(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
25 July 2013 (25.07.2013)

WIPO | PCT

(10) International Publication Number
WO 2013/109764 A1

(51) International Patent Classification:
H04B 5/00 (2006.01)

(21) International Application Number:
PCT/US2013/021955

(22) International Filing Date:
17 January 2013 (17.01.2013)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
13/352,024 17 January 2012 (17.01.2012) US

(71) Applicant: **RAYTHEON BBN TECHNOLOGIES CORP.** [US/US]; 10 Moulton Street, Cambridge, Massachusetts 02138 (US).

(72) Inventor: **INSANIC, Edin**; 9 Francis St., Belmont, Massachusetts 02478 (US).

(74) Agents: **MADDEN, Robert B.** et al.; P.O. Box 2938, Minneapolis, Minnesota 55402 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

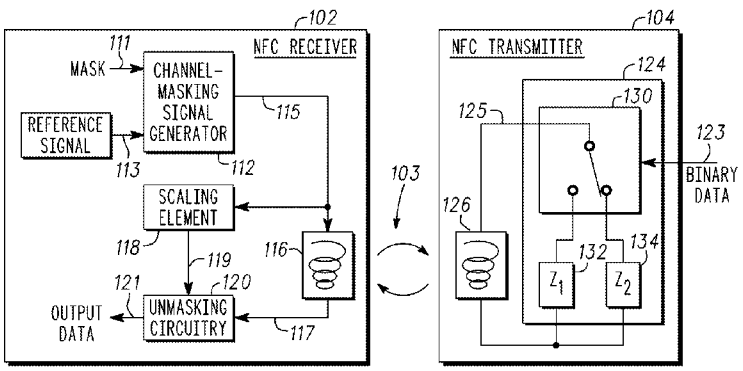
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))*

(54) Title: NEAR-FIELD COMMUNICATION (NFC) SYSTEM AND METHOD FOR PRIVATE NEAR-FIELD COMMUNICATION



100

Fig. 1

(57) Abstract: Embodiments of a near-field communication (NFC) system and method for private near-field communication are generally described herein. In some embodiments, a resonance-coupled channel is masked with a random channel-masking signal. The channel-masking signal may be scaled based on near-field channel conditions. Signals received through the channel may be unmasked with the scaled channel-masking signal to determine data that may have been conveyed by an NFC transmitting device by affecting the impedance of the resonance-coupled channel. In some embodiments, a reference signal may be scrambled with a mask to generate the channel-masking signal. The mask may include at least one of a random symbol mask, an amplitude mask and a phase mask. For additional privacy, the mask may include a random symbol mask and at least one of an amplitude mask and a phase mask.

WO 2013/109764 A1

NEAR-FIELD COMMUNICATION (NFC) SYSTEM AND METHOD FOR PRIVATE NEAR-FIELD COMMUNICATION

CLAIM OF PRIORITY

This application claims the benefit of priority to United States Patent Application Serial No. 13/352,024, filed January 17, 2012, the entire contents of which is incorporated herein by reference in its entirety and is made a part hereof.

TECHNICAL FIELD

Embodiments pertain to private near-field communications. Some embodiments relate to radio-frequency identification (RFID) technology. Some embodiments relate to financial transaction systems. Some embodiments relate to near-field enabled mobile communication devices. Some embodiments relate to private key exchange.

BACKGROUND

Near-field communication (NFC) is a wireless communication technique in which the communicating devices are separated by less than a wavelength. Near-field communication is being adopted by the mobile phone industry for financial transactions and is anticipated to replace the use of magnetic strips of credit cards. One issue with near-field communication is privacy. Although near-field communication takes place between closely located devices, an eavesdropper may still be able to determine the information being exchanged. Conventional encryption techniques that use either symmetric or asymmetric keys have several drawbacks including increased complexity, cost and processing requirements.

Thus, there are general needs for private near-field communication systems and methods that reduce the complexity, cost and processing requirements. There are also general needs for private near-field communication systems and methods suitable for financial transactions. There are also general needs for private near-field communication systems and methods suitable for key exchange. There are also general needs for private near-field communication systems and methods suitable for smart phones and mobile communication devices.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a functional block diagram of a near-field communication system for resonance-coupled communications in accordance with some embodiments;

FIG. 2 illustrates the generation of a channel-masking signal in accordance with some embodiments;

FIG. 3 is a procedure for private near-field communication in accordance with some embodiments; and

FIG. 4 is a calibration procedure for near-field communication through a private channel in accordance with some embodiments.

DETAILED DESCRIPTION

The following description and the drawings sufficiently illustrate specific embodiments to enable those skilled in the art to practice them. Other embodiments may incorporate structural, logical, electrical, process, and other changes. Portions and features of some embodiments may be included in, or substituted for, those of other embodiments. Embodiments set forth in the claims encompass all available equivalents of those claims.

FIG. 1 is a functional block diagram of a near-field communication system for resonance-coupled communications in accordance with some embodiments. NFC system 100 includes an NFC receiver 102 and an NFC transmitter 104. In accordance with embodiments, the NFC receiver 102 may receive data privately from the NFC transmitter 104 through a resonance-coupled channel 103. In these embodiments, the NFC receiver 102 may mask the resonance-coupled channel 103 with a random channel-masking signal and may scale the channel-masking signal based on near-field channel conditions. The NFC receiver 102 may also unmask signals received through the channel 103 with the scaled channel-masking signal to determine data that may be conveyed by the NFC transmitter 104. In these embodiments, the NFC transmitter 104 may convey the data by affecting an impedance of the resonance-coupled channel 103. The NFC receiver 102 may be positioned within the near field of the NFC transmitter 104, and the application of the channel-masking signal to the resonance-coupled channel 103 may create a private resonance-coupled channel.

