US 20080240440A1

(19) United States

(12) Patent Application Publication

(10) Pub. No.: US 2008/0240440 A1

(43) Pub. Date: Oct. 2, 2008

Rose et al.

(54) SYNCHRONIZATION TEST FOR DEVICE AUTHENTICATION

(76) Inventors: **Gregory Gordon Rose**, San Diego, CA (US); **Lu Xiao**, San Diego, CA (US); **David Jonathan JULIAN**, San Diego, CA (US)

Correspondence Address:
QUALCOMM INCORPORATED
5775 MOREHOUSE DR.
SAN DIEGO, CA 92121 (US)

(21) Appl. No.: **11/844,855**

(22) Filed: **Aug. 24, 2007**

Related U.S. Application Data

(60) Provisional application No. 60/908,271, filed on Mar. 27, 2007.

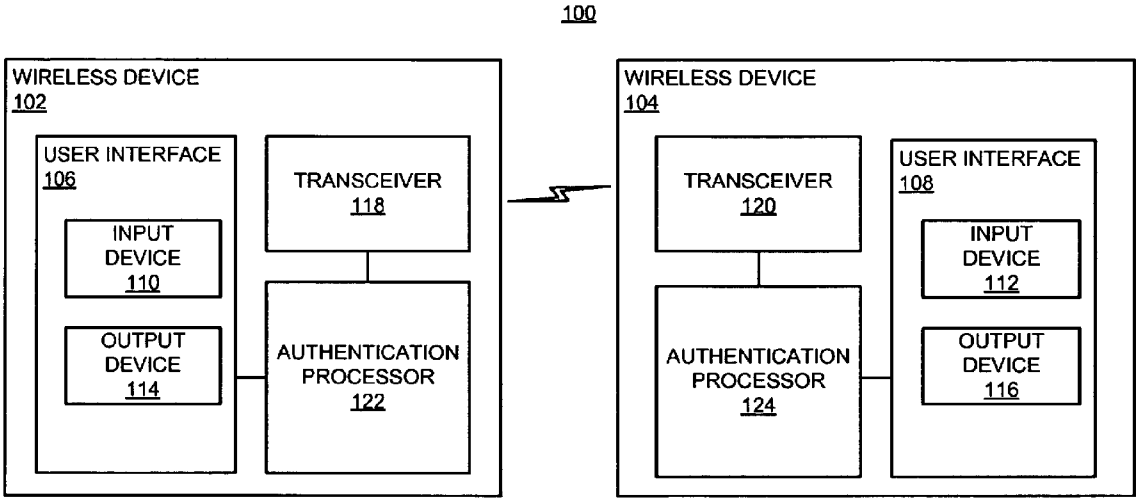
Publication Classification

(51) **Int. Cl.**
H04L 9/30 (2006.01)
H04L 9/32 (2006.01)

(52) **U.S. Cl.** **380/277**; 713/169

(57) **ABSTRACT**

Device authentication is based on the ability of a human to synchronize the movements of his or her fingers. A pairing procedure for two wireless devices may thus involve a synchronization test that is based on the relative timing of actuations of input devices on each of the wireless devices. In some aspects a synchronization test involves determining whether actuations of user input devices on two different wireless devices occurred within a defined time interval. In some aspects a synchronization test involves comparing time intervals defined by multiple actuations of user input devices on two wireless devices.



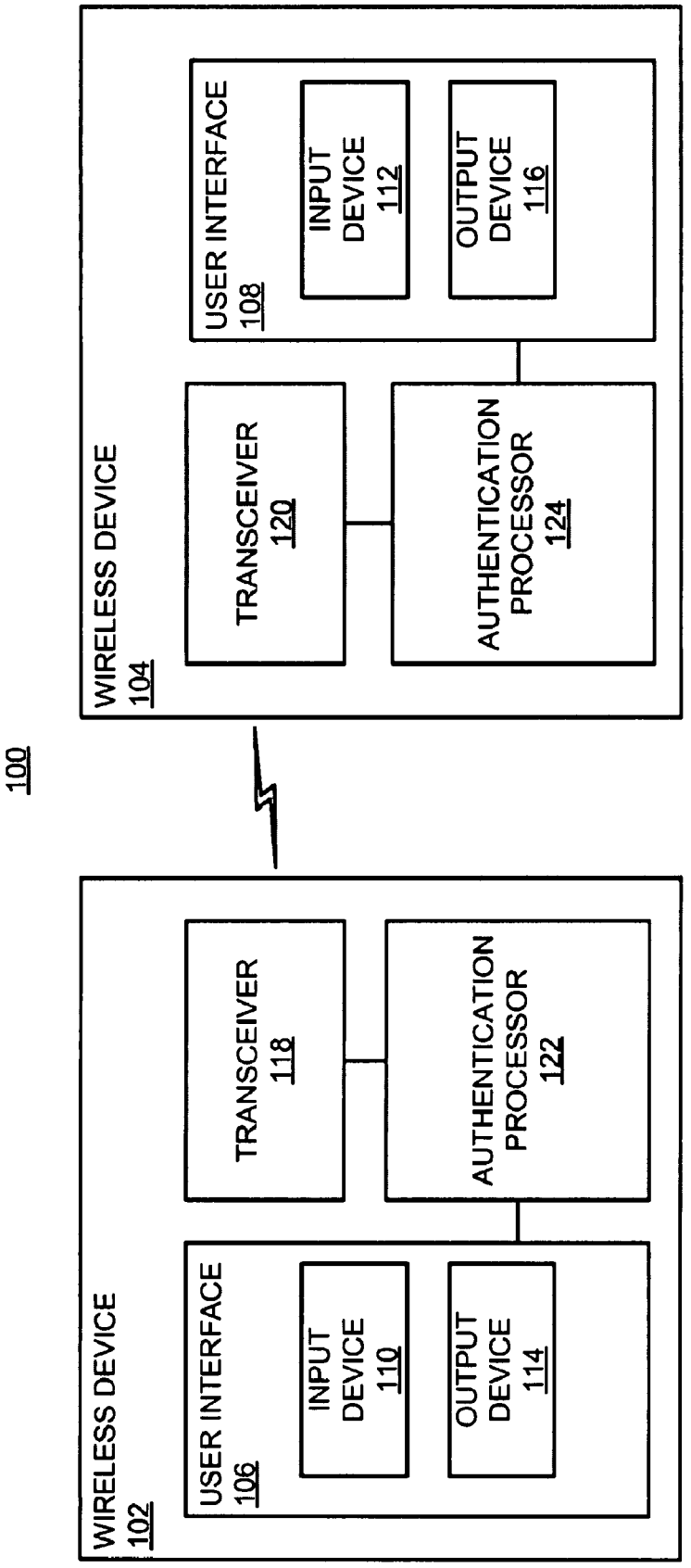

100
WIRELESS DEVICE
102
USER INTERFACE
106
INPUT DEVICE
110
OUTPUT DEVICE
114
TRANSCEIVER
118
AUTHENTICATION PROCESSOR
122
WIRELESS DEVICE
104
USER INTERFACE
108
INPUT DEVICE
112
OUTPUT DEVICE
116
TRANSCEIVER
120
AUTHENTICATION PROCESSOR
124

FIG. 1

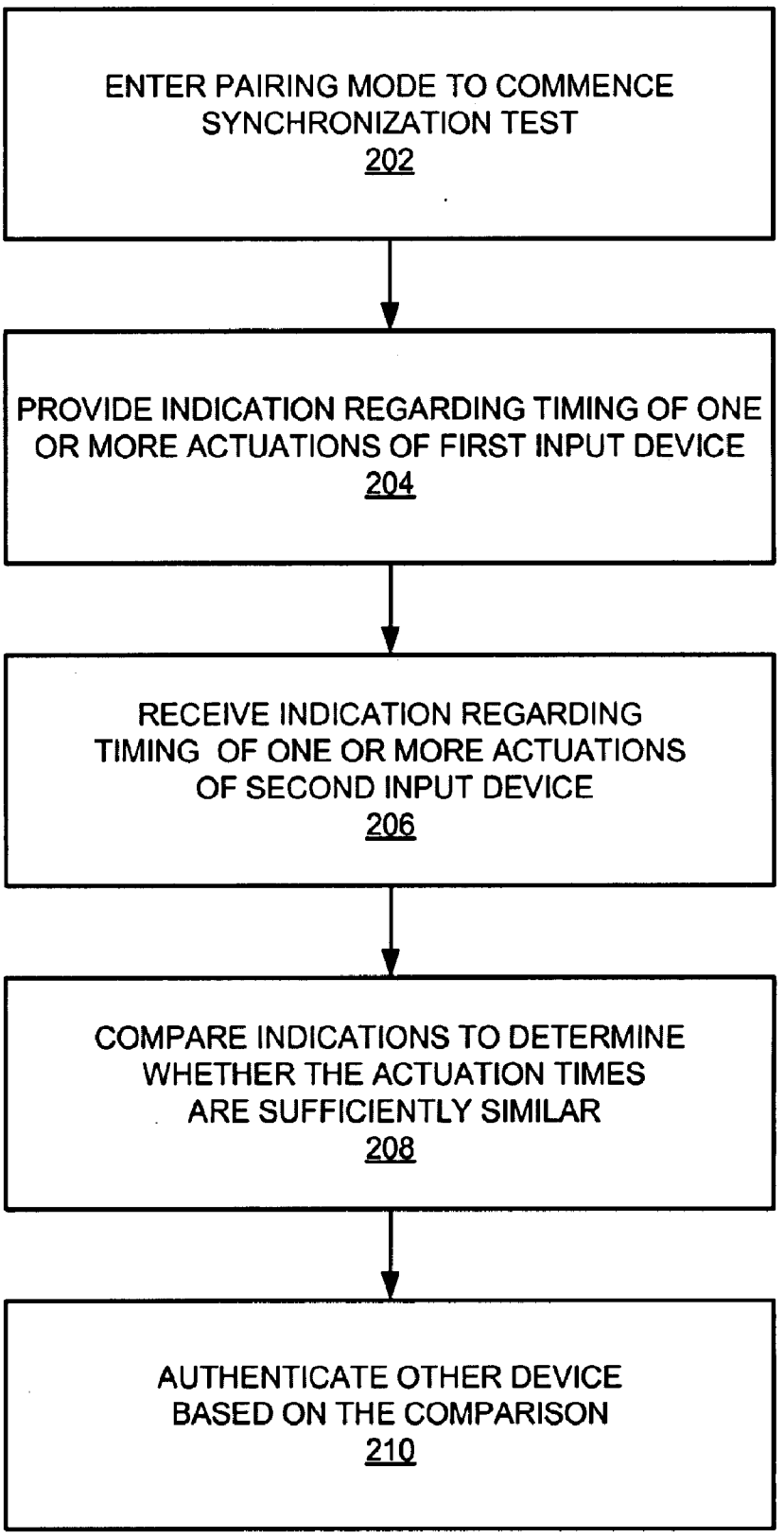

ENTER PAIRING MODE TO COMMENCE SYNCHRONIZATION TEST
202
PROVIDE INDICATION REGARDING TIMING OF ONE OR MORE ACTUATIONS OF FIRST INPUT DEVICE
204
RECEIVE INDICATION REGARDING TIMING OF ONE OR MORE ACTUATIONS OF SECOND INPUT DEVICE
206
COMPARE INDICATIONS TO DETERMINE WHETHER THE ACTUATION TIMES ARE SUFFICIENTLY SIMILAR
208
AUTHENTICATE OTHER DEVICE BASED ON THE COMPARISON
210

