

# CPC COOPERATIVE PATENT CLASSIFICATION

## H ELECTRICITY

(NOTE omitted)

## H04 ELECTRIC COMMUNICATION TECHNIQUE

(NOTE omitted)

## H04K SECRET COMMUNICATION; JAMMING OF COMMUNICATION

### NOTE

In this subclass, the following expression is used with the meaning indicated:

- "secret communication" includes secret line and radiation transmission systems, i.e. those in which apparatus at the transmitting station modifies the signal in such a way that the information cannot be intelligibly received without corresponding modifying apparatus at the receiving station.

|             |  |       |   |
|-------------|--|-------|---|
| <b>1/00</b> | <b>Secret communication</b>  | 3/25  | . . {based on characteristics of target signal or of transmission (as countermeasure against surveillance <a href="#">H04K 3/827</a> ), e.g. using direct sequence spread spectrum or fast frequency hopping (spread spectrum techniques <a href="#">H04B 1/69</a> )} |
| 1/003       | . {by varying carrier frequency at or within predetermined or random intervals ( <a href="#">H04K 1/04</a> takes precedence)}  |       |   |
| 1/006       | . {by varying or inverting the phase, at periodic or random intervals}   |       |   |
| 1/02        | . by adding a second signal to make the desired signal unintelligible  | 3/255 | . . . {based on redundancy of transmitted data, transmission path or transmitting source}   |
| 1/025       | . . {using an analogue chaotic signal}   | 3/28  | . . {with jamming and anti-jamming mechanisms both included in a same device or system, e.g. wherein anti-jamming includes prevention of undesired self-jamming resulting from jamming}   |
| 1/04        | . by frequency scrambling, i.e. by transposing or inverting parts of the frequency band or by inverting the whole band   |       |   |
| 1/06        | . by transmitting the information or elements thereof at unnatural speeds or in jumbled order or backwards   | 3/40  | . {Jamming having variable characteristics}   |
| 1/08        | . by varying the polarisation of transmitted waves   | 3/41  | . . {characterized by the control of the jamming activation or deactivation time (control of jamming activation and deactivation time only for the purpose of alternating between jamming mode and target monitoring mode <a href="#">H04K 3/45</a> )}                |
| 1/10        | . by using two signals transmitted simultaneously or successively  | 3/415 | . . . {based on motion status or velocity, e.g. for disabling use of mobile phones in a vehicle}  |
| <b>3/00</b> | <b>Jamming of communication; Counter-measures</b>  |       |   |
| 3/20        | . {Countermeasures against jamming (in radar <a href="#">G01S 7/36</a> ; interference suppression in receivers <a href="#">H04B 1/10</a> )}  | 3/42  | . . {characterized by the control of the jamming frequency or wavelength}   |
| 3/22        | . . {including jamming detection and monitoring}   | 3/43  | . . {characterized by the control of the jamming power, signal-to-noise ratio or geographic coverage area}  |
| 3/222       | . . . {wherein jamming detection includes detecting the absence or impossibility of intelligible communication on at least one channel}  | 3/44  | . . {characterized by the control of the jamming waveform or modulation type}   |
| 3/224       | . . . {with countermeasures at transmission and/or reception of the jammed signal, e.g. stopping operation of transmitter or receiver, nulling or enhancing transmitted power in direction of or at frequency of jammer} | 3/45  | . . {characterized by including monitoring of the target or target signal, e.g. in reactive jammers or follower jammers for example by means of an alternation of jamming phases and monitoring phases, called "look-through mode"}                                   |
| 3/226       | . . . . {Selection of non-jammed channel for communication (spectrum sharing arrangements <a href="#">H04W 16/14</a> ; selection of wireless resources by user or terminal <a href="#">H04W 72/02</a> )}                 | 3/46  | . . {characterized in that the jamming signal is produced by retransmitting a received signal, after delay or processing}   |
| 3/228       | . . . . {Elimination in the received signal of jamming or of data corrupted by jamming (interference suppression in receivers <a href="#">H04B 1/10</a> )}   | 3/60  | . {Jamming involving special techniques}  |
|             |  | 3/62  | . . {by exposing communication, processing or storing systems to electromagnetic wave radiation, e.g. causing disturbance, disruption or damage of electronic circuits, or causing external injection of faults in the information}                                   |
|             |  | 3/65  | . . {using deceptive jamming or spoofing, e.g. transmission of false signals for premature triggering of RCIED, for forced connection or disconnection to/from a network or for generation of dummy target signal}  |

## H04K

- 3/68 . . {using passive jamming, e.g. by shielding or reflection (shielding of apparatus or components against electric or magnetic field [H05K 9/00](#))}
- 3/80 . {Jamming or countermeasure characterized by its function}
- 3/82 . . {related to preventing surveillance, interception or detection}
- 3/822 . . . {by detecting the presence of a surveillance, interception or detection}
- 3/825 . . . {by jamming}
- 3/827 . . . {using characteristics of target signal or of transmission (as countermeasure against jamming [H04K 3/25](#)), e.g. using direct sequence spread spectrum or fast frequency hopping (spread spectrum techniques [H04B 1/69](#))}
- 3/84 . . {related to preventing electromagnetic interference in petrol station, hospital, plane or cinema}
- 3/86 . . {related to preventing deceptive jamming or unauthorized interrogation or access, e.g. WLAN access or RFID reading (record carriers with integrated circuit chips including means for preventing undesired reading or writing from or to record carriers by hindering electromagnetic reading or writing [G06K 19/07318](#); arrangements for sensing record carriers including arrangements for protecting the interrogation against piracy attacks [G06K 7/10257](#))}
- 3/88 . . {related to allowing or preventing alarm transmission}
- 3/90 . . {related to allowing or preventing navigation or positioning, e.g. GPS}
- 3/92 . . {related to allowing or preventing remote control}
- 3/94 . . {related to allowing or preventing testing or assessing}

### **2203/00 Jamming of communication; Countermeasures**

- 2203/10 . Jamming or countermeasure used for a particular application
- 2203/12 . . for acoustic communication
- 2203/14 . . for the transfer of light or images, e.g. for video-surveillance, for television or from a computer screen
- 2203/16 . . for telephony
- 2203/18 . . for wireless local area networks or WLAN
- 2203/20 . . for contactless carriers, e.g. RFID carriers
- 2203/22 . . for communication related to vehicles
- 2203/24 . . for communication related to weapons
- 2203/30 . Jamming or countermeasure characterized by the infrastructure components
- 2203/32 . . including a particular configuration of antennas
- 2203/34 . . involving multiple cooperating jammers
- 2203/36 . . including means for exchanging jamming data between transmitter and receiver, e.g. in forward or backward direction