The NFC receiver 102 may include a channel-masking signal generator 112 to randomly scramble a reference signal 113 and generate a channel-masking signal 115 for application to the resonance-coupled channel 103. The NFC receiver 102 may also include a scaling element 118 to scale the channel-masking signal 115 based, at least in part, on near-field channel conditions. The NFC receiver 102 may also include unmasking circuitry 120 to combine the scaled channel-masking signal 119 with resonance-coupled signals 117 received through the resonance-coupled channel 103 to generate binary data as output data 121. The output data 121 may comprise unmasked bits.

The NFC transmitter 104 may include an impedance-switching element 130 to affect an impedance of the resonance-coupled channel 103 based on binary data 123 to be conveyed to the NFC receiver 102. The output data 121 generated by the unmasking circuitry 120 may correspond to the binary data 123.

Accordingly, the binary data 123 may be conveyed by modulating the impedance of the resonance-coupled channel 103 that is masked by the channel-masking signal 115. This allows the unmasking circuitry 120 to recover the binary data 123 by unmasking the resonance-coupled signals 117 received through the resonance-coupled channel 103 with the scaled channel-masking signal 119. In this way, a private channel is established through impedance coupling allowing the private communication of the binary data 123 between NFC devices since the resonance-coupled signals 117 may be incomprehensible without knowledge of the channel-masking signal 115. In these embodiments, the channel-masking signal 115 may be random, inhibiting an eavesdropper from locking onto signals within the resonance-coupled channel 103 and determining any values of the binary data 123.

The impedance-switching element 130 of the NFC transmitter 104 may affect the impedance of the resonance-coupled channel 103 by switching between a first impedance 132 and a second impedance 134 based on the binary data 123 that is to be conveyed to the NFC receiver 102. The first impedance 132 is illustrated as impedance Z_1 and the second impedance 134 is illustrated as impedance Z_2. In these embodiments, although the NFC transmitter 104 is referred to as a transmitter, the NFC transmitter 104 does not actually transmit the binary data 123 in the conventional sense in which a carrier wave or other RF signal is modulated with data. The NFC transmitter 104 modulates the impedance of the resonance-coupled channel 103 based on the binary data 123.

The first impedance 132 may represent an open and the second impedance 134 may represent a short allowing the impedance-switching element 130 to modulate the impedance of the resonance-channel coupled 103 between a minimum and maximum. Other impedance values may be used for the first impedance 132 and the second impedance 134 depending on the amount of privacy desired and the amount of scrambling provided by the channel-masking signal generator 112. For example, various impedance values between a short and an open may be used.

The NFC receiver 102 may also include a reactive element 116 to affect the resonance-coupled channel 103 with the channel-masking signal 115. The reactive element 116 may also be used receive the resonance-coupled signals 117. The NFC transmitter 104 may also include a reactive element 126 to modulate the resonance-coupled channel 103 based on a switched impedance signal 125 provided by the impedance switching element 124. In these embodiments, the reactive elements 116 and 126 may be mutually coupled when operating in their near fields.

The switching between the first impedance 132 and the second impedance 134 may be performed at a rate based on the resonance frequency of the resonance-coupled channel 103. The switching rate may range from several kHz to several hundred kHz although other switching rates may also be suitable. The NFC transmitter 104 may modulate the impedance of reactive element 126 based on the bit values of the binary data 123 to modulate the impedance of the resonance-coupled channel 103. In some of these embodiments, the NFC transmitter 104 may implement a switched-impedance transmission technique, although this is not a requirement. In these embodiments, the unmasking circuitry 220 may combine the scaled channel-masking signal 119 with the resonance-coupled signals 117 received through the resonance-coupled channel 103 by the reactive element 116 to generate output data 121, which may correspond to the binary data 123.

In some embodiments, reactive element 116 and reactive element 126 may be mutually-coupled inductors that emit electromagnetic energy. In some embodiments, reactive element 116 and reactive element 126 may be mutually-coupled antennas operating in their near-fields. The antennas may comprise coils of wire and may be helical coils although the scope of the embodiments is not limited in this respect as other antenna, inductor and capacitor configurations may be suitable.

In some embodiments, the NFC receiver 102 and the NFC transmitter 104 may be configured to communicate through an array of channels in which each channel has a different resonance. In these embodiments, different sets of reactive elements may be used for each channel.

In some embodiments, the NFC receiver 102 may be part of an NFC reader and the NFC transmitter 104 may be part of an NFC tag. Unlike a conventional radio frequency identification (RFID) tag system, data is conveyed through a private channel created with the channel-masking signal 115. Unlike conventional RFID tag systems, the NFC receiver 102 does not operate as a clock transmitter since the NFC receiver 102 does not transmit a clock signal, and the NFC transmitter 104 does not operate as a clock receiver since the NFC transmitter 104 does not receive a clock signal.

The scaling element 118 may scale the channel-masking signal 115 in both amplitude and phase based on parameters determined during a calibration process. In these embodiments, the scaling by scaling element 118 may take into account, among other things, the delay between the scaled channel-masking signal 119 and the received resonance-coupled signal 117 to allow the unmasking circuitry 120 to effectively remove the channel effects and the effects of the channel-masking signal 115. In these embodiments, the phase scaling may allow the unmasking circuitry 120 to operate on signals that have the same temporal reference. The calibration process is discussed in more detail below.

