control of devices – surveillance i. of speech in meeting rooms	

Type*	**Location**	**Old Note**	**New/Modified Note**
		ii. of electromagnetic emissions from a computer screen – interception or detection of a wirelessly transmitted signal } 2. {In this group, the following acronyms are used: GPS = global positioning system RCIED = remote controlled improvised explosive device RFID = radio frequency identification WLAN= wireless local area network}	

*N = new note, M = modified note, D = deleted note

NOTE: The “Location” column only requires the symbol PRIOR to the location of the note. No further directions such as “before” or “after” are required.

2. A. DEFINITIONS (modified)

H04K

Definition statement

This place covers:

Delete: The following existing paragraph:

Two main groups (H04K 1/00 - secret communication, H04K 3/00 - Jamming of communication; Countermeasures), which both relate to communication and to (ensuring or attacking) the security of the physical transmission channel.

Insert: The following replacement paragraphs:

This subclass covers secret line and radiation transmission systems in which the signal is modified at the transmitting station in such a way that the information cannot be intelligibly received without corresponding modification at the receiving station.
The signal can be modified using, for example, frequency scrambling or scrambling by combination with a second signal.
This subclass also covers the jamming of communications and counter-measures against jamming or against surveillance.

Insert: The following *new* Relationships section:

Relationships with other classification places

Systems using reduced bandwidth or suppressed carrier techniques, or using sub-carriers or spread spectrum techniques are classified in H04B. In particular, spread spectrum as counter-measure against jamming is classified in H04K 3/00 whereas spread spectrum communication as such is classified in H04B.

Analogue scrambling, jamming or counter-measures to achieve secure communication are classified in H04K whereas encryption of digital signals is classified in H04L.

Insert: The following new References section (heading) and the following two subsections: *Application-oriented references* and *Informative references*.

References

Application-oriented references

Examples of places where the subject matter of this place is covered when specially adapted, used for a particular purpose, or incorporated in a larger system:

Means for anti-jamming used in radar or analogous systems	G01S7/36
Jamming means used in radar or analogous systems	G01S7/38
Counter-measures or counter-counter-measures used in lidar or analogous systems	G01S7/495
Counter measures or counter-counter-measures used in sonar or analogous systems	G01S7/537
Arrangements for the secret or secure communication of digital information, encryption of digital signals	H04L9/00
Secrecy systems used in scanning, transmission or reproduction of documents	H04N1/44
Analogue secrecy systems or analogue subscription systems for television	H04N7/16

Informative references

Attention is drawn to the following places, which may be of interest for search:

Arrangements for protecting computers or computers systems	G06F21/00
Ciphering or deciphering apparatus per se	G09C
Systems with reduced bandwidth or suppressed carrier	H04B1/66, H04B1/68
Spread spectrum techniques	H04B1/69
Photonic quantum communication	H04B10/70

Protection from unauthorised access for optical transmission, e.g. eavesdrop protection	H04B10/85
Transmission systems characterised by the use of a sub-carrier	H04B14/08
Arrangements for preventing the taking of data from a data transmission channel without authorisation	H04L12/22
Selective content distribution, e.g. interactive television, VOD	H04N21/00

Insert: The following new Glossary of terms section.

Glossary of terms

In this place, the following terms or expressions are used with the meaning indicated:

Secret communication	Secret line and radiation transmission systems, i.e., those in which the signal is modified at the transmitting station in such a way that the information cannot be intelligibly received without corresponding modification at the receiving station.
Jamming of communication	Apparatus, circuits or systems purposefully trying to interfere with the physical transmission and reception of communication.
Frequency scrambling	Transposing or inverting parts of the frequency band or by inverting the whole band
Follower jammer	Jammer adapted to determine and follow the frequency of a jamming target signal that uses frequency hopping techniques
Look-through mode	Operation mode wherein jamming and monitoring of the jamming target alternate
Reactive jammer	Jammer wherein jamming is activated only when a target has been detected
RCIED	Remote Controlled Improvised Explosive Device

Insert: The following new Synonyms and Keywords section:

Synonyms and Keywords

In patent documents, the following words/expressions are often used as synonyms:

- “confidential”, "sensitive", “undercover”, “private”, “sneaky”
- “hidden”, "scrambled", "blinded", "obscured", "obfuscated", "masked", "concealed", "covert", "coded"

H04K 1/00

Insert: The following new Relationships section:

Relationships with other classification places

Secret communication in the analogue domain, or analogue scrambling, jamming or counter-measures are classifed in H01K 1/00 whereas transmission systems for the secret or secure communication of digital information are classified in H04L, with details of encryption in the digital domain most likely classified in H04L 9/00 and H04L12/00.

Limiting references

Delete: The entire existing *Limiting references* section.