FIG. 2

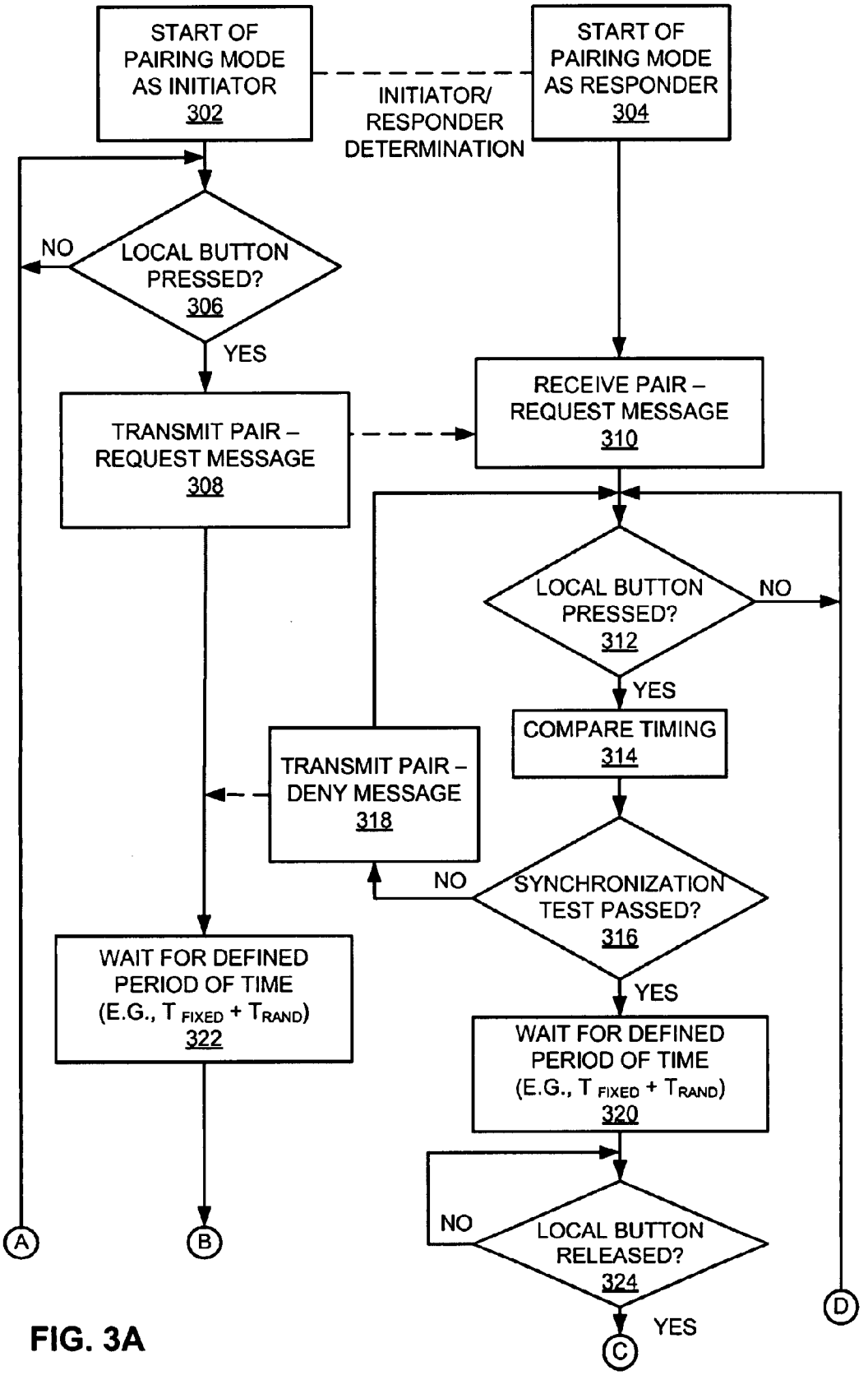

START OF PAIRING MODE AS INITIATOR 302
INITIATOR/ RESPONDER DETERMINATION
START OF PAIRING MODE AS RESPONDER 304
LOCAL BUTTON PRESSED? 306
NO
YES
TRANSMIT PAIR – REQUEST MESSAGE 308
RECEIVE PAIR – REQUEST MESSAGE 310
LOCAL BUTTON PRESSED? 312
NO
YES
COMPARE TIMING 314
TRANSMIT PAIR – DENY MESSAGE 318
SYNCHRONIZATION TEST PASSED? 316
NO
YES
WAIT FOR DEFINED PERIOD OF TIME (E.G., T FIXED + T RAND) 322
WAIT FOR DEFINED PERIOD OF TIME (E.G., T FIXED + T RAND) 320
LOCAL BUTTON RELEASED? 324
NO
YES
A
B
C
D

FIG. 3A

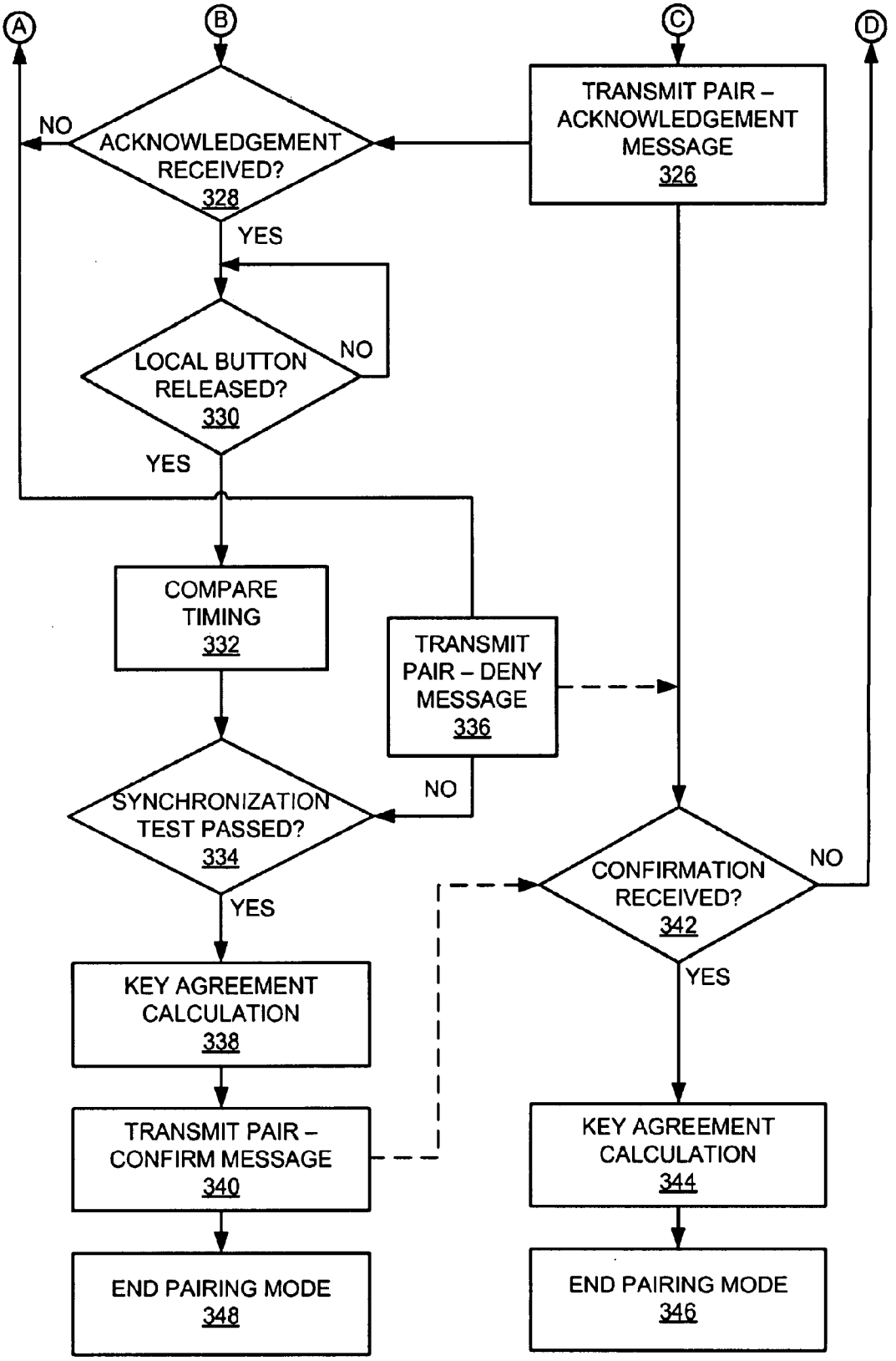

A
B
C
D
TRANSMIT PAIR – ACKNOWLEDGEMENT MESSAGE 326
NO
ACKNOWLEDGEMENT RECEIVED? 328
YES
LOCAL BUTTON RELEASED? 330
NO
YES
COMPARE TIMING 332
TRANSMIT PAIR – DENY MESSAGE 336
NO
SYNCHRONIZATION TEST PASSED? 334
YES
CONFIRMATION RECEIVED? 342
NO
YES
KEY AGREEMENT CALCULATION 338
TRANSMIT PAIR – CONFIRM MESSAGE 340
KEY AGREEMENT CALCULATION 344
END PAIRING MODE 348
END PAIRING MODE 346

FIG. 3B

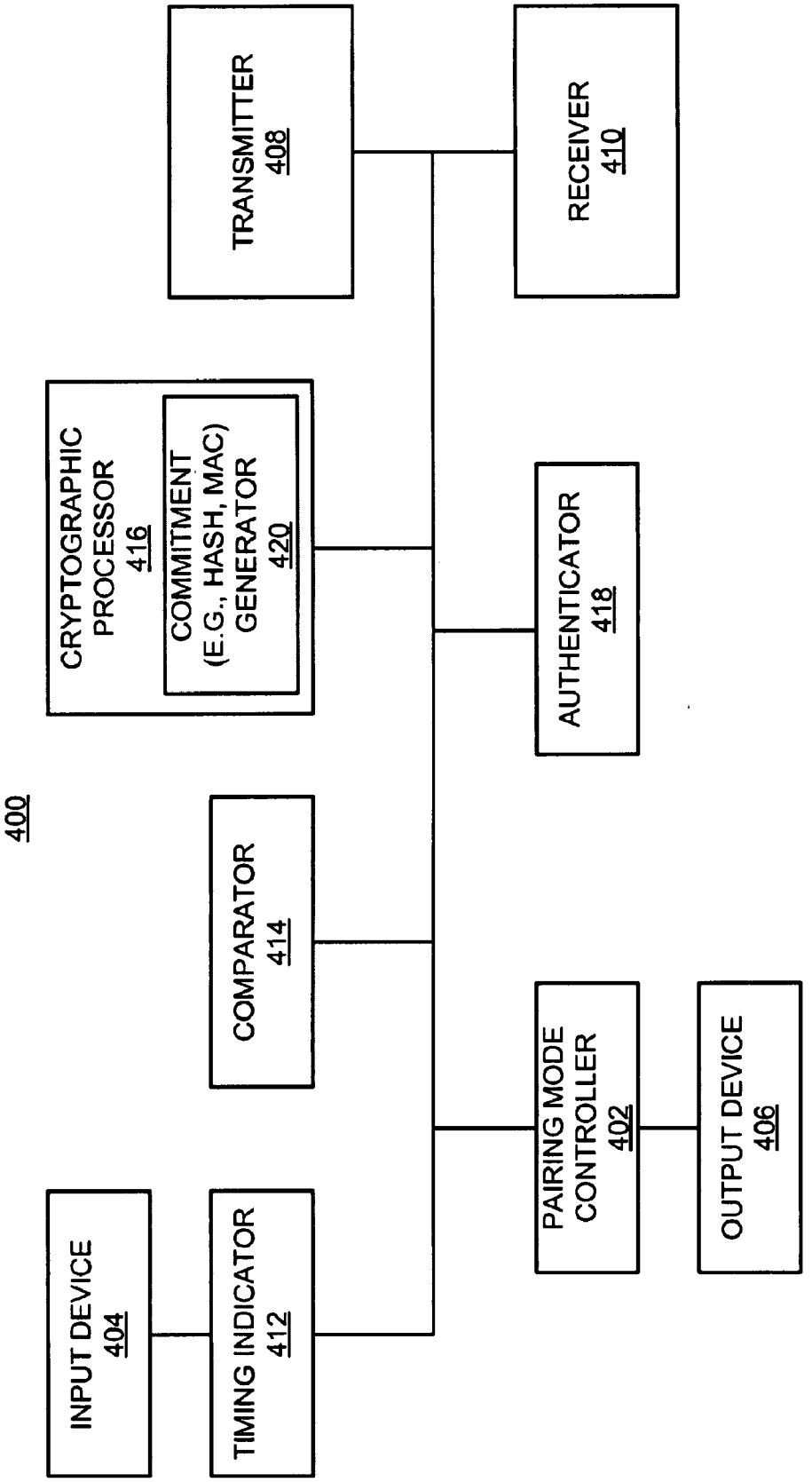

400
TRANSMITTER 408
RECEIVER 410
CRYPTOGRAPHIC PROCESSOR 416
COMMITMENT (E.G., HASH, MAC) GENERATOR 420
AUTHENTICATOR 418
COMPARATOR 414
PAIRING MODE CONTROLLER 402
OUTPUT DEVICE 406
INPUT DEVICE 404
TIMING INDICATOR 412

FIG. 4

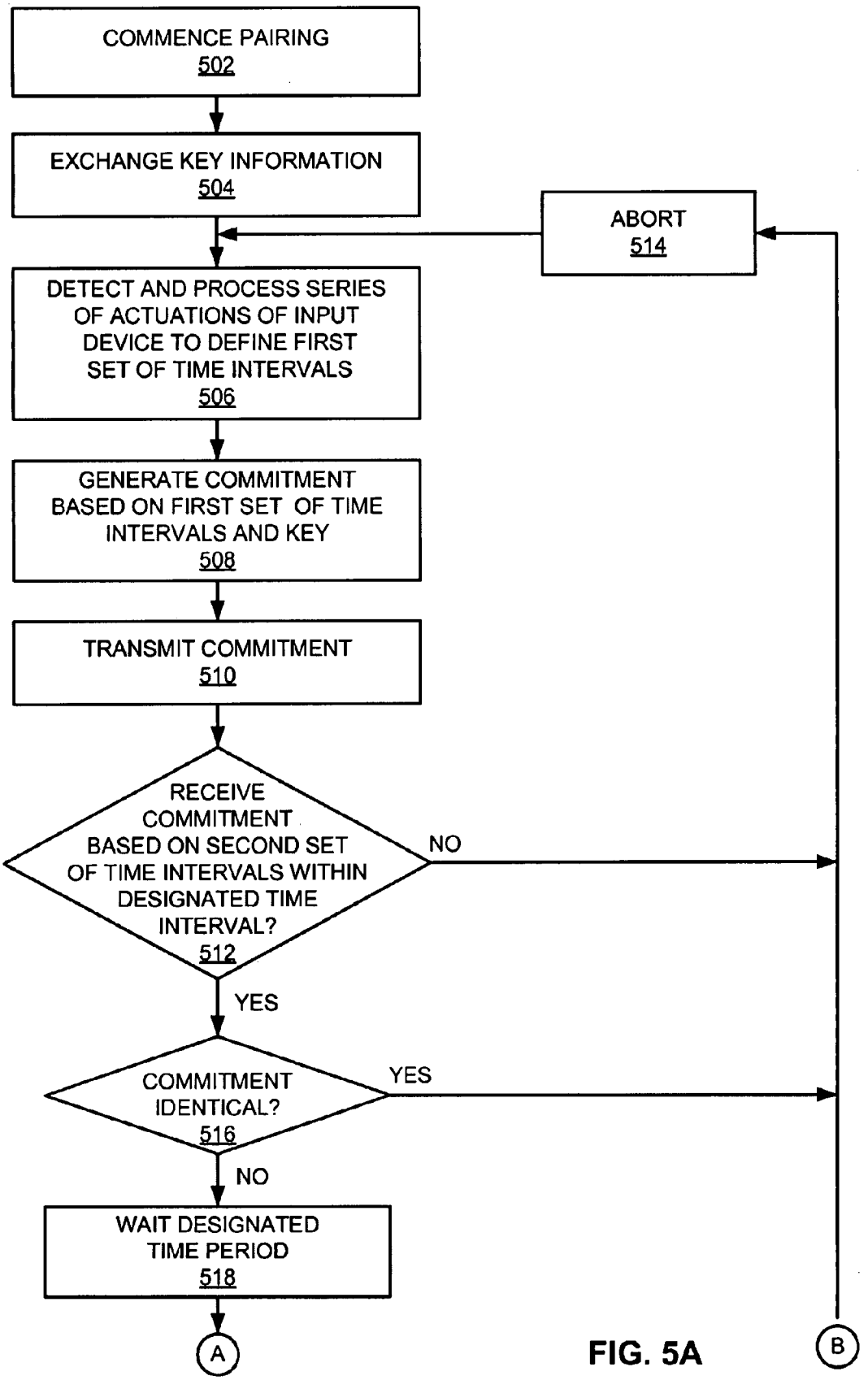

COMMENCE PAIRING
502
EXCHANGE KEY INFORMATION
504
ABORT
514
DETECT AND PROCESS SERIES OF ACTUATIONS OF INPUT DEVICE TO DEFINE FIRST SET OF TIME INTERVALS
506
GENERATE COMMITMENT BASED ON FIRST SET OF TIME INTERVALS AND KEY
508
TRANSMIT COMMITMENT
510
RECEIVE COMMITMENT BASED ON SECOND SET OF TIME INTERVALS WITHIN DESIGNATED TIME INTERVAL?
512
NO
YES
COMMITMENT IDENTICAL?
516
YES
NO
WAIT DESIGNATED TIME PERIOD
518
A
B