FIG. 2 illustrates the generation of a channel-masking signal in accordance with some embodiments. In these embodiments, the channel-masking signal generator 112 (FIG. 1) may scramble the reference signal 113 (FIG. 1) by modulating the reference signal 113 with a mask 111 (FIG. 1) to generate the channel-masking signal 115 (FIG. 1). The mask 111 may comprise a random symbol mask 206, and at least one of an amplitude mask 202 and a phase mask 204. In some embodiments, the symbol mask 206 may be randomly generated allowing the reference signal 113 to be randomly scrambled. In some embodiments, a symbol mask 206, an amplitude mask 202 and a phase mask 204 may be used for maximum privacy.

In other embodiments (e.g., when less privacy is desired) only a symbol mask 206 may be used, or a symbol mask 206 with either an amplitude mask 202 or a phase mask 204 may be used. In some embodiments, the symbol mask 206 may be a bit mask, the amplitude mask 202 may be a level mask, and the phase mask 204 may be a temporal mask, although the scope of the embodiments is not limited in this respect. In these embodiments, the masking of the binary data 123 may be achieved by placing a confidential signal in the same space-time domain as the channel-masking signal 115. In some embodiments, the symbol mask 206, the amplitude mask 202 and the phase mask 204 comprise non-correlated random sequences.

The channel-masking signal generator 112 may generate the channel-masking signal 115 by applying the symbol mask 206 to the reference signal 113 to generate a symbol-modulated signal, which may be amplitude and/or phase modulated respectively with the amplitude mask 202 and/or the phase mask 204. In some of these embodiments, the reference signal 113 may be a sinusoidal signal, and the application of the symbol mask 206 to the sinusoidal signal may result in a random symbol-modulated signal. Random amplitude and/or phase modulation may be added for increased privacy, which may help reduce the ability of an eavesdropper to exploit environmental and hardware signatures that may be conventionally exploited by the use of a symbol mask alone.

In some embodiments, the amplitude mask 202 and the phase mask 204 may be used to generate in-phase (I) and quadrature-phase (Q) signals. In some embodiments, the reference signal 113 may be randomly generated as a symbol or as a bit modulated signal. In some embodiments, the channel-masking signal 115 may be generated by summing a random signal with amplitude modulated and phase modulated signals. In some embodiments, the symbol mask 206 may comprise a randomly constructed scrambling signal that corresponds to a particular modulation level, such as on/off keying, BPSK, and QAM, although the scope of the embodiments is not limited in this respect.

The channel-masking signal 115 may be a digital signal and the NFC receiver 102 may include digital-to-analog converter to convert a digital channel-masking signal to an analog signal for application to the reactive element 116 for affecting the channel impedance. In these embodiments, the NFC receiver 102 may also include an analog-to-digital converter to convert analog signals received through the reactive element 116 to digitals signals for use by the unmasking circuitry 120.

In accordance with embodiments, the NFC receiver 102 may receive data privately from the NFC transmitter 104 through the resonance-coupled channel 103 and may engage in near-field communication when the NFC receiver 102 is positioned within a near field of the NFC transmitter 104. The near field may be less than about a wavelength of an operating frequency, although less than about a quarter-wavelength may be preferable. The operating frequency may be based on the resonance frequency of the resonance-coupled channel 103. In some embodiments, the reference signal 113 may be a carrier-wave (CW) signal at the operating frequency that is scrambled as described above, although other signal types may also be used.

In accordance with embodiments, the scaling element 118 may provide a residual signal that is zero or close to zero (i.e., as an output) when the NFC transmitter 104 is not affecting the impedance of the resonance-coupled channel 103. Scaling parameters to provide a zero output may be determined during the calibration process. The NFC receiver 102 and the NFC transmitter 104 may perform the calibration process when operating in the near field. The calibration process may determine parameters for use by the scaling element 118. In some embodiments, a training sequence known to both the NFC receiver 102 and the NFC transmitter 104 may be used for calibration. The calibration process may determine a load-impedance estimate of the resonance-coupled channel 103 that takes into account near-field effects of the NFC receiver 102 and the NFC transmitter 104. The calibration process may be performed prior to conveyance of binary data 123 by the NFC transmitter 104. In some embodiments, the calibration process may include the use of a handshake (e.g., a handshake protocol) that includes the use of a known training sequence to determine the channel effects and the signal delay between the NFC receiver 102 and the NFC transmitter 104. The delay may be used to determine the phase scaling by the scaling element 118. The channel effects may be used to determine the amplitude scaling. In some embodiments, the scaling element 118 may perform an impedance transform to channel-masking signal 115 based, at least in part, on near-field effects introduced by the NFC transmitter 104 determined during the calibration process.

In some embodiments, the amplitude mask 202 may provide a random noise mask to help conceal amplitude signature differences between the communicating parties and /or the limitations of scaling element 118 at least in part due to the accuracy of calibration. The phase mask 204 may provide a random noise mask to help conceal temporal signature differences between the communicating parties and /or limitations of scaling element 118 at least in part due to the accuracy of calibration.

In some embodiments, the scaling element 118 may address any large-scale variations in the received signal 117, such as those originating due to the environmental influence (i.e., physical distance) and/or hardware inconsistencies between devices. The scaling element 118 may include a buffer or delay element to mimic the delay introduced by the physical separation between the NFC receiver 102 and the NFC transmitter 104. In digital embodiments, the buffer or delay element may be a digital memory buffer. In analog embodiments, an analog delay line may be used.