Insert: The following new *Informative references* section.

Informative references

Attention is drawn to the following places, which may be of interest for search:

Ciphering or deciphering apparatus per se	G09C
Systems with reduced bandwidth or suppressed carrier	H04B 1/66
Spread spectrum techniques in general	H04B 1/69
By using a sub-carrier	H04B 14/08
By multiplexing	H04J
Transmission systems for secret digital information, encryption of digital signals	H04L9/00, H04L12/00
Secret or subscription television systems	H04N 7/16, H04N 21/00

H04K 3/00

Definition statement

This place covers:

Delete: All of the text in the Definitions statement section, from the first statement:

- "jamming", only when it means purposefully trying to interfere with the physical transmission and reception of communication.

to the last statement:

ii) of electromagnetic emissions from a computer screen H04K 2203/14)
- interception or detection of a wirelessly transmitted signal (H04K 3/825)

Insert: The following replacement text in the Definitions statement section.

"jamming", only when it means purposefully trying to interfere with the physical transmission and reception of communication.
Provided this condition is met, this group covers devices and methods for:

- jamming of communication, e.g. jamming by intentionally decreasing the signal to noise ratio, deceptive jamming (H04K 3/65), passive jamming (H04K 3/68), destructive jamming (H04K 3/62);
- countermeasures against jamming (H04K 3/20);
- countermeasures against undesired self-jamming resulting from jamming (H04K 3/28);
- countermeasures against surveillance, interception or detection (H04K 3/82);
- other electronic countermeasures using or against electromagnetic or acoustic waves (H04K 3/00);
- signal detection techniques used in relation to jamming for interception and monitoring of the jamming target signal (H04K 3/45);
- signal detection techniques used in relation to anti-jamming for jamming detection (H04K 3/22);
- signal detection techniques used in relation to anti-surveillance for surveillance detection (H04K 3/822)

In particular, this group covers:

- jamming for testing or assessing countermeasures (H04K 3/94);
- jamming used to prevent cellular phone communication (H04K 2203/16), e.g. in a vehicle during motion (H04K 3/415), in particular areas, including prisons, hospitals, planes, petrol stations, theatres (H04K 3/84), and to trigger RCIEDs (H04K 3/92 and H04K 2203/24);
- jamming used to prevent reception of positioning data using GPS (H04K 3/90);
- jamming used to prevent wireless communication in ad hoc networks or in sensor networks (H04K 2203/18);
- jamming used to prevent exchange of data between wirelessly connected devices or device units, on Bluetooth, infrared or near field links;
- jamming used to prevent unauthorized access to network, service or information (H04K 3/86), including access to a WLAN network (H04K 2203/18) and access to information stored in contactless carriers, including RFID carriers (H04K 2203/20);
- jamming used to prevent transmission of an alarm against burglary or vehicle theft (H04K 3/88);
- jamming used to prevent remote control of devices (H04K 3/92);
- jamming used to prevent surveillance (H04K 3/82), e.g. of speech in meeting rooms (H04K 2203/12), of electromagnetic emissions from a computer screen H04K 2203/14);
- jamming used to prevent interception or detection of a wirelessly transmitted signal (H04K 3/825).

Relationships with other classification places

Delete: The following four paragraphs (1st, 2nd, 7th and 11th paragraphs) and the punctuation period (.) before line H04K3/00 and H04K1/00 from the existing Relationships section.

H04K 3/00 and application fields

Application fields (e.g. in the lower part of the "Informative reference" table below): when a patent document discloses how the jamming, anti-jamming, anti-surveillance or any other countermeasure covered by H04K 3/00 is carried out, it should be classified in H04K 3/00.

This distinction in the terminology is however not always respected in patent documents (in particular in the expressions "transceiver self-jamming" and "jamming cancellation", where jamming means interference).

Since intentional and unintentional disturbances often present similar characteristics, they can be countered by the same techniques. Therefore, there exists an overlap between H04K3/20 and H04B, and some documents are classified in both places.

the lonely punctuation period (.)

References

Limiting references

Delete: The entire *Limiting references* section.

Insert: The following new *Application-oriented references* section.

Examples of places where the subject matter of this place is covered when specially adapted, used for a particular purpose, or incorporated in a larger system:

Counter-measures used in radar or analogous systems	G01S 7/00
Counter-measures used in radar	G01S 7/36, G01S 7/38
Counter-measures used in lidar	G01S 7/495
Counter-measures used in sonar	G01S 7/537

Informative references

Delete: The following existing row in the *Informative references* table:

Contactless record carriers (e.g. RFID carriers)	G06K19/00, G06K7/00

Insert: The following new row in the *Informative references* table:

Counter-measures used in radar or analogous systems	G01S7/00