FIG. 5A

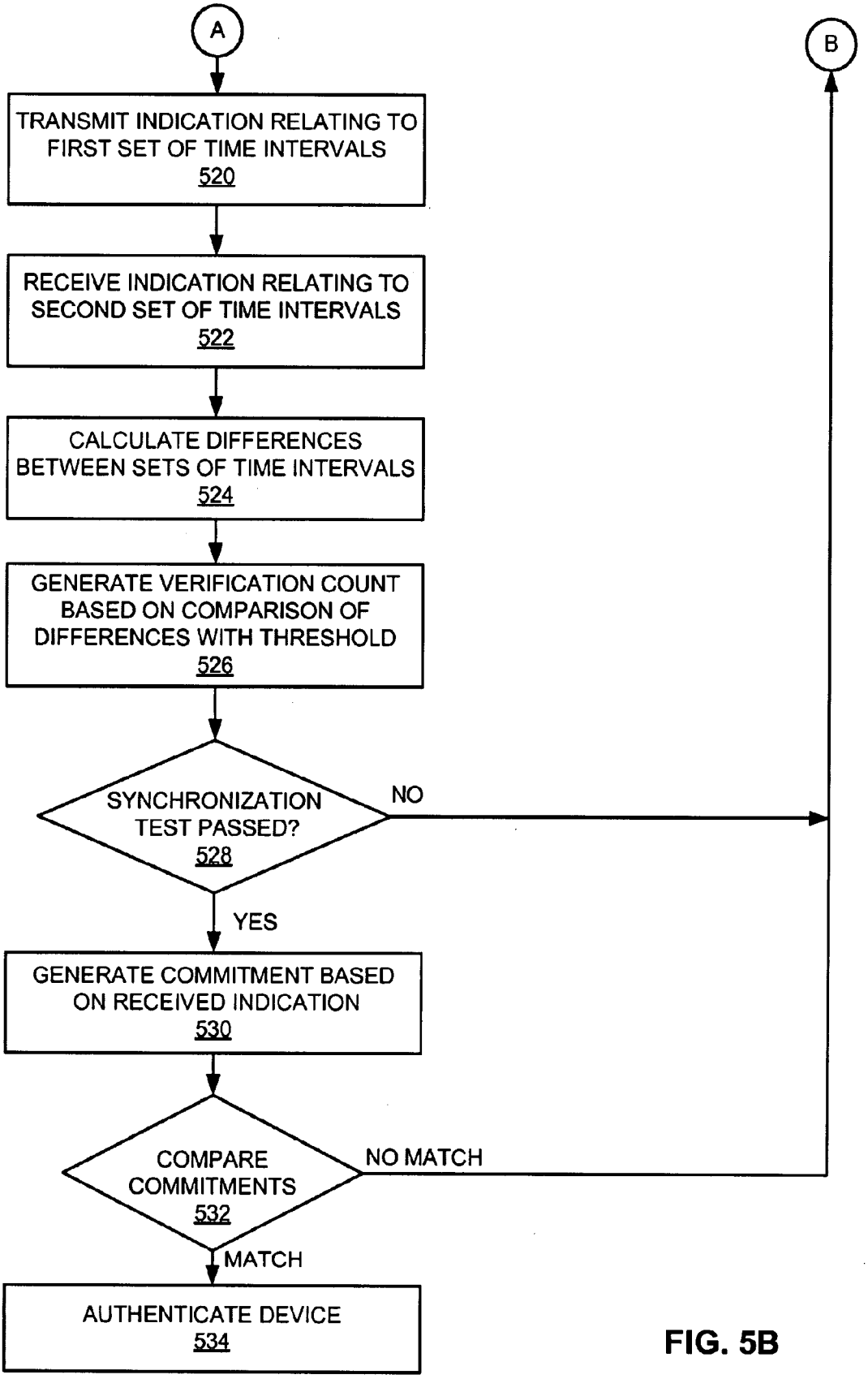

A
B
TRANSMIT INDICATION RELATING TO FIRST SET OF TIME INTERVALS
520
RECEIVE INDICATION RELATING TO SECOND SET OF TIME INTERVALS
522
CALCULATE DIFFERENCES BETWEEN SETS OF TIME INTERVALS
524
GENERATE VERIFICATION COUNT BASED ON COMPARISON OF DIFFERENCES WITH THRESHOLD
526
SYNCHRONIZATION TEST PASSED?
528
NO
YES
GENERATE COMMITMENT BASED ON RECEIVED INDICATION
530
COMPARE COMMITMENTS
532
NO MATCH
MATCH
AUTHENTICATE DEVICE
534

FIG. 5B

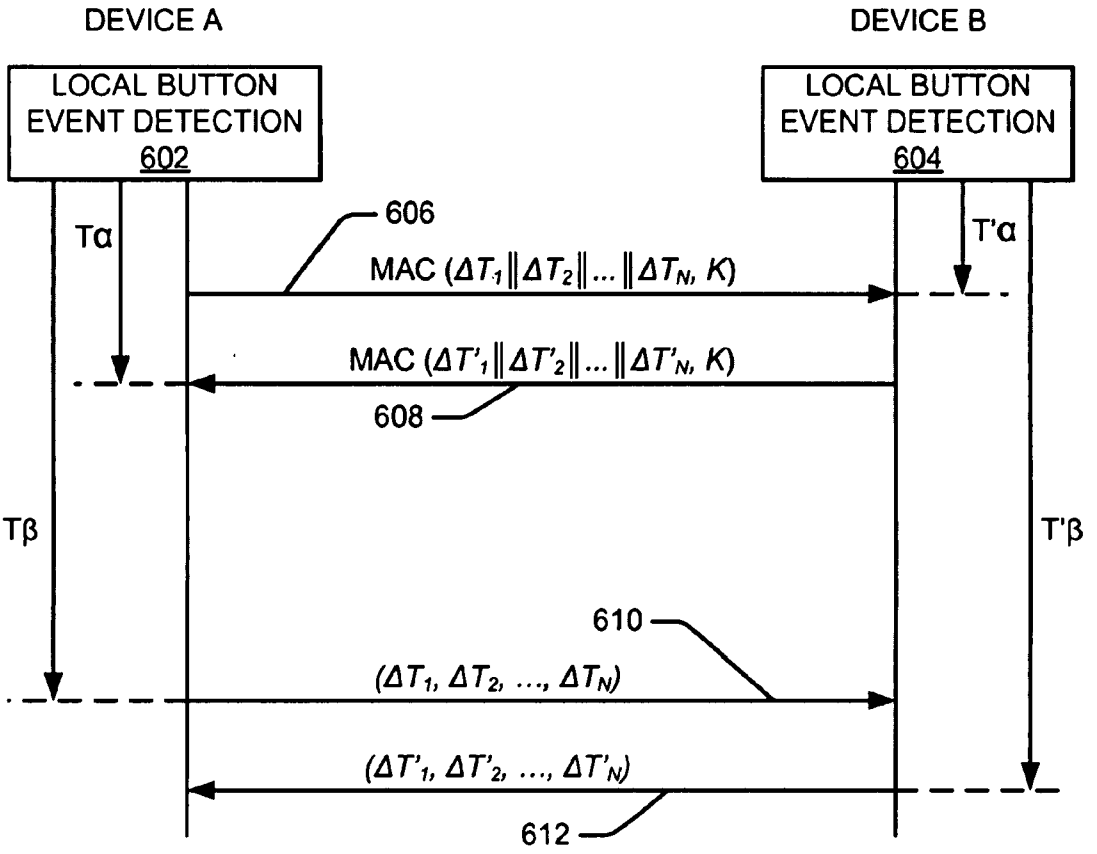

DEVICE A
DEVICE B
LOCAL BUTTON EVENT DETECTION 602
LOCAL BUTTON EVENT DETECTION 604
606
Tα
T'α
MAC ($\Delta T_1 \| \Delta T_2 \| \ldots \| \Delta T_N$, K)
MAC ($\Delta T'_1 \| \Delta T'_2 \| \ldots \| \Delta T'_N$, K)
608
Tβ
T'β
610
(ΔT_1, ΔT_2, ..., ΔT_N)
($\Delta T'_1$, $\Delta T'_2$, ..., $\Delta T'_N$)
612

FIG. 6

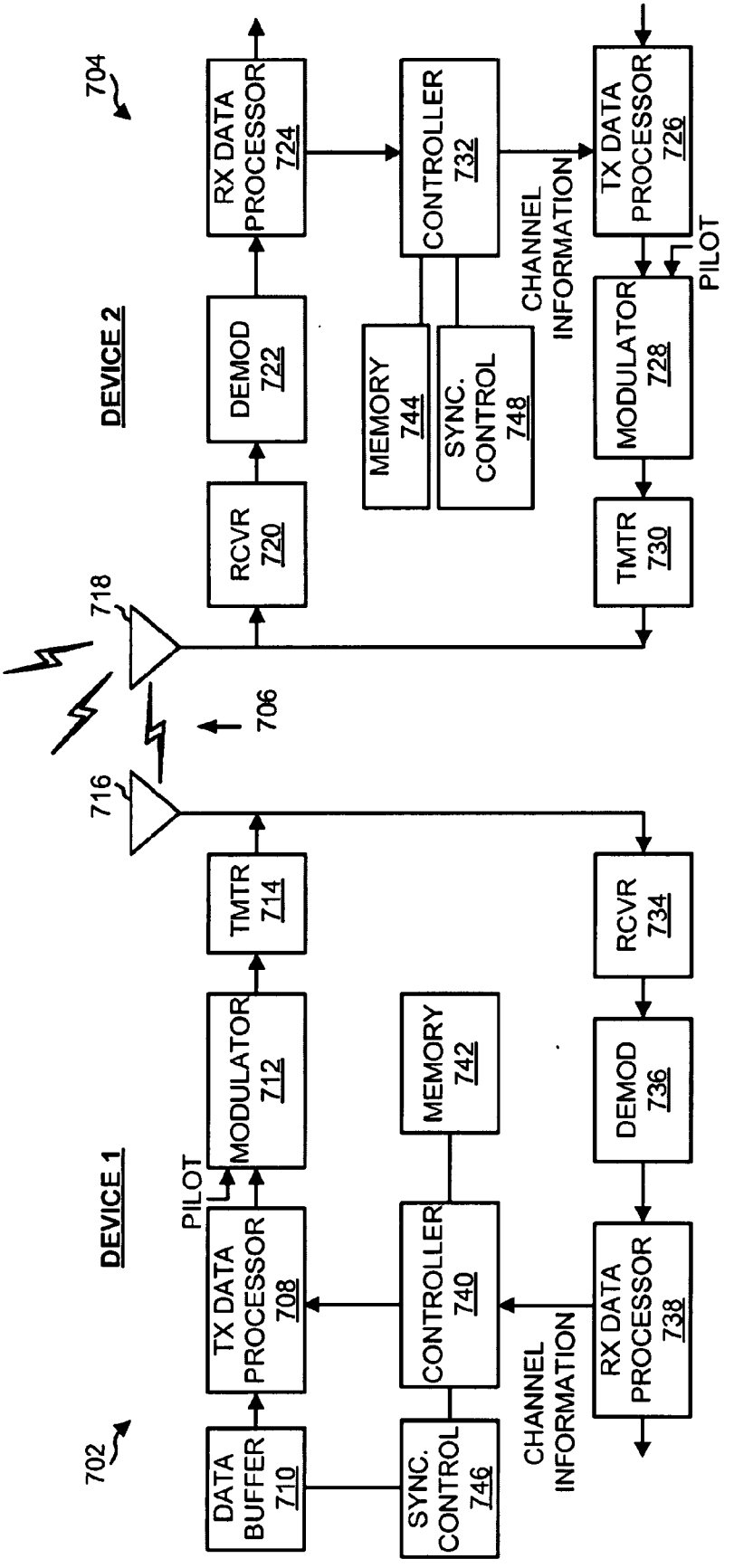

DEVICE 1
DEVICE 2
702
704
706
716
718
DATA BUFFER 710
TX DATA PROCESSOR 708
MODULATOR 712
TMTR 714
SYNC. CONTROL 746
CONTROLLER 740
MEMORY 742
PILOT
CHANNEL INFORMATION
RX DATA PROCESSOR 738
DEMOD 736
RCVR 734
RCVR 720
DEMOD 722
RX DATA PROCESSOR 724
MEMORY 744
SYNC. CONTROL 748
CONTROLLER 732
CHANNEL INFORMATION
TX DATA PROCESSOR 726
MODULATOR 728
PILOT
TMTR 730