The unmasking circuitry 120 may include a transfer function block to modify the received signals 117 to compensate for medium and physical implementation limitations. For example, transfer function block may operate in the impedance domain and may adjust a characteristic impedance of the NFC receiver 102 to match a characteristic impedance of the NFC transmitter 104 and the changes introduced by the physical channel environment.

Although FIG. 1 illustrates the NFC receiver 102 and the NFC transmitter 104 having elements for the one-way communication of binary data 123 from the NFC transmitter 104 to the NFC receiver 102, the scope of the embodiments is not limited in this respect. In some two-way communication embodiments, each NFC device may include the circuitry of both the NFC receiver 102 and the NFC transmitter 104 to provide for two-way communication of data through separate private channels. The NFC receiver 102 and the NFC transmitter 104 may include additional circuitry, such as a processor or controller for coordinating the activities of the illustrated functional elements as well as performing calibration.

In some embodiments, a method for key exchange between devices using NFC is provided. In these embodiments, an NFC device may mask a resonance-coupled channel with a random channel-masking signal. The first NFC device may scale the channel-masking signal based on near-field channel conditions and may unmask signals received through the channel with the scaled channel-masking signal to determine a key conveyed by a second NFC device. The second NFC device may convey the key by affecting an impedance of the resonance-coupled channel based on binary values of the key.

In some embodiments, a system for secure financial transactions between NFC devices is provided. In these embodiments, the system includes an NFC transmitter and an NFC receiver. The NFC receiver may receive financial data from the NFC transmitter through a resonance-coupled channel when positioned within a near-field of the NFC transmitter. The NFC receiver may include a channel-masking signal generator to scramble a reference signal and generate a channel-masking signal for affecting the resonance-coupled channel, and a scaling element to scale the channel-masking signal based on near-field channel conditions. The NFC receiver may also include unmasking circuitry to combine the scaled channel-masking signal with signals received through the resonance-coupled channel to generate binary data. The NFC transmitter may affect the impedance of the resonance-coupled channel based on values of the financial data to be conveyed to the NFC receiver.

In these embodiments, the financial data may include information similar to the information that would be conventionally conveyed by a magnetic strip of a credit card for a credit-card transaction, although the scope of the embodiments is not limited in this respect. In these embodiments, private communication of the financial, medical and other confidential data may be achieved through the random masking of the impedance-coupled channel. The NFC transmitter may be provided within a mobile communication device (e.g., a smart phone) and the NFC receiver may be provided within a point-of-sale (POS) terminal to allow financial information to be conveyed in private.

FIG. 3 is a procedure for private near-field communication in accordance with some embodiments. Procedure 300 may be performed by an NFC receiver, such as NFC receiver 102 (FIG. 1) although other device configurations may also be suitable. Procedure 300 may be implemented to receive data privately from an NFC transmitter, such as NFC transmitter 104 (FIG. 1), through a resonance-coupled channel.

In operation 302, a resonance-coupled channel may be masked with a random channel-masking signal. In some embodiments, a reference signal may be scrambled by modulating it with a mask to generate the channel-masking signal. For true privacy, the mask may comprise a random symbol mask and at least one of an amplitude mask and a phase mask. For lower privacy applications, one of a random symbol mask, an amplitude mask and a phase mask may be used. The NFC receiver may be positioned within the near field of an NFC transmitter, and the application of the channel-masking signal to the resonance-coupled channel may create a private resonance-coupled channel.

In operation 304, the channel-masking signal may be scaled based, at least in part, on near-field channel conditions. The channel-masking signal may be scaled in both amplitude and phase based on scaling parameters determined during a calibration process.

In operation 306, signals received through the resonance-coupled channel may be unmasked by combining the scaled channel-masking signal with the received signals to generate binary data as an output. In these embodiments, the

NFC transmitter may affect the impedance of the resonance-coupled channel based on binary data to be conveyed.

FIG. 4 is a calibration procedure for near-field communication through a private channel in accordance with some embodiments. Calibration procedure 400 may be performed by an NFC receiver, such as NFC receiver 102 (FIG. 1), to determine calibration parameters for private NFCs with an NFC transmitter, such as NFC transmitter 104 (FIG. 1).

In operation 402, a request may be received for a private channel, and in operation 404, the request may be accepted. In some embodiments, the NFC transmitter may request the private channel (e.g., when it has data to send) and the NFC receiver may accept the request, although the scope of the embodiments is not limited in this respect as the NFC receiver may request a private channel and the NFC transmitter may accept the request.

In operation 406, the NFC receiver may receive a known training sequence that is sent by the NFC transmitter. The training sequence may be sent by affecting the impedance of the resonance-coupled channel based on values of the training sequence. For example, an impedance-switching element may be used to affect the impedance of the resonance-coupled channel by switching between a first impedance and a second impedance based on binary values of the training sequence. During receipt of the training sequence, the NFC receiver may scramble a reference signal and may generate a channel-masking signal for application to the resonance-coupled channel.

In operation 408, the NFC receiver may determine calibration parameters based on channel load impedances due to near-field channel conditions. The calibration parameters may be based on a comparison between the known training sequence, the channel masking signal, and signals received through the resonance-coupled channel. The calibration parameters may include the scaling parameters to be used by a scaling element, such as scaling element 118 (FIG. 1).

In operation 410, the NFC receiver may determine whether sufficient privacy is achieved. If sufficient privacy is not achieved, operations 406 and 408 may be repeated and the NFC receiver may change the channel mask. Once sufficient privacy is achieved, the calibration parameters may be stored for use by the scaling element.

In operation 412, the NFC receiver may send a confirmation to the NFC transmitter that sufficient privacy has been achieved.

In operation 414, data may be received through the private channel. In some embodiments, operation 414 may include performing the operations of procedure 300 (FIG. 3).

The calibration procedure 400 may provide the NFC receiver with, among other things, estimates of the load impedances and channel propagation delays, allowing the NFC receiver to adjust its mean signal levels to help provide complete ambiguity, while, at the same time, helping to insure the use of minimum signal levels to address power consumption as well as to provide additional layers of privacy. Although the calibration procedure 400 is performed in an open or unsecure environment and impedances may be determined by an eavesdropper, operations 406 – 410 may be repeated until the target confidence level of privacy is achieved when combined with the use of a randomly scrambled reference signal.

Embodiments described herein are applicable to several types of near-field communication depending on the system configuration, mode of operation, and desired level of security. In passive modes of operation, the NFC transmitter does not have channel masking or de/encryption capability, so private communication may occur one way. In this situation, the NFC receiver provides the channel masking function. This mode may be used for passive applications such as bus tickets, credit cards and other low-cost RFID tags. In some of these embodiments, an encryption key may also be used.

In some active modes of operation, the NFC receiver and the NFC transmitter may switch their channel-masking functions subsequently. In these embodiments, the NFC receiver may include the functional elements of an NFC transmitter, such as NFC transmitter 104 (FIG. 1), and the NFC transmitter may include the functional elements of an NFC receiver, such as NFC receiver 102 (FIG. 1). In these embodiments, bi-directional data communication may occur within private channels. These modes may be used in systems where sufficient power is available to both NFC devices and in situations where security is not provided by an application layer.

In a hybrid mode of operation, the NFC receiver and the NFC transmitter may perform a key exchange in a secure manner. The keys may be used for open encrypted communications. In a multimodal mode operation, the NFC receiver and the NFC transmitter perform key exchange. Subsequent encrypted communications may occur in a private channel. This multimodal mode may provide a higher level of security because the communications are both encrypted and private.

Although the NFC receiver 102 and the NFC transmitter 104 are illustrated as having several separate functional elements, one or more of the functional elements may be combined and may be implemented by combinations of software-configured elements, such as processing elements including digital signal processors (DSPs), and/or other hardware elements. For example, some elements may comprise one or more microprocessors, DSPs, application specific integrated circuits (ASICs), radio-frequency integrated circuits (RFICs) and combinations of various hardware and logic circuitry for performing at least the functions described herein. In some embodiments, the functional elements of the NFC receiver 102 and the NFC transmitter 104 may refer to one or more processes operating on one or more processing elements.

Embodiments may be implemented in one or a combination of hardware, firmware and software. Embodiments may also be implemented as instructions stored on a computer-readable storage device, which may be read and executed by at least one processor to perform the operations described herein. A computer-readable storage device may include any non-transitory mechanism for storing information in a form readable by a machine (e.g., a computer). For example, a computer-readable storage device may include read-only memory (ROM), random-access memory (RAM), magnetic disk storage media, optical storage media, flash-memory devices, and other storage devices and media. In some embodiments, the NFC receiver 102 and the NFC transmitter 104 may include one or more processors and may be configured with instructions stored on a computer-readable storage device.

The Abstract is provided to comply with 37 C.F.R. Section 1.72(b) requiring an abstract that will allow the reader to ascertain the nature and gist of the technical disclosure. It is submitted with the understanding that it will not be used to limit or interpret the scope or meaning of the claims. The following claims are hereby incorporated into the detailed description, with each claim standing on its own as a separate embodiment.

CLAIMS

What is claimed is:

1. A near-field communication (NFC) system comprising an NFC receiver to receive data privately from an NFC transmitter through a resonance-coupled channel, the NFC receiver comprising:

a channel-masking signal generator to scramble a reference signal and generate a channel-masking signal for application to the resonance-coupled channel;

a scaling element to scale the channel-masking signal based, at least in part, on near-field channel conditions; and

unmasking circuitry to combine the scaled channel-masking signal with resonance-coupled signals received through the resonance-coupled channel to generate binary data as an output comprising unmasked bits.

2. The NFC system of claim 1 wherein the NFC transmitter comprises an impedance-switching element to affect an impedance of the resonance-coupled channel based on binary data to be conveyed to the NFC receiver.

3. The NFC system of claim 2 wherein the impedance-switching element is to affect the impedance of the resonance-coupled channel by switching between a first impedance and a second impedance based on the binary data that is to be conveyed to the NFC receiver.

4. The NFC system of claim 2 wherein the NFC receiver further comprises a reactive element to affect the resonance-coupled channel with the channel-masking signal and receive the resonance-coupled signals, and

wherein the NFC transmitter further comprises a reactive element to modulate the resonance-coupled channel based on a switched impedance signal provided by the impedance-switching element.

5. The NFC system of claim 2 wherein the NFC receiver further comprises a first antenna to provide the resonance-coupled channel affected with the channel-masking signal and receive the resonance-coupled signals, and

wherein the NFC transmitter further comprises a second antenna to modulate the resonance-coupled channel based on a switched impedance signal provided by the impedance-switching element.