FIG. 7

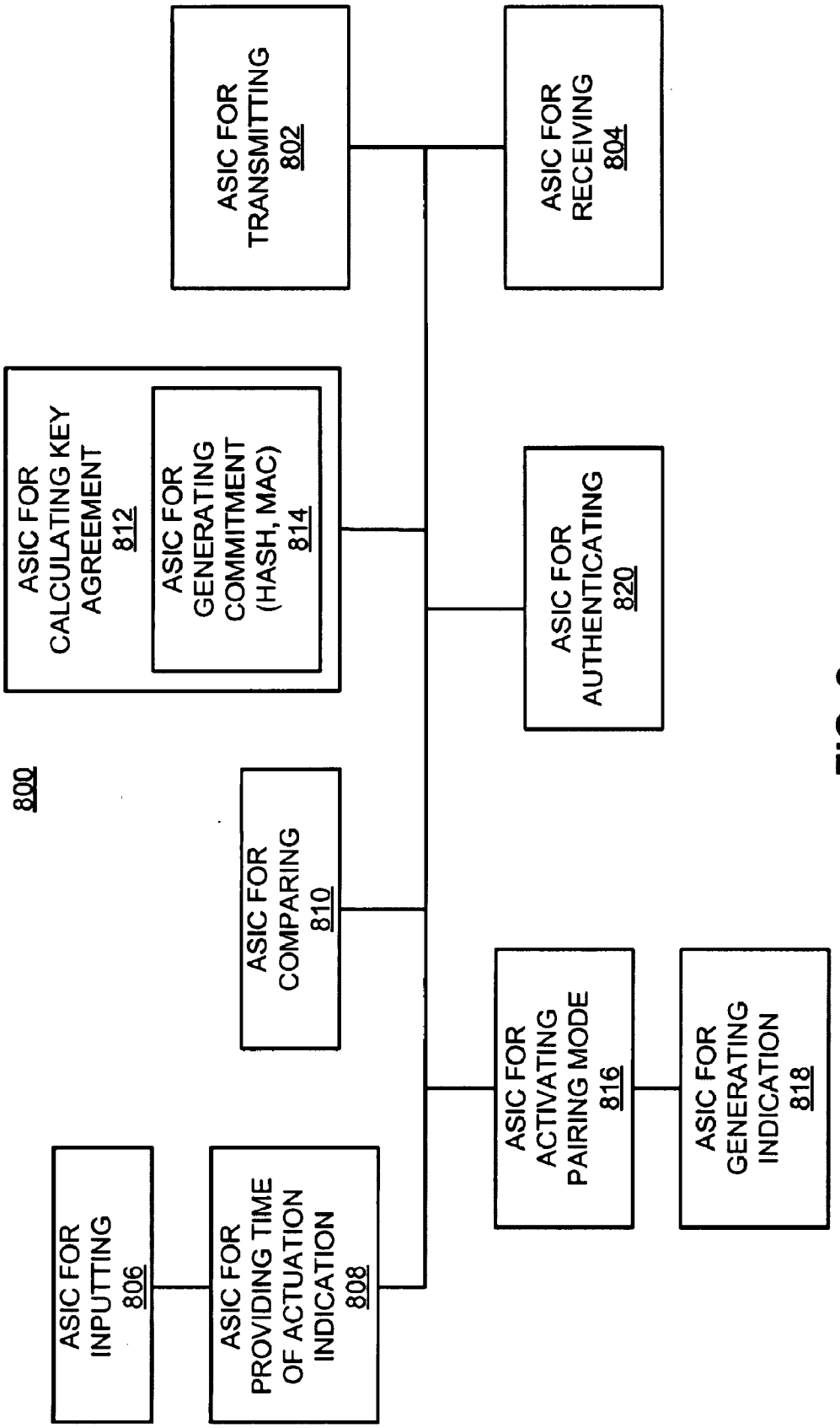

800
ASIC FOR TRANSMITTING 802
ASIC FOR RECEIVING 804
ASIC FOR CALCULATING KEY AGREEMENT 812
ASIC FOR GENERATING COMMITMENT (HASH, MAC) 814
ASIC FOR AUTHENTICATING 820
ASIC FOR COMPARING 810
ASIC FOR ACTIVATING PAIRING MODE 816
ASIC FOR GENERATING INDICATION 818
ASIC FOR INPUTTING 806
ASIC FOR PROVIDING TIME OF ACTUATION INDICATION 808

FIG. 8

SYNCHRONIZATION TEST FOR DEVICE AUTHENTICATION

CLAIM OF PRIORITY UNDER 35 U.S.C. §119

[0001] This application claims the benefit of and priority to commonly owned U.S. Provisional Patent Application No. 60/908,271, filed Mar. 27, 2007, and assigned Attorney Docket No. 061886P1, the disclosure of which is hereby incorporated by reference herein.

BACKGROUND

[0002] 1. Field

[0003] This application relates generally to wireless communication and more specifically, but not exclusively, to synchronization tests for device authentication.

[0004] 2. Background

[0005] Wireless devices may employ a pairing process in an attempt to form a level of trust with one another in conjunction with authenticating with each other or exchanging cryptographic keys that may be used for services that are protected by cryptographic techniques. For example, in Bluetooth, authentication between two devices may involve the exchange of a passcode between the devices. In some implementations such a procedure may involve the use of a sophisticated user interface for passcode input. Conversely, in implementations that employ relatively simple user interface devices for passcode input, the associated provisioning cost may be relatively high. Moreover, a typical passcode used by users may be four to eight digits long, which may not be strong enough to prevent the security of the devices from being compromised by conventional cryptanalysis.

[0006] Bluetooth V2.1 proposes using elliptic curve Diffie-Hellman for key exchange. Here, based on a secret derived from elliptic curve Diffie-Hellman, device authentication may be based on numeric comparison or passkey entry. However, these methods may utilize a sophisticated user interface and may be relatively susceptible to man-in-the-middle attacks.

[0007] Near field communication technology also may be used for device authentication. For example, near field communication devices may be designed to perform a handshake only when they are brought within a defined "touching" distance of each other. It may be possible, however, to design a near field communication device with a custom antenna that extends the working distance for the handshake. In this case, an unauthorized person or device may be able to authenticate with another device from relatively long range thereby thwarting the security otherwise provided the requirement of relatively close proximity of the devices. Consequently, authentication that is based on a relatively small touching distance as provided by near field communication may not provide a sufficient level of security.

SUMMARY

[0008] A summary of sample aspects of the disclosure follows. It should be understood that any reference to aspects herein may refer to one or more aspects of the disclosure.

[0009] The disclosure relates in some aspects authenticating devices or performing other similar operations based on the ability of a human to synchronize the movements of his or her fingers. For example, a person may be able to press or release two buttons in a simultaneous manner or in a substantially simultaneous manner. In contrast, it may be relatively difficult for an onlooker to anticipate and synchronize to the timings of the finger movements of the other person. Consequently, a pairing procedure for two wireless devices may involve a synchronization test that is based on the relative timing of actuations of input devices on each of the wireless devices. Here, it is unlikely that an onlooker would be able to press or release a button on his or her own wireless device in an attempt to interfere with the pairing of the wireless devices by the other person.

[0010] In some aspects, for purposes of device authentication, presence management, or other operations a pair of wireless devices may be deemed trustable with respect to one another if the same person is physically holding the two wireless devices. Consequently, when two wireless devices being held by the same person communicate with each other, a message sent by a first one of the wireless devices relating to a local synchronization event (e.g., actuation of a user input device) at the first device may be deemed trustable by a second one of the wireless devices that receives the message. To ensure that the same person is holding the devices, the receiving device verifies that the timing of the received message is substantially synchronized with a similar local synchronization event at the second device. Consequently, an authentication or other similar procedure may involve determining whether an input device on a first device is actuated (e.g., depressed and/or released) at substantially the same time or times that an input device on a second device is actuated.

[0011] The disclosure relates in some aspects to a synchronization test that involves determining whether actuations of user input devices on two different wireless devices occurred within a defined time interval with respect to one another. Here, a user may be instructed to simultaneously actuate a user input device on each wireless device. A first one of the wireless devices may determine the actuation time associated with a second one of the wireless devices based on the time at which the first device receives a message from the second device relating to the actuation of the second device. The first device may thus compare the actuation time of its user input device with the time it received the message from the second device. The second device may perform a similar synchronization test. In the event the synchronization tests pass on both devices, the devices may authenticate one another. In some aspects a cryptographic key agreement scheme may be employed in conjunction with the synchronization tests. In addition, in some aspects the synchronization tests may be based on the timings of more than one actuation of each user input device.

[0012] The disclosure relates in some aspects to a synchronization test that involves comparing time intervals between multiple actuations of user input devices on two different wireless devices. Here, a user may be instructed to simultaneously actuate a user input device on each wireless device in a repeated (e.g., random) manner. That is, the user may repeatedly actuate each user input device at the same time. In this way a set of time intervals corresponding to the times between actuations will be defined on each wireless device. Each of the devices may then send a commitment value (e.g., a hash code or a message authentication code) that is based on its set of time intervals to the other device. The description that follows describes the use of a hash value, a message authentication code or other schemes to illustrate sample ways to implement a commitment scheme. It should be appreciated that other cryptographic techniques may be used to

generate a commitment value in accordance with the teachings herein. As one step of the verification process, each of the devices may compare an actuation time of its user input device with the time it received the commitment (e.g., hash) message from the other device. Assuming this step of the verification process passes, after a delay period the devices may each send its set of time intervals to the other device. In this way, in another step of the verification process the devices may determine whether corresponding pairs of time intervals from each of the two sets of time intervals are sufficiently similar. In addition, in yet another step of the verification process, the devices may generate a commitment (e.g., hash) value based on the set of time intervals it received from the other device and compare that commitment value with the commitment value it previously received from the other device to verify that both received messages relate to the same set of time intervals. In the event the synchronization tests pass on both devices, the devices may authenticate one another.

BRIEF DESCRIPTION OF THE DRAWINGS

[0013] These and other aspects of the disclosure will be more fully understood when considered with respect to the following detailed description, appended claims, and accompanying drawings, wherein:

[0014] FIG. **1** is a simplified block diagram of several sample aspects of a communication system comprising wireless devices;

[0015] FIG. **2** is a flowchart of several sample aspects of operations that may be performed to authenticate two or more devices;

[0016] FIG. **3**, including FIGS. **3**A and **3**B, is a flowchart of several sample aspects of operations that may be performed to pair two wireless devices based on the time difference between an actuation of a user input device of each wireless device;

[0017] FIG. **4** is a simplified block diagram of several sample aspects of a wireless device;

[0018] FIG. **5**, including FIGS. **5**A and **5**B, is a flowchart of several sample aspects of operations that may be performed to pair two wireless devices based on differences between time durations defined by a series of actuations of a user input device of each wireless device;

[0019] FIG. **6** is a simplified diagram of sample timing relating to the operations of FIG. **5**;

[0020] FIG. **7** is a simplified block diagram of several sample aspects of communication components; and

[0021] FIG. **8** is a simplified block diagram of several sample aspects of an apparatus configured to support a synchronization test.

[0022] The various features illustrated in the drawings may not be drawn to scale and may be simplified for clarity. Consequently, the drawings may not depict every aspect of a particular apparatus (e.g., device) or method. In addition, similar reference numerals may be used to denote similar features herein.

DETAILED DESCRIPTION

[0023] Various aspects of the disclosure are described below. It should be apparent that the teachings herein may be embodied in a wide variety of forms and that any specific structure, function, or both being disclosed herein is merely representative. Based on the teachings herein one skilled in the art should appreciate that an aspect disclosed herein may be implemented independently of any other aspects and that two or more of these aspects may be combined in various ways. For example, an apparatus may be implemented or a method may be practiced using any number of the aspects set forth herein. In addition, such an apparatus may be implemented or such a method may be practiced using other structure, functionality, or structure and functionality in addition to or other than one or more of the aspects set forth herein. As an example of the above, as discussed below first and second actuation timing-related indications may be compared to determine whether at least one time of actuation of a first user input device is sufficiently similar to at least one time of actuation of a second user input device. In some aspects each of the at least one time of actuation of the first and second user input devices relates to a single time of actuation of each input device. In contrast, in some aspects each of the at least one time of actuation of the first and second user input devices relates to a set of time intervals defined by a series of actuations of each of the input devices.

[0024] FIG. **1** illustrates sample aspects of a communication system **100** where a first wireless device **102** may be paired with a second wireless device **104**. This pairing may be performed in conjunction with, for example, an authentication procedure relating to establishing communication between the devices **102** and **104**, a presence management operation that involves the devices **102** and **104**, or some other operation that involves an interaction between the devices **102** and **104** where the interaction is predicated on a determination that the other device is trustworthy. For convenience, FIG. **1** and the discussion that follows may generally refer to a pairing process between two wireless devices. It should be appreciated, however, that the teachings herein may be adaptable to creating trust between more than two devices and that such devices need not be wireless.

[0025] Sample operations of the system **100** will be discussed in more detail in conjunction with the flowchart of FIG. **2**. For convenience, the operations of FIG. **2** (or any other operations discussed or taught herein) may be described as being performed by specific components (e.g., system **100**). It should be appreciated, however, that these operations may be performed by other types of components and may be performed using a different number of components. It also should be appreciated that one or more of the operations described herein may not be employed in a given implementation.

[0026] As represented by block **202** of FIG. **2**, at some point in time a decision may be made to pair the devices **102** and **104**. As an example, a user may wish to use a wireless headset (e.g., device **104**) with his or her cell phone (e.g., device **102**). Here, it may be desirable to ensure that any communication between the headset and the cell phone remains private. Accordingly, in conjunction with the pairing operation the devices **102** and **104** may exchange one or more cryptographic keys that are then used to secure (e.g., encrypt) any messages sent between the devices **102** and **104**. Before exchanging such keys, however, each device **102** and **104** may wish to ensure that it is communicating with the intended device and not some other unauthorized device that may be attempting to compromise communication of either one or both of the devices **102** and **104**. Accordingly, in accordance with some aspects of the disclosure a pairing process based on one or more synchronization tests may be employed to enable

the devices **102** and **104** to verify whether they are indeed communicating with a trusted device.

[0027] In some aspects the pairing mode may be initiated through the use of user interfaces **106** and **108** of the devices **102** and **104**, respectively. For example, a user may actuate input devices **110** and **112** of the user interfaces **106** and **108**, respectively, to commence the pairing mode. In conjunction with these operations, the user interfaces **106** and **108** may respectively include output devices **114** and **116** that provide one or more indications relating to the progress of the pairing mode operations. As an example, once the devices **102** and **104** are ready to commence a synchronization test an appropriate indication may be generated by one or both of the output devices **114** and **116** to inform the user that he or she should simultaneously actuate the input devices **110** and **112**.

[0028] The user interfaces **106** and **108** may be implemented in a variety of ways. For example, in some implementations, each device **102** and **104** has a user input device (e.g., a button-type switch) and at least one of the devices **102** and **104** has a relatively simple user output device (e.g., a LED). As an example, a device **102** (e.g., a mobile phone) may have a keypad and a display screen that may serve as the user input device **110** and the user output device **114**, respectively. The device **104** may then simply employ a button or some other user input device **112** that the user may actuate in conjunction with the actuation of the keypad. In this case, an indication may be provided on the display screen to inform the user when to commence simultaneous actuation of the input devices **110** and **112**.

[0029] In general, a user input device may comprise one or more of a variety of components that enable a user to provide some form of input to an associated device. For example, the user input device may comprise one or more switches such as a pushbutton or a keypad. The user input device also may comprise a touch-screen, a touchpad, or other similar input mechanism. The user input device may comprise a pointing device such as a mouse, trackball, an electronic pen, a pointing stick, etc. The user input device also may be adapted to receive other forms of input such as an audio (e.g., voice) input, an optical-based input, an RF-based input, or some other suitable form of input.

[0030] As represented by block **204** of FIG. **2**, each of the devices **102** and **104** provide one or more indications relating to the timing of one or more actuations of its respective input device. For example, as will be discussed in more detail in conjunction with FIG. **3**, this indication may relate to the time at which an input device was actuated. Alternatively, as will be discussed in conjunction with FIG. **5**, this indication may relate to a set of time intervals defined by multiple actuations of an input device.

[0031] To enable each device to compare its actuation timing with the actuation timing of the other device, each of the devices may transmit one or more indications relating to its actuation timing to the other device. For example, upon actuation of the input device **110** a transceiver **118** (e.g., including transmitter and receiver components) of the device **102** may transmit a message to a similar transceiver **120** of the device **104** to indicate that the input device **110** has been actuated. In addition, the indication may include information relating to the timing of that actuation (e.g., the time of actuation or a set of time intervals defined by multiple actuations). As discussed below conjunction with FIG. **5**, the indication also may comprise a commitment value (e.g., a hash code or a message authentication code) that is based on a set of time intervals generated at block **204**.

[0032] As represented by block **206**, the device **104** (e.g., the transceiver **120**) may thus receive one or more indications from the device **102** relating to the timing of one or more actuations for the device **102**, and vice versa. As mentioned above, in some implementations the indication of block **206** may simply comprise the time at which a message was received from the other device.

[0033] As represented by block **208**, authentication processors **122** and **124** on each device may then compare one or more indications relating to its actuation timing with one or more received indications that relate to the actuation timing of the other device. For example, as discussed below conjunction with FIG. **3** the authentication processor **124** may use the time of receipt of the message from the device **102** as an indication of the time of actuation of the input device **110**. The authentication processor **124** may then compare that time of receipt with the time of actuation of its input device **112** to determine whether the actuations were sufficiently synchronized. Alternatively, as discussed below conjunction with FIG. **5** the authentication processor **124** may compare a received set of time intervals with its own set of time intervals and/or compare commitment (e.g., hash) values generated from these different sets of time intervals. In some implementations the above comparison operations may employ one or more time duration threshold values that define maximum allowable deviations between the timings of the indications of the two devices. Concurrently with the above operations, the authentication processor **122** may perform similar comparison operations for its indication(s) and the indication(s) that it receives from the device **104**.

[0034] As represented by block **210**, if the results above the above synchronization tests indicate that there is a sufficient probability that the input devices **110** and **112** were actuated by the same person, the devices **102** and **104** may complete the pairing process. For example, in some implementations the authentication processor **122** of the device **102** may authenticate the device **104**, and the authentication processor **124** of the device **104** may authenticate the device **102**. In conjunction with this operation or at some other point in time, the devices **102** and **104** may exchange or otherwise cooperate to create one or more cryptographic keys to facilitate secure communications between the devices or to facilitate some other form of device interaction.

[0035] In some implementations the synchronization test may be performed before the commencement of an authentication procedure (e.g., as a prerequisite to commencing an authentication procedure) or as part of an authentication procedure. In addition, in some implementations a synchronization test may serve as both a prerequisite to an authentication procedure and form a part of an authentication procedure.

[0036] With the above overview in mind, additional details relating to one type of synchronization test will be discussed in conjunction with the flowchart of FIG. **3**. In general, the blocks on the left side of FIG. **3** relate to operations that may be performed by a wireless device (e.g., device **102** of FIG. **1**) that initiates the pairing mode while the blocks on the right side of FIG. **3** relate to operations that may be performed by another wireless device (e.g., the device **104** of FIG. **1**) that responds to the initiation of the pairing mode. Here, it should be appreciated that the specific sequence of operations

depicted in FIG. **3** is for illustration purposes only, and that different circumstances may involve different sequences of operations.

[0037] For illustration purposes, the operations of FIG. **3** will be discussed in the context of being performed by various components of a wireless device **400** as shown in FIG. **4**. It should be appreciated, however, that the illustrated components of the wireless device **400** are merely representative of components that may be employed here and that one or more of the operations of FIG. **3** may be performed by or in conjunction with other suitable components.

[0038] In addition, for convenience the operations of both an initiator device and responder device will be discussed in conjunction with the single wireless device **400** depicted in FIG. **4**. Thus, while the discussion below will refer to similar components it should be understood that the initiator device and the responder device will comprise separate devices **400**.

[0039] At blocks **302** and **304** the two devices are set to pairing mode. In some implementations pairing mode may be initiated by a user using a user interface (e.g., interface **106** in FIG. **1**) to invoke the corresponding functionality on the device (e.g., device **102**). Here, an underlying protocol may enable each device to: (1) find its peer; and (2) determine which device is the initiator and which is the responder. The designations of initiator and responder may be determined in various ways. For example, in some implementations the responder is the device with a user interface (e.g., an LED). In some implementations the devices may each generate a random number whereby the device that generates, for example, the larger number is selected as the initiator.

[0040] In FIG. **4** the initiation of the pairing mode may be accomplished, for example, through the use of a pairing mode controller **402** that receives an input from an input device **404**, causes an appropriate indication to be provided on an output device **406** (if applicable), and transmits an appropriate indication to another device via a transmitter **408** (if applicable). For example, at least one of the initiator and responder devices may inform the user that it is in pairing mode (e.g., LED blinking). In some implementations pairing mode may simply be initiated by the user pressing the same user input devices (e.g., buttons) that are used for the synchronization operations. In other implementations a wireless device may support other techniques (e.g., menu selection) to enable pairing mode.

[0041] In some implementations similar operations may be performed here by the responding devices. Alternatively, one of the devices may simply be set to pairing mode upon reception of an appropriate message from the other device. In this case, a receiver **410** may receive the message from the other device and provide the associated information to the pairing mode controller **402** that invokes pairing mode operations on that device (e.g., device **104**).

[0042] The devices **102** and **104** may be in pairing mode for a designated period of time (e.g., for $T_{pair\_enabled}$ seconds). This time period may be defined large enough so that both devices may enter pairing mode without synchronization.

[0043] In some implementations the initiator device and/or the responder device may generate an indication to inform the user when to commence actuating the input devices of the initiator and responder devices. Such an indication may comprise, for example, a visual command on a display, a specific configuration of lighting elements (e.g., turning on or turning off LEDs), a vibration, or an audio command.

[0044] At block **306** the initiator device waits until its local input device (e.g., device **404**) has been actuated. As mentioned above, in some implementations this may involve a user pressing a button of the initiator device at the same time he or she presses a button on the responder device. Once the initiator device detect the local actuation event, at block **308** a timing indicator **412** and the transmitter **408** of the initiator device cooperate to transmit a pair-request message to the responder device. The receiver **410** of the responder device receives this pair-request message as represented by block **310**. As mentioned above, this time at which this message is received may serve as an indication as to the timing of the actuation at block **306**.

[0045] Similar to the initiator device operation of block **306**, at block **312** the responder device waits until its local input device (e.g., device **404**) has been actuated. In practice, the detection operation of block **312** may be made before or after the pair-request message is received at block **310**, depending on the relative timings of the actuations of the devices and the processing time for each device to identify an actuation and to process the pair-request message.

[0046] At block **314** a comparator **414** of the responder device compares the timing of the actuation of block **312** with the timing of the receipt of the request message at block **310**. The operation may involve, for example, determining the difference between these two timings and comparing the resulting difference with a threshold.

[0047] For example, assuming the button was pressed (block **312**) before the pair-request message was received, upon receipt of the pair-request message the comparator **414** may compare the current time t with the recorded timing of a button-pressing event at block **312**, denoted by $T_{resp\_button\_pressing}$. Thus, the synchronization test of blocks **314** and **316** may comprise determining whether: $|t-T_{resp\_button\_pressing}|<T_{max}$.

[0048] Here, T_{max} denotes the maximal allowable time interval between t and $T_{resp\_button\_pressing}$ when the two buttons are pressed by the same person. In some implementations T_{max} may be on the order of, for example, less than 0.1 seconds. Here, the message transmission delay may be ignored because it typically is much smaller than T_{max}. The button sensing delay may, in large part, be compensated at the other wireless device.

[0049] As represented by block **316**, if the synchronization test did not pass the responder device transmits a pair-deny message at block **318** to the initiator device. The operations of both devices may then go back to the beginning of the pairing process. In this case, there may be no change in the user interface (e.g., LED still blinking).

[0050] If, on the other hand, the synchronization test did pass at block **316**, the pairing process may continue. In some implementations the synchronization test involves multiple actuations by the user. For example, a subsequently detected actuation may involve the user releasing the buttons. Consequently, one or both of the devices may inform the user to keep holding the buttons (e.g., as indicated by maintaining the LED continuously ON). It should be appreciated here that similar functionality may be provided in other ways (e.g., by waiting for the local button to be pressed again).

[0051] At block **320** the responder device than waits for a defined period of time before performing the next operation (e.g., waiting for another actuation). Similarly, as represented by block **322**, the initiator device waits for the defined period of time after transmitting a message at block **308** before

performing its next operation (e.g., waiting for another actuation). Here, the defined period of time may comprise a fixed time T_{FIXED} plus a random time T_{RAND}.

[0052] At block **324** the responder device waits until its local button is released. Here, at the expiration of the time period of block **320**, the responder device may inform the user to simultaneously release the two buttons (e.g., LED blinking).

[0053] As represented by block **326**, once the local actuation is detected at block **324**, the responder device transmits a pair-acknowledgment message to the initiator device. Again, this operation may be performed by the cooperation of the timing indicator **412** and the transmitter **408** of the responder.

[0054] The receiver **410** of the initiator device receives this pair-acknowledgement message as represented by block **328**. The time at which this message is received may thus serve as an indication as to the timing of the actuation at block **324**.

[0055] As represented by block **330**, the initiator device waits until its local input device (e.g., device **404**) has again been actuated. As mentioned above, in some implementations this may involve the user releasing a button or performing some other suitable act. In practice, the detection operation of block **330** may occur before or after the pair-request message is received at block **328**.

[0056] At block **332** the comparator **414** of the initiator device compares the timing of the actuation of block **330** with the timing of the receipt of the acknowledgment message at block **328**. Again, this operation may involve determining the difference between these two timings and comparing the resulting difference with a threshold. For example, the initiator device may compare the current time t with the recorded time of, for example, the local button releasing event, denoted by $T_{init\_button\_releasing}$. The synchronization test at blocks **332** and **334** may thus involve determining whether: $|t-T_{init\_button\_releasing}|<T_{max}$.

[0057] As represented by block **334**, if the synchronization test did not pass, at block **336** the initiator device transmits a pair-deny message to the responder device. The pairing process may then be aborted.

[0058] If, on the other hand, the synchronization test did pass at block **334**, the cryptographic processor component **416** may optionally perform a key agreement calculation at block **338**. This operation may relate to, for example, providing one or more keys for use in subsequent operations of the initiator and responder devices.

[0059] At block **340** the initiator device may transmit a pair-confirm message to the responder device. In some implementations this message may include authentication-related information (e.g., that is used to generate a key to be used for subsequent secure operations). In the event this message is not received at the responder device the current pairing operation is aborted as represented by block **342**.

[0060] On the other hand, if the confirmation message is received a block **342**, the responding device may optionally perform its own key agreement calculation at block **344**. Here, the pair-request and pair-acknowledgement messages may have their own payloads. Consequently, a key to be used for securing subsequent operations may be generated from them. The key agreement scheme may be a Diffie-Hellman algorithm or any entropy mixing scheme (e.g., SHA-256 (payload1||payload2)). When a Diffie-Hellman algorithm is used, the payload may comprise the sender's public key information and the confidentiality of the exchange key is protected. For example, the pair-request message may include the initiator's public key and the pair-acknowledgement message may include the responder's public key.