6. The NFC system of claim 1 wherein the NFC receiver is part of an NFC reader and the NFC transmitter is part of an NFC tag.

7. The NFC system of claim 1 wherein the scaling element is to scale the channel-masking signal in both amplitude and phase based on parameters determined during a calibration process.

8. The NFC system of claim 1 wherein the channel-masking signal generator is to scramble the reference signal by modulating the reference signal with a mask to generate the channel-masking signal, and

wherein the mask comprises a random symbol mask, and at least one of an amplitude mask and a phase mask.

9. The NFC system of claim 8 wherein the symbol mask, the amplitude mask and the phase mask comprise non-correlated random sequences.

10. The NFC system of claim 1 wherein the NFC receiver is to receive data privately from the NFC transmitter through the resonance-coupled channel when the NFC receiver is positioned within a near field of the NFC transmitter, the near field being less than ¼ wavelength of an operating frequency.

11. The NFC system of claim 10 wherein when the NFC receiver and the NFC transmitter are configured to perform a calibration process when operating in the near field, the calibration process to determine parameters for use by the scaling element.

12. A method for private communication through a resonance-coupled channel, the method comprising:

masking the resonance-coupled channel with a random channel-masking signal;

scaling the channel-masking signal based on near-field channel conditions; and

unmasking signals received through the resonance-coupled channel with the scaled channel-masking signal to determine data, the data conveyed by a transmitting device by affecting an impedance of the resonance-coupled channel.

13. The method of claim 12 wherein the transmitting device is to affect the impedance of the resonance-coupled channel based on binary data to be conveyed to a receiving device,

wherein masking comprises scrambling a reference signal by modulating the reference signal with a mask to generate the random channel-masking signal, and

wherein the mask comprises one of a random symbol mask, an amplitude mask and a phase mask.

14. The method of claim 13 wherein masking includes affecting the resonance-coupled channel with the channel-masking signal using a first reactive element,

wherein the method includes receiving the signals through the resonance-coupled channel with the first reactive element,

wherein a second reactive element is used by the transmitting device to modulate the resonance-coupled channel based on a switched impedance signal.

15. The method of claim 14 wherein the receiving device is to receive data privately from the transmitting device through the resonance-coupled channel when the receiving device is positioned within a near field of the transmitting device, the near field being less than ¼ wavelength of an operating frequency.

16. A method for secure key exchange between devices using near-field communication, the method comprising:

masking, by a first near-field communication (NFC) device, a resonance-coupled channel with a random channel-masking signal;

scaling, by the first NFC device, the channel-masking signal based on near-field channel conditions; and

unmasking signals received through the resonance-coupled channel by the first NFC device with the scaled channel-masking signal to determine a key conveyed to a second NFC device by affecting an impedance of the resonance-coupled channel based on binary values of the key.

17. A system for secure financial transactions between near-field communication (NFC) devices, the system comprising an NFC transmitter and an NFC receiver to receive financial data from the NFC transmitter through a resonance-coupled channel when positioned within a near-field of the NFC transmitter, the NFC receiver comprising:

a channel-masking signal generator to scramble a reference signal and generate a channel-masking signal for modulating the resonance-coupled channel;

a scaling element to scale the channel-masking signal based on near-field channel conditions; and

unmasking circuitry to combine the scaled channel-masking signal with signals received through the resonance-coupled channel to generate binary data as an output comprising unmasked bits,

wherein the NFC transmitter is to affect an impedance of the resonance-coupled channel based on values of the financial data to be conveyed to the NFC receiver.

18. The system of claim 17 wherein the NFC transmitter is provided with a mobile communication device (smart phone) and wherein the NFC receiver is provided within a point-of-sale (POS) terminal.