[0061] As represented by blocks **346** and **348** the initiator and responder devices may then successfully terminate the pairing mode. Here, the responder device may inform the user of a successful pairing (e.g., the LED is continuously ON for a period of time, and is then turned OFF). An authenticator component **418** of each device may then perform any other operations that need to be performed in conjunction with authenticating these devices to one another.

[0062] It should be appreciated that various modifications may be made to one or more of the above operations. For example, holding the buttons may not be considered necessary, or multiple clicks of buttons may be used for additional assurance.

[0063] A number of advantages may be provided through the use of the above pairing operations. For example, if a hacker wants to launch a man-in-the-middle attack, the hacker has to send pair-request or pair-confirm synchronized with the two target devices. Since the two target devices are being physically held by their real owner, it is highly unlikely that the hacker can figure out the right timing to send these messages. That is, one person can click the buttons within a time limit that is much smaller than the normal human reaction time. Consequently, by the time an observer sees a button being pressed and tries to press the button on their intruding device, it will be too late.

[0064] A hacker also may mount an attack that involves sending a large number of fake pair-request or pair-confirm messages continuously with the intent that one of them is received within the legal time interval. To thwart such an attack, the receiver of the target device (either the initiator or the responder) may only record the first valid message from the other end and may reject (e.g., ignore or discard) the repeated messages of the same type. By doing so, only the first of these fake messages will be recorded. In this case, however, it is unlikely that this fake message will be received within the legal time interval. For example, the fake message would likely be received before actuation of a receiving device's input device.

[0065] Referring now to FIG. **5**, another type of synchronization test that is based on time intervals between actuations will be treated in detail. In a similar manner as above, the operations of FIG. **5** will be discussed in the context of the wireless device **400**. Again, it should be appreciated that the referenced components are merely representative and that the operations of FIG. **5** may be performed by or in conjunction with other suitable components.

[0066] FIG. **6** illustrates sample timing relationships between messages that may be transmitted between a pair of wireless device (e.g., devices **102** and **104**) in conjunction with, for example, the operations of FIG. **5**. Briefly, at blocks **602** and **604** these operations involve detection of a local button event by each device (designated device A and device B in FIG. **6**). In this case, the local button events at the devices A and B relate to a series of actuations that define a set of time intervals (designated $\Delta T_1-\Delta T_N$ and $\Delta T'_1-\Delta T'_N$, respectively). In this example, upon detection of the local button event, each device generates a message authentication code ("MAC") based on the corresponding set of time intervals and a cryptographic key K, and transmits the message authentication code to the other device as represented by the arrows **606** and **608**. Each of the devices A and B then waits for a defined period of time ($T\alpha$ and $T'\alpha$, respectively) to receive a message

from the other device. In the event the verification tests associated with these messages passes (as be discussed in more detail below in conjunction with FIG. **5**), device A and device B wait for another defined period of time (Tβ and T'β, respectively), then transmit messages relating to their respective set of time intervals as represented by the arrows **610** and **612**.

[0067] Sample operations that may be performed by wireless devices A and B will now be discussed in more detail in conjunction with FIG. **5**. Since the operations of these devices are complementary, FIG. **5** simply depicts the operations of one of the wireless devices.

[0068] At block **502** the wireless devices commence the pairing procedure. These operations may be similar to the pairing commencement operations discussed above in conjunction with blocks **302** and **304**.

[0069] At block **504** the wireless devices may exchange key information or otherwise cooperate to enable each wireless device to obtain one or more keys to be used in conjunction with the pairing operation. In some implementations the operations of block **504** are performed before the commencement of the pairing procedure. Here, the cryptographic processors **416** (FIG. **4**) of the devices may cooperate to generate a key K to be used to generate message authentication codes. In general, the devices determine the value K in a manner that ensures that no other device may establish an identical key with both of these devices.

[0070] One method of generating such a key is this is through the use of a Diffie-Hellman key agreement. As noted above, the key K used in the message authentication code is determined by both sides of the key exchange. Thus, a man-in-the-middle could try to set up this protocol separately with the two devices. However, when the Diffie-Hellman key exchange is used, it is relatively infeasible for the man-in-the-middle to establish the same key K for two separate processes. Here, replaying the same message authentication code between the two targets would fail.

[0071] To save manufacturing cost, the two devices may use ephemeral Diffie-Hellman keys to derive the key K. By doing so, each device may generate a Diffie-Hellman key pair when it boots up or each time before device authentication is required. Also, in devices with restricted memory and computation power, elliptic curve Diffie-Hellman may be used for key exchange.

[0072] To perform device authentication, or some other operation, the user again physically holds the two devices (e.g., one in each hand). The user then picks several random timings to simultaneously press and/or release a button on each device.

[0073] At block **506** the timing indicator **412** of each wireless device detects the series of actuations at its respective input device (e.g., device **404**) and defines a respective set of time intervals. Here, there are two sequences of timings, one recorded by device A: $(T_0, T_1, T_2, \ldots, T_N)$, and another recorded by device B: $(T'_0, T'_1, T'_2, \ldots, T'_N)$.

[0074] Two sequences of time differences may thus be computed from these series of timings for device A and device B, respectively: $(\Delta T_1, \Delta T_2, \ldots, \Delta T_N)$ and $(\Delta T'_1, \Delta T'_2, \ldots, \Delta T'_N)$, where $\Delta T_i = T_i - T_{i-1}$ and $\Delta T'_i = T'_i - T'_{i-1}$, where $(1 \leqq i \leqq N)$.

[0075] Each time interval in a set thus indicates the amount of time that elapsed between unique pairs of successive actuations. For example, the first time interval in a set may correspond to the elapsed time between the first actuation and the second actuation. The second time interval in a set may then correspond to the elapsed time between the second actuation and the third actuation.

[0076] Although the two devices may not have synchronized clocks, the two sequences of time differences should contain very similar values since these button events are triggered by two fingers that are well synchronized by a human being. Consequently, their difference $(\Delta T_i - \Delta T'_i)$ should be less than a threshold, ΔT_{th}.

[0077] At block **508** a commitment generator **420** (e.g., a hash or message authentication code generator) of each wireless device generates a commitment value (e.g., hash code or message authentication code) or performs some other suitable operation based that device's set of time intervals. For example, in some implementations the wireless device A generates a message authentication code based on $(\Delta T_1 \| \Delta T_2 \| \ldots \| \Delta T_N)$ and K while the wireless device B generates a message authentication code based on $(\Delta T'_1 \| \Delta T'_2 \| \ldots \| \Delta T'_N)$ and K. Here, "‖" denotes concatenation, and all time differences may be expressed as bit strings. It should be appreciated that in other implementations the time interval data may be manipulated in other ways (e.g., summed). In addition, it should be appreciated that the commitment generator **420** may implement other types of keyed hash algorithms including, for example, HMAC or may implement a block cipher in CBC-MAC or CMAC mode.

[0078] In some aspects, a commitment scheme may involve generating a commitment based on a "secret" such as the time intervals and, optionally, other data to be authenticated and providing the commitment to another device. The other device performs complementary operations. Here, it may be impossible or impractical for a device to determine the "secret" of the other device based on the received commitment. Thus, a given device may not use the other device's "secret" to generate its commitment. After the above exchange, a subsequent verification operation involves sending the "secret" (e.g., the time intervals) to the other device. In this way, each device may use the "secret" and the commitment it received to authenticate the other device.

[0079] In general, the operations of block **508** (and block **530** discussed below) relate to performing a cryptographic operation on the data to be transmitted. Consequently, similar functionality may be provided through the use of other cryptographic techniques such as a digital signature. Thus, in this case the commitment generator **420** may comprise a digital signature generator.

[0080] At block **510** each wireless device transmits its commitment (e.g., message authentication code) to the other wireless device. In some aspects this message comprises an indication relating to the timing of the actuations of block **506**. This transmission may be asynchronous with respect to the other wireless device. That is, the time at which one wireless device transmits its message authentication code may not be based on the time at which the other wireless device transmits its message authentication code.

[0081] As represented by block **512**, each device waits to receive a commitment (e.g., message authentication code) from the other device. For example, in the event the message authentication code is not received within a defined period of time the process may be aborted as represented by block **514** (e.g., and the process is restarted from button event detection). In some implementations the operations of block **512** involve the comparator **414** determining the time difference between a time relating to the actuation times (e.g., the last local button

event time T_N or T'_N) and the time of receipt of the incoming message authentication code at block **512**. In some aspects, this difference value must be less than a predefined threshold ΔT_α. The incoming message authentication code for device A may thus be deemed valid if: $(T_\alpha - T_N) < \Delta T_{\alpha\text{-}max}$. Similarly, the incoming message authentication code for device B may be deemed valid if: $(T'_\alpha - T'_N) < \Delta T_{\alpha\text{-}max}$.

[0082] As represented by block **516**, the process may be aborted in the event the two devices send identical commitments (e.g., message authentication codes) to each other. In this way, the pairing scheme prevents another device from simply transmitting back, for example, a message authentication code that it received from either device A or device B (e.g., in an attempted "replay attack").

[0083] If the incoming message authentication code is valid, at block **518** each device remains idle until more than a defined period of time (e.g., $\Delta T_{\beta\text{-}min}$) elapses after a designated time relating to the corresponding actuation times (e.g., the last local button event T_N or T'_N). Here, $\Delta T_{\beta\text{-}min}$ may be defined to be less than or equal to $\Delta T_{\alpha\text{-}max}$. Thus, for device A: $(T_\beta - T_N) > \Delta T_{\beta\text{-}min}$, and for device B: $(T'_\beta - T'_N) > \Delta T_{\beta\text{-}min}$.

[0084] The use of timing constraints as described above may prevent a man-in-the-middle attack where the attacker fails in authentication with one target but obtains the genuine sequence of time differences. In such a case, the attacker could try to use this sequence to authenticate to the other target. However, the man-in-the-middle will not pass the timing check for T_α and T_β because it is too late to send the correct message authentication code. That is, under the scheme set forth above a device will not transmit its set of time intervals (line **610** or **612** in FIG. **6**) until it receives a commitment such as the message authentication code (line **606** or **608** in FIG. **6**) from the other device.

[0085] At block **520** each wireless device transmits its set of time intervals to the other side for verification. As represented by block **522**, each wireless device thereby receives the corresponding set of time intervals from the other device. This message thus comprises an indication relating to the timing of the actuations of block **506**.

[0086] At block **524** the comparator **414** calculates the difference between corresponding time intervals of each set of time intervals. For example, the comparator **414** determines the difference in time between the first time interval in the set of intervals generated at device A and the first time interval in the set of intervals generated at device B. A similar time difference may then be calculated for each time interval in each set.

[0087] At block **526** the comparator **414** generates a verification count based on these time differences. As an example, the operations of blocks **524-528** may take the form of Equation 1.

$$\sum_{i=1}^{n} f(|\Delta T_i - \Delta T'_i|, \Delta T_{th}) \geq m \qquad \text{EQUATION 1}$$

where F(x, y) returns 1 if x<y and 0 if x≧y.

[0088] Here, the defined value m is the minimum number of successful tests that is deemed acceptable to pass the verification process (m≦n). In other words, this test determines whether an acceptable number of the time differences are within the range defined by ΔT_{th}. At block **528**, in the event an acceptable number of the time differences are not within the range defined by ΔT_{th}, the pairing process may be aborted.

[0089] On the other hand, if the synchronization test passed at block **528**, the wireless device may verify that a commitment (e.g., message authentication code) generated from the set of time intervals received at block **522** matches the commitment (e.g., message authentication code) received at block **512**. For example, at block **530** the message authentication code generator **420** may generate a message authentication code based on the set of time intervals received at block **522** and the key K. The comparator **414** may then compare this message authentication code with the message authentication code received from the other wireless device at block **512**. Exchanging the message authentication code at the beginning of the protocol (e.g., at blocks **510-512**) may thereby prevent either side from cheating. For example, once the message authentication code is transmitted, it may be infeasible to find another input message (e.g., sequence of time differences) with the same message authentication code.

[0090] At block **532**, if the commitment (e.g., message authentication code) based on the incoming message from block **522** does not match the commitment (e.g., message authentication code) from block **512**, the pairing process may be aborted. Otherwise, the other wireless device may be deemed successfully authenticated (block **534**).

[0091] Various advantages may be achieved through the use of the teachings herein. For example, in some aspects the techniques taught herein may be employed to prevent a malicious device from capturing finger movement timings through eavesdropping and analysis of wireless traffic during device pairing. In some aspects an implementation based on the teachings herein may not require complicated protocol or high cost device provisioning.

[0092] The use of the MAC associates the key K with the device authentication process. As a result, K is authenticated at block **534** as well. In other words, K may have been initially exchanged between devices that did not trust one another. By using K in the message authentication code, however, K is authenticated by the above distance-based authentication whereby trust derives from the same person operating the devices. Once authenticated, K may be used for subsequent cryptographic operations (e.g., encryption, authentication, and so on).

[0093] It should be appreciated that a commitment operation may be implemented in a variety of ways. For example, cryptographic operations other than MAC-based operations may be employed here. In addition, any of the operations taught herein may be used to associate additional data for authentication. Also, a pre-shared secret key K may not be required. For example, the commitment value can be the hash of (time intervals ||Diffie-Hellman public key ||device identifier) so that the Diffie-Hellman public key and the identifier of the other device are authenticated at block **534**. An advantage of such an approach is that a time consuming and computationally intensive key exchange (e.g., a Diffie-Hellman operation to provide K to each device) need not be performed until after the devices authenticate one another. Also, it should be appreciated that the commitment may be based on any type of data that needs to be authenticated. Thus, the above MAC operation may be based on other data in addition to or other than one or more of the pre-shared key K, the public key, and the device ID discussed above.

[0094] In some implementations a commitment scheme may employ encryption and decryption operations. For

example, the commitment scheme may involve using a key to encrypt a secret (e.g., time interval information). The resulting cipher text is transmitted to another device. Once the complementary cipher text is received from the other device, the key is transmitted to the other device. Each device may then use the key it receives to decrypt the received cipher text to thereby obtain the "secret" of the other device. This restored "secret" may then be compared with the received "secret" (e.g., the time intervals) to authenticate the other device.

[0095] In some implementations a commitment may be based on information that is provided to prevent a replay attack. For example, a first device may generate a MAC based on the time intervals and some type of information (referred to as a device identifier in the following discussion) that distinguishes the first device (e.g., an initiator) from a second device (e.g., a responder). The first device transmits the MAC to the second device that is expected to perform a complementary operation. After receiving a MAC from the other device, each device transmits its device identifier (e.g., "0" for the first device and "1" for the second device) in the clear. For example, the device identifier may be transmitted in the plain text of the MAC message (e.g., at block **510** in FIG. **5**) or along with the time interval information. Thus, if the second device attempts to "replay" the first device's MAC back to the first device, this will be apparent because the MAC from the second device will be based on the wrong device identifier (e.g., "0"). Similarly, in conjunction with the replay the second device may transmit the device identifier of the first device (e.g., "0") in the clear. In this case, the first device may readily determine that this is a replay upon checking the device identifier. Referring to FIG. **5**, the operation of block **516** (or some other block) may thus be replaced (or augmented) with checking the received device identifier to make sure that it is different than the device identifier of the device performing the check (e.g., the first device above).

[0096] The teachings herein may be incorporated into a device employing various components for communicating with at least one other device. FIG. **7** depicts several sample components that may be employed to facilitate communication between devices. Here, a first device **702** and a second device **704** are adapted to communicate via a wireless communication link **706** over a suitable medium.

[0097] Initially, components involved in sending information from the device **702** to the device **704** (e.g., a reverse link) will be treated. A transmit ("TX") data processor **708** receives traffic data (e.g., data packets) from a data buffer **710** or some other suitable component. The transmit data processor **708** processes (e.g., encodes, interleaves, and symbol maps) each data packet based on a selected coding and modulation scheme, and provides data symbols. In general, a data symbol is a modulation symbol for data, and a pilot symbol is a modulation symbol for a pilot (which is known a priori). A modulator **712** receives the data symbols, pilot symbols, and possibly signaling for the reverse link, and performs modulation (e.g., OFDM or some other suitable modulation) and/or other processing as specified by the system, and provides a stream of output chips. A transmitter ("TMTR") **714** processes (e.g., converts to analog, filters, amplifies, and frequency upconverts) the output chip stream and generates a modulated signal, which is then transmitted from an antenna **716**.

[0098] The modulated signals transmitted by the device **702** (along with signals from other devices in communication with the device **704**) are received by an antenna **718** of the device **704**. A receiver ("RCVR") **720** processes (e.g., conditions and digitizes) the received signal from the antenna **718** and provides received samples. A demodulator ("DEMOD") **722** processes (e.g., demodulates and detects) the received samples and provides detected data symbols, which may be a noisy estimate of the data symbols transmitted to the device **704** by the other device(s). A receive ("RX") data processor **724** processes (e.g., symbol demaps, deinterleaves, and decodes) the detected data symbols and provides decoded data associated with each transmitting device (e.g., device **702**).

[0099] Components involved in sending information from the device **704** to the device **702** (e.g., a forward link) will be now be treated. At the device **704**, traffic data is processed by a transmit ("TX") data processor **726** to generate data symbols. A modulator **728** receives the data symbols, pilot symbols, and signaling for the forward link, performs modulation (e.g., OFDM or some other suitable modulation) and/or other pertinent processing, and provides an output chip stream, which is further conditioned by a transmitter ("TMTR") **730** and transmitted from the antenna **718**. In some implementations signaling for the forward link may include power control commands and other information (e.g., relating to a communication channel) generated by a controller **732** for all devices (e.g. terminals) transmitting on the reverse link to the device **704**.

[0100] At the device **702**, the modulated signal transmitted by the device **704** is received by the antenna **716**, conditioned and digitized by a receiver ("RCVR") **734**, and processed by a demodulator ("DEMOD") **736** to obtain detected data symbols. A receive ("RX") data processor **738** processes the detected data symbols and provides decoded data for the device **702** and the forward link signaling. A controller **740** receives power control commands and other information to control data transmission and to control transmit power on the reverse link to the device **704**.

[0101] The controllers **740** and **732** direct various operations of the device **702** and the device **704**, respectively. For example, a controller may determine an appropriate filter, reporting information about the filter, and decode information using a filter. Data memories **742** and **744** may store program codes and data used by the controllers **740** and **732**, respectively.

[0102] FIG. **7** also illustrates that the communication components may include one or more components that perform operations relating to synchronization tests as taught herein. For example, a synchronization ("SYNC.") control component may cooperate with the controller **740** and/or other components of the device **702** to send/receive synchronization-related information to/from another device (e.g., device **704**). Similarly, a synchronization control component **748** may cooperate with the controller **732** and/or other components of the device **704** to send/receive synchronization-related information to/from another device (e.g., device **702**).

[0103] A wireless device may include various components that perform functions based on signals that are transmitted by or received at the wireless device. For example, a wireless headset may include a transducer adapted to provide an audio output based on a signal received via the receiver. A wireless watch may include a user interface adapted to provide an indication based on a signal received via the receiver. A wireless sensing device may include a sensor adapted to provide data to be transmitted to another device.

[0104] A wireless device may communicate via one or more wireless communication links that are based on or otherwise support any suitable wireless communication technology. For example, in some aspects a wireless device may associate with a network. In some aspects the network may comprise a body area network or a personal area network (e.g., an ultra-wideband network). In some aspects the network may comprise a local area network or a wide area network. A wireless device may support or otherwise use one or more of a variety of wireless communication technologies, protocols, or standards such as, for example, CDMA, TDMA, OFDM, OFDMA, WiMAX, and Wi-Fi. Similarly, a wireless device may support or otherwise use one or more of a variety of corresponding modulation or multiplexing schemes. A wireless device may thus include appropriate components (e.g., air interfaces) to establish and communicate via one or more wireless communication links using the above or other wireless communication technologies. For example, a device may comprise a wireless transceiver with associated transmitter and receiver components (e.g., transmitter **408** and receiver **410**) that may include various components (e.g., signal generators and signal processors) that facilitate communication over a wireless medium.

[0105] In some aspects a wireless device may communicate via an impulse-based wireless communication link. For example, an impulse-based wireless communication link may utilize ultra-wideband pulses that have a relatively short length (e.g., on the order of a few nanoseconds) and a relatively wide bandwidth. In some aspects the ultra-wideband pulses may have a fractional bandwidth on the order of approximately 20% or more and/or have a bandwidth on the order of approximately 500 MHz or more.

[0106] The teachings herein may be incorporated into (e.g., implemented within or performed by) a variety of apparatuses (e.g., devices). For example, one or more aspects taught herein may be incorporated into a phone (e.g., a cellular phone), a personal data assistant ("PDA"), an entertainment device (e.g., a music or video device), a headset (e.g., headphones, an earpiece, etc.), a microphone, a medical device (e.g., a biometric sensor, a heart rate monitor, a pedometer, an EKG device, etc.), a user I/O device (e.g., a watch, a remote control, a light switch, a keyboard, a mouse, etc.), a tire pressure monitor, a computer, a point-of-sale device, an entertainment device, a hearing aid, a set-top box, or any other suitable device.

[0107] These devices may have different power and data requirements. In some aspects, the teachings herein may be adapted for use in low power applications (e.g., through the use of an impulse-based signaling scheme and low duty cycle modes) and may support a variety of data rates including relatively high data rates (e.g., through the use of high-bandwidth pulses).

[0108] In some aspects a wireless device may comprise an access device (e.g., a Wi-Fi access point) for a communication system. Such an access device may provide, for example, connectivity to another network (e.g., a wide area network such as the Internet or a cellular network) via a wired or wireless communication link. Accordingly, the access device may enable another device (e.g., a Wi-Fi station) to access the other network or some other functionality. In addition, it should be appreciated that one or both of the devices may be portable or, in some cases, relatively non-portable.

[0109] The components described herein may be implemented in a variety of ways. Referring to FIG. **8**, an apparatus **800** is represented as a series of interrelated functional blocks that may represent functions implemented by, for example, one or more integrated circuits (e.g., an ASIC) or may be implemented in some other manner as taught herein. As discussed herein, an integrated circuit may include a processor, software, other components, or some combination thereof.

[0110] The apparatus **800** may include one or more modules that may perform one or more of the functions described above with regard to various figures. For example, an ASIC for transmitting **802** may correspond to, for example, a transmitter as discussed herein. An ASIC for receiving **804** may correspond to, for example, a receiver as discussed herein. An ASIC for inputting **806** may correspond to, for example, an input device as discussed herein. An ASIC for providing time of actuation indication **808** may correspond to, for example, a timing indicator as discussed herein. An ASIC for comparing **810** may correspond to, for example, a comparator as discussed herein. An ASIC for calculating key agreement **812** may correspond to, for example, a cryptographic processor as discussed herein. An ASIC for generating a commitment (hash, MAC) **814** may correspond to, for example, a commitment (e.g., hash/MAC) generator as discussed herein. An ASIC for activating pairing mode **816** may correspond to, for example, a pairing mode controller as discussed herein. An ASIC for generating indication **818** may correspond to, for example, an output device as discussed herein. An ASIC for authenticating **820** may correspond to, for example, an authenticator as discussed herein.

[0111] As noted above, in some aspects these components may be implemented via appropriate processor components. These processor components may in some aspects be implemented, at least in part, using structure as taught herein. In some aspects a processor may be adapted to implement a portion or all of the functionality of one or more of these components. In some aspects one or more of the components represented by dashed boxes are optional.

[0112] As noted above, the apparatus **800** may comprise one or more integrated circuits. For example, in some aspects a single integrated circuit may implement the functionality of one or more of the illustrated components, while in other aspects more than one integrated circuit may implement the functionality of one or more of the illustrated components.

[0113] In addition, the components and functions represented by FIG. **8** as well as other components and functions described herein, may be implemented using any suitable means. Such means also may be implemented, at least in part, using corresponding structure as taught herein. For example, the components described above in conjunction with the "ASIC for" components of FIG. **8** also may correspond to similarly designated "means for" functionality. Thus, in some aspects one or more of such means may be implemented using one or more of processor components, integrated circuits, or other suitable structure as taught herein.

[0114] Also, it should be understood that any reference to an element herein using a designation such as "first," "second," and so forth does not generally limit the quantity or order of those elements. Rather, these designations are used herein as a convenient method of distinguishing between two or more different devices, sets, etc. Thus, a reference to first and second devices or sets does not mean that only two devices or sets may be employed there or that the first device or set must precede the second device or set in some manner.

[0115] Those of skill in the art would understand that information and signals may be represented using any of a variety

of different technologies and techniques. For example, data, instructions, commands, information, signals, bits, symbols, and chips that may be referenced throughout the above description may be represented by voltages, currents, electromagnetic waves, magnetic fields or particles, optical fields or particles, or any combination thereof.

[0116] Those of skill would further appreciate that any of the various illustrative logical blocks, modules, processors, means, circuits, and algorithm steps described in connection with the aspects disclosed herein may be implemented as electronic hardware (e.g., a digital implementation, an analog implementation, or a combination of the two, which may be designed using source coding or some other technique), various forms of program or design code incorporating instructions (which may be referred to herein, for convenience, as "software" or a "software module"), or combinations of both. To clearly illustrate this interchangeability of hardware and software, various illustrative components, blocks, modules, circuits, and steps have been described above generally in terms of their functionality. Whether such functionality is implemented as hardware or software depends upon the particular application and design constraints imposed on the overall system. Skilled artisans may implement the described functionality in varying ways for each particular application, but such implementation decisions should not be interpreted as causing a departure from the scope of the present disclosure.

[0117] The various illustrative logical blocks, modules, and circuits described in connection with the aspects disclosed herein may be implemented within or performed by an integrated circuit ("IC"), an access terminal, or an access point. The IC may comprise a general purpose processor, a digital signal processor (DSP), an application specific integrated circuit (ASIC), a field programmable gate array (FPGA) or other programmable logic device, discrete gate or transistor logic, discrete hardware components, electrical components, optical components, mechanical components, or any combination thereof designed to perform the functions described herein, and may execute codes or instructions that reside within the IC, outside of the IC, or both. A general purpose processor may be a microprocessor, but in the alternative, the processor may be any conventional processor, controller, microcontroller, or state machine. A processor may also be implemented as a combination of computing devices, e.g., a combination of a DSP and a microprocessor, a plurality of microprocessors, one or more microprocessors in conjunction with a DSP core, or any other such configuration.

[0118] It is understood that any specific order or hierarchy of steps in any disclosed process is an example of a sample approach. Based upon design preferences, it is understood that the specific order or hierarchy of steps in the processes may be rearranged while remaining within the scope of the present disclosure. The accompanying method claims present elements of the various steps in a sample order, and are not meant to be limited to the specific order or hierarchy presented.

[0119] The steps of a method or algorithm described in connection with the aspects disclosed herein may be embodied directly in hardware, in a software module executed by a processor, or in a combination of the two. A software module (e.g., including executable instructions and related data) and other data may reside in a data memory such as RAM memory, flash memory, ROM memory, EPROM memory, EEPROM memory, registers, a hard disk, a removable disk, a CD-ROM, or any other form of computer-readable storage medium known in the art. A sample storage medium may be coupled to a machine such as, for example, a computer/processor (which may be referred to herein, for convenience, as a "processor") such the processor can read information (e.g., code) from and write information to the storage medium. A sample storage medium may be integral to the processor. The processor and the storage medium may reside in an ASIC. The ASIC may reside in user equipment. In the alternative, the processor and the storage medium may reside as discrete components in user equipment. Moreover, in some aspects any suitable computer-program product may comprise a computer-readable medium comprising codes (e.g., executable by at least one computer) relating to one or more of the aspects of the disclosure. In some aspects a computer program product may comprise packaging materials.