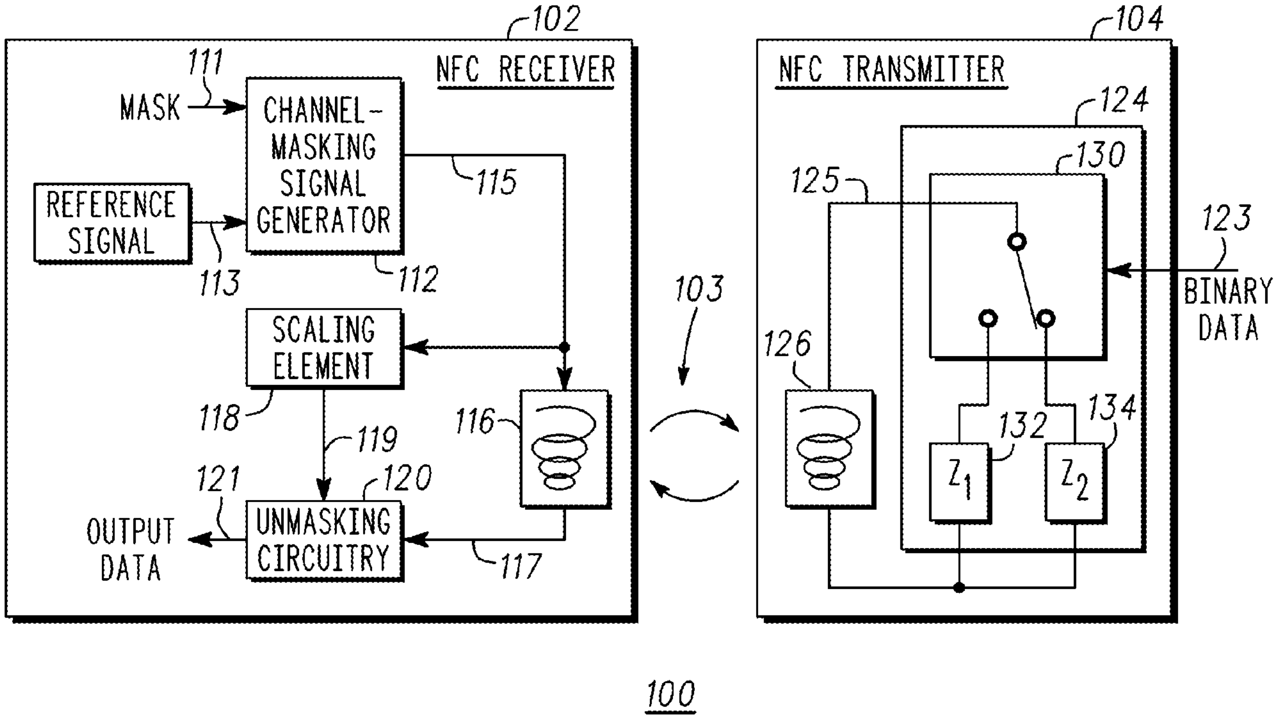

102
NFC RECEIVER
111
MASK
CHANNEL-MASKING SIGNAL GENERATOR
REFERENCE SIGNAL
115
113
112
SCALING ELEMENT
118
119
116
121
120
OUTPUT DATA
UNMASKING CIRCUITRY
117
103
104
NFC TRANSMITTER
124
130
125
123
BINARY DATA
126
132
134
Z_1
Z_2
100

Fig. 1

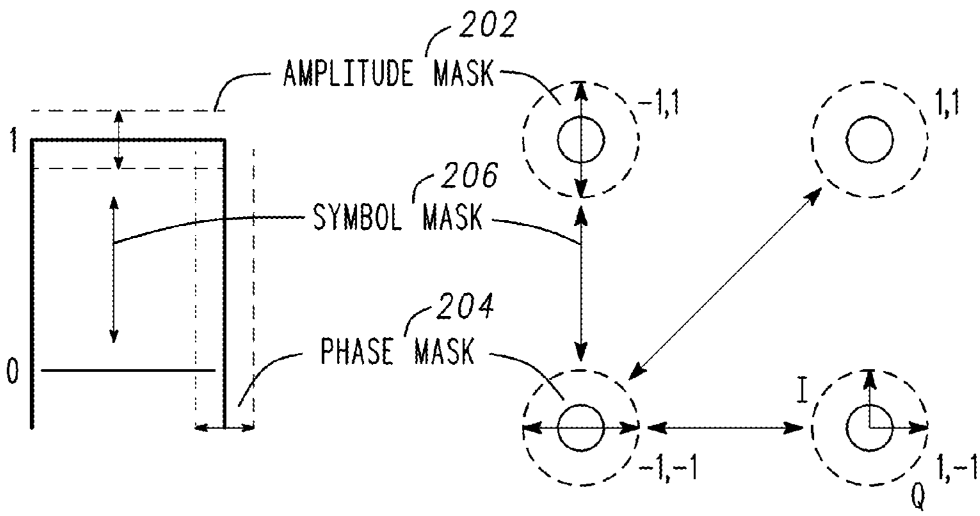

202
AMPLITUDE MASK
-1,1
1,1
1
206
SYMBOL MASK
204
PHASE MASK
0
I
-1,-1
1,-1
Q

Fig. 2

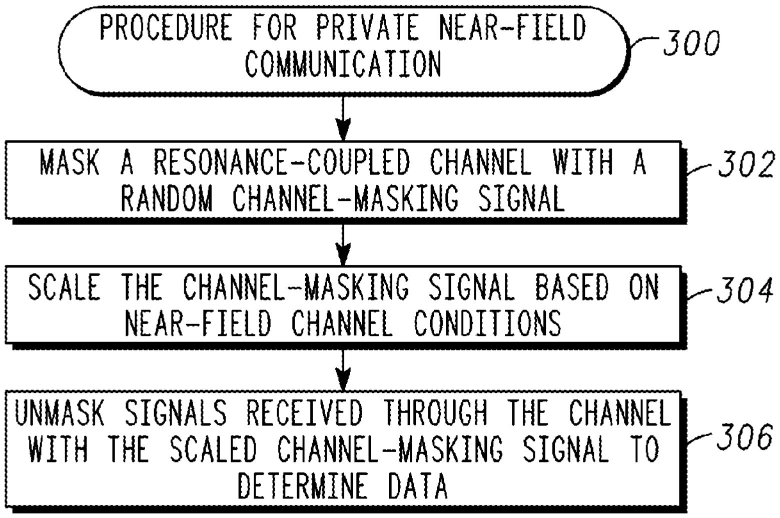

PROCEDURE FOR PRIVATE NEAR-FIELD COMMUNICATION
300
MASK A RESONANCE-COUPLED CHANNEL WITH A RANDOM CHANNEL-MASKING SIGNAL
302
SCALE THE CHANNEL-MASKING SIGNAL BASED ON NEAR-FIELD CHANNEL CONDITIONS
304
UNMASK SIGNALS RECEIVED THROUGH THE CHANNEL WITH THE SCALED CHANNEL-MASKING SIGNAL TO DETERMINE DATA
306