[0120] The previous description of the disclosed aspects is provided to enable any person skilled in the art to make or use the present disclosure. Various modifications to these aspects will be readily apparent to those skilled in the art, and the generic principles defined herein may be applied to other aspects without departing from the scope of the disclosure. Thus, the present disclosure is not intended to be limited to the aspects shown herein but is to be accorded the widest scope consistent with the principles and novel features disclosed herein.

What is claimed is:

1. A method of authenticating, comprising:

providing a first indication relating to at least one time of actuation of a first user input device that is associated with a first device;

receiving a second indication relating to at least one time of actuation of a second user input device that is associated with a second device;

comparing the first indication with the second indication to determine whether the at least one time of actuation of the first user input device is sufficiently similar to the at least one time of actuation of the second user input device; and

authenticating the second device based on the comparison.

2. The method of claim **1**, wherein:

the first indication indicates a time at which the first user input device was actuated; and

the second indication relates to a time at which the second user input device was actuated.

3. The method of claim **2**, wherein the second indication indicates a time at which a message from the second device was received at the first device.

4. The method of claim **2**, wherein:

the comparison comprises calculating a time difference between the time at which the first user input device was actuated and the time at which the second user input device was actuated; and

the authentication of the second device is based on whether the time difference is less than or equal to a threshold time interval.

5. The method of claim **4**, further comprising transmitting, if the time difference is less than or equal to the threshold time interval, a third indication relating to another time the first user input device was actuated.

6. The method of claim **4**, wherein:

the first indication indicates a time at which the first user input device was engaged; and

the third indication indicates a time at which the first user input device was disengaged.

7. The method of claim **4**, further comprising performing a key agreement calculation if the time difference is less than or equal to the threshold time interval, wherein the key agreement calculation is based on:

a first cryptographic key associated with the first device; and

a second cryptographic key associated with the second device and received in conjunction with the second indication.

8. The method of claim **7**, wherein the key agreement calculation provide a cryptographic key for securing communication between the first and second devices.

9. The method of claim **2**, wherein:

the first indication is provided and the second indication is received in conjunction with a synchronization test; and

the method further comprises rejecting, during the synchronization test and after the reception of the second indication, any indications purporting to be representative of at least one time of actuation of the second user input device.

10. The method of claim **1**, wherein:

the at least one time of actuation of the first user input device comprises a plurality of actuation times that define a first set of time intervals; and

the at least one time of actuation of the second user input device comprises a plurality of actuation times that define a second set of time intervals.

11. The method of claim **10**, wherein the comparison comprises:

calculating a series of time differences between each interval of the first set of time interval and a corresponding interval of the second set of time intervals; and

generating a verification count based on how many of the time differences are less than or equal to a threshold time interval.

12. The method of claim **11**, wherein the authentication of the second device is based on whether the verification count is greater than or equal to a threshold count.

13. The method of claim **10**, further comprising receiving a first commitment value that is based on the second set of time intervals.

14. The method of claim **13**, wherein the first commitment value comprises a hash code or a message authentication code.

15. The method of claim **13**, wherein the first commitment value is further based on data to be authenticated.

16. The method of claim **15**, wherein the data to be authenticated comprises at least one of the group consisting of: a pre-shared key, a public key, and a device identifier.

17. The method of claim **13**, wherein the first commitment value comprises a message authentication code that is further based on a cryptographic key that is shared by the first and second devices.

18. The method of claim **13**, further comprising:

generating a second commitment value based on the second set of time intervals;

wherein the authentication of the second device is based on whether the second commitment value equals the first commitment value.

19. The method of claim **13**, further comprising:

determining a time difference between a time of receipt of the first commitment value and a verification start time associated with the at least one time of actuation of the first user input device;

wherein the authentication of the second device is based on whether the time difference is less than or equal to a threshold time interval.

20. The method of claim **19**, further comprising transmitting, if the time difference is less than or equal to the threshold time interval, a third indication relating to the at least one time of actuation of the first user input device.

21. The method of claim **20**, wherein the third indication is transmitted a defined period of time after the verification start time.

22. The method of claim **13**, further comprising transmitting a commitment value relating to the first set of time intervals.

23. The method of claim **10**, wherein the authentication of the second device is based on the first set of time intervals being different than the second set of time intervals.

24. The method of claim **10**, wherein the actuation times that define the first set of time intervals comprise a random sequence of times.

25. The method of claim **1**, wherein each of the actuations comprises an engagement of a respective one of the user input devices or a disengagement of a respective one of the user input devices.

26. The method of claim **1**, wherein the first user input device comprises a pushbutton, a keypad, a switch, or a touchscreen.

27. The method of claim **1**, further comprising activating a pairing mode of the first device prior to acquiring the first indication.

28. The method of claim **1**, further comprising generating an indication to initiate the actuation of the user input devices.

29. The method of claim **28**, wherein the generation of the indication comprises activating or deactivating a lighting element or providing an output on a display screen.

30. An apparatus for authenticating, comprising:

a timing indicator configured to provide a first indication relating to at least one time of actuation of a first user input device that is associated with a first device;

a receiver configured to receive a second indication relating to at least one time of actuation of a second user input device that is associated with a second device;

a comparator configured to compare the first indication with the second indication to determine whether the at least one time of actuation of the first user input device is sufficiently similar to the at least one time of actuation of the second user input device; and

an authenticator configured to authenticate the second device based on the comparison.

31. The apparatus of claim **30**, wherein:

the first indication indicates a time at which the first user input device was actuated; and

the second indication relates to a time at which the second user input device was actuated.

32. The apparatus of claim **31**, wherein the second indication indicates a time at which a message from the second device was received at the first device.

33. The apparatus of claim **31**, wherein:

the comparator is further configured to calculate a time difference between the time at which the first user input

device was actuated and the time at which the second user input device was actuated; and

the authenticator is further configured to authenticate the second device based on whether the time difference is less than or equal to a threshold time interval.

34. The apparatus of claim **33**, further comprising a transmitter configured to transmit, based on whether the time difference is less than or equal to the threshold time interval, a third indication relating to another time the first user input device was actuated.

35. The apparatus of claim **33**, wherein:

the first indication indicates a time at which the first user input device was engaged; and

the third indication indicates a time at which the first user input device was disengaged.

36. The apparatus of claim **33**, further comprising a cryptographic processor configured to perform a key agreement calculation if the time difference is less than or equal to the threshold time interval, wherein the key agreement calculation is based on:

a first cryptographic key associated with the first device; and

a second cryptographic key associated with the second device and received in conjunction with the second indication.

37. The apparatus of claim **36**, wherein the key agreement calculation provide a cryptographic key for securing communication between the first and second devices.

38. The apparatus of claim **31**, wherein:

the first indication is provided and the second indication is received in conjunction with a synchronization test; and

the receiver is further configured to reject, during the synchronization test and after the receipt of the second indication, any indications purporting to be representative of at least one time of actuation of the second user input device.

39. The apparatus of claim **30**, wherein:

the at least one time of actuation of the first user input device comprises a plurality of actuation times that define a first set of time intervals; and

the at least one time of actuation of the second user input device comprises a plurality of actuation times that define a second set of time intervals.

40. The apparatus of claim **39**, wherein the comparator is further configured to:

calculate a series of time differences between each interval of the first set of time interval and a corresponding interval of the second set of time intervals; and

generate a verification count based on how many of the time differences are less than or equal to a threshold time interval.

41. The apparatus of claim **40**, wherein the authenticator is further configured to authenticate the second device based on whether the verification count is greater than or equal to a threshold count.

42. The apparatus of claim **39**, wherein the receiver is further configured to receive a first commitment value that is based on the second set of time intervals.

43. The apparatus of claim **42**, wherein the first commitment value comprises a hash code or a message authentication code.

44. The apparatus of claim **42**, wherein the first commitment value is further based on data to be authenticated.

45. The apparatus of claim **44**, wherein the data to be authenticated comprises at least one of the group consisting of: a pre-shared key, a public key, and a device identifier.

46. The apparatus of claim **42**, wherein the first commitment value comprises a message authentication code that is further based on a cryptographic key that is shared by the first and second devices.

47. The apparatus of claim **42**, further comprising:

a commitment generator configured to generate a second commitment value based on the second set of time intervals;

wherein the authenticator is further configured to authenticate the second device based on whether the second commitment value equals the first commitment value.

48. The apparatus of claim **42**, wherein:

the comparator is further configured to determine a time difference between a time of receipt of the first commitment value and a verification start time associated with the at least one time of actuation of the first user input device; and

the authenticator is further configured to authenticate the second device based on whether the time difference is less than or equal to a threshold time interval.

49. The apparatus of claim **48**, further comprising a transmitter configured to transmit, if the time difference is less than or equal to the threshold time interval, a third indication relating to the at least one time of actuation of the first user input device.

50. The apparatus of claim **49**, wherein the third indication is transmitted a defined period of time after the verification start time.

51. The apparatus of claim **42**, further comprising a transmitter configured to transmit a commitment value relating to the first set of time intervals.

52. The apparatus of claim **39**, wherein the authenticator is further configured to authenticate the second device based on the first set of time intervals being different than the second set of time intervals.

53. The apparatus of claim **39**, wherein the actuation times that define the first set of time intervals comprise a random sequence of times.

54. The apparatus of claim **30**, wherein each of the actuations comprises an engagement of a respective one of the user input devices or a disengagement of a respective one of the user input devices.

55. The apparatus of claim **30**, wherein the first user input device comprises a pushbutton, a keypad, a switch, or a touchscreen.

56. The apparatus of claim **30**, further comprising a pairing mode controller configured to activate a pairing mode of the first device prior to acquiring the first indication.

57. The apparatus of claim **30**, further comprising an output device configured to generate an indication to initiate the actuation of the user input devices.

58. The apparatus of claim **57**, wherein the output device is further configured to activate or deactivate a lighting element or provide an output on a display screen.

59. An apparatus for authenticating, comprising:

means for providing a first indication relating to at least one time of actuation of a first means for inputting that is associated with a first device;

means for receiving a second indication relating to at least one time of actuation of a second means for inputting that is associated with a second device;

means for comparing the first indication with the second indication to determine whether the at least one time of actuation of the first means for inputting is sufficiently similar to the at least one time of actuation of the second means for inputting; and

means for authenticating the second device based on the comparison.

60. The apparatus of claim **59**, wherein:

the first indication indicates a time at which the first means for inputting was actuated; and

the second indication relates to a time at which the second means for inputting was actuated.

61. The apparatus of claim **60**, wherein the second indication indicates a time at which a message from the second device was received at the first device.

62. The apparatus of claim **60**, wherein:

the means for comparing calculates a time difference between the time at which the first means for inputting was actuated and the time at which the second means for inputting was actuated; and

the means for authenticating authenticates the second device based on whether the time difference is less than or equal to a threshold time interval.

63. The apparatus of claim **62**, further comprising means for transmitting, based on whether the time difference is less than or equal to the threshold time interval, a third indication relating to another time the first means for inputting was actuated.

64. The apparatus of claim **62**, wherein:

the first indication indicates a time at which the first means for inputting was engaged; and

the third indication indicates a time at which the first means for inputting was disengaged.

65. The apparatus of claim **62**, further comprising means for performing a key agreement calculation if the time difference is less than or equal to the threshold time interval, wherein the key agreement calculation is based on:

a first cryptographic key associated with the first device; and

a second cryptographic key associated with the second device and received in conjunction with the second indication.

66. The apparatus of claim **65**, wherein the key agreement calculation provide a cryptographic key for securing communication between the first and second devices.

67. The apparatus of claim **60**, wherein:

the first indication is provided and the second indication is received in conjunction with a synchronization test; and

the means for receiving rejects, during the synchronization test and after the receipt of the second indication, any indications purporting to be representative of at least one time of actuation of the second means for inputting.

68. The apparatus of claim **59**, wherein:

the at least one time of actuation of the first means for inputting comprises a plurality of actuation times that define a first set of time intervals; and

the at least one time of actuation of the second means for inputting comprises a plurality of actuation times that define a second set of time intervals.

69. The apparatus of claim **68**, wherein the means for comparing:

calculates a series of time differences between each interval of the first set of time interval and a corresponding interval of the second set of time intervals; and

generates a verification count based on how many of the time differences are less than or equal to a threshold time interval.

70. The apparatus of claim **69**, wherein the means for authenticating authenticates the second device based on whether the verification count is greater than or equal to a threshold count.

71. The apparatus of claim **68**, wherein the means for receiving receives a first commitment value that is based on the second set of time intervals.

72. The apparatus of claim **71**, wherein the first commitment value comprises a hash code or a message authentication code.

73. The apparatus of claim **71**, wherein the first commitment value is further based on data to be authenticated.

74. The apparatus of claim **73**, wherein the data to be authenticated comprises at least one of the group consisting of: a pre-shared key, a public key, and a device identifier.

75. The apparatus of claim **71**, wherein the first commitment value comprises a message authentication code that is further based on a cryptographic key that is shared by the first and second devices.

76. The apparatus of claim **71**, further comprising:

means for generating a second commitment value based on the second set of time intervals;

wherein the means for authenticating authenticates the second device based on whether the second commitment value equals the first commitment value.

77. The apparatus of claim **71**, wherein:

the means for comparing determines a time difference between a time of receipt of the first commitment value and a verification start time associated with the at least one time of actuation of the first means for inputting; and

the means for authenticating authenticates the second device based on whether the time difference is less than or equal to a threshold time interval.

78. The apparatus of claim **77**, further means for transmitting, if the time difference is less than or equal to the threshold time interval, a third indication relating to the at least one time of actuation of the first means for inputting.

79. The apparatus of claim **78**, wherein the third indication is transmitted a defined period of time after the verification start time.

80. The apparatus of claim **71**, further comprising means for transmitting a commitment value relating to the first set of time intervals.

81. The apparatus of claim **68**, wherein the means for authenticating authenticates the second device based on the first set of time intervals being different than the second set of time intervals.

82. The apparatus of claim **68**, wherein the actuation times