Fig. 3

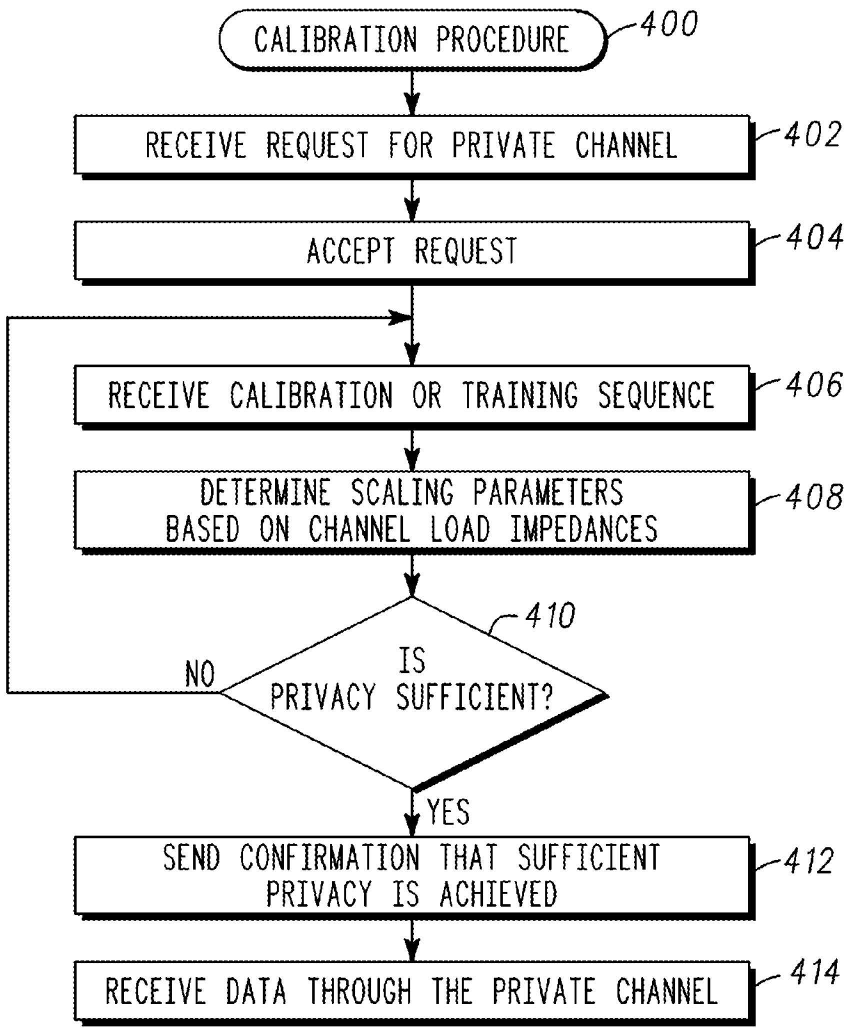

CALIBRATION PROCEDURE
400
RECEIVE REQUEST FOR PRIVATE CHANNEL
402
ACCEPT REQUEST
404
RECEIVE CALIBRATION OR TRAINING SEQUENCE
406
DETERMINE SCALING PARAMETERS BASED ON CHANNEL LOAD IMPEDANCES
408
IS PRIVACY SUFFICIENT?
410
NO
YES
SEND CONFIRMATION THAT SUFFICIENT PRIVACY IS ACHIEVED
412
RECEIVE DATA THROUGH THE PRIVATE CHANNEL
414

Fig. 4

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2013/021955

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04B5/00
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y A	US 2004/179510 A1 (KUFFNER STEPHEN [US] ET AL) 16 September 2004 (2004-09-16) paragraphs [0046] - [0059], [0096] - [0099], [0113], [0126], [0127], [0130], [0143], [0165], [0167]; figures 11,15,16 -----	1,6,7, 10-12,16 2-5,8,9, 13-15, 17,18
Y A	US 2009/138715 A1 (XIAO SHENG [US] ET AL) 28 May 2009 (2009-05-28) paragraphs [0004] - [0006], [0050], [0072], [0082], [0094] - [0118], [0138], [0139], [0142]; figure 4 ----- -/--	1,6,7, 10-12,16 2-5,8,9, 13-15, 17,18

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
19 June 2013	01/07/2013

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Ernst, Christian

1

International application No
PCT/US2013/021955

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 01/15064 A1 (PHYSICAL OPTICS CORP [US]) 1 March 2001 (2001-03-01) page 1, lines 10-16 page 3, line 21 - page 4, line 30 page 6, line 24 - page 7, line 9 page 13, line 27 - page 20, line 14 page 36, line 23 - page 37, line 12 page 38, line 11 - page 39, line 10 -----	1-18

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2013/021955

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2004179510 A1	16-09-2004	CN 1759324 A	12-04-2006
		EP 1601981 A2	07-12-2005
		JP 2006521036 A	14-09-2006
		KR 20050115902 A	08-12-2005
		TW I242346 B	21-10-2005
		US 2004179510 A1	16-09-2004
		WO 2004082304 A2	23-09-2004
US 2009138715 A1	28-05-2009	NONE	
WO 0115064 A1	01-03-2001	AU 6629400 A	19-03-2001
		CA 2381517 A1	01-03-2001
		CN 1399764 A	26-02-2003
		EP 1218850 A1	03-07-2002
		EP 2107498 A2	07-10-2009
		JP 2003528363 A	24-09-2003
		KR 20080088664 A	02-10-2008
		TW 484106 B	21-04-2002
		US 6744909 B1	01-06-2004
		US 2004101168 A1	27-05-2004
		WO 0115064 A1	01-03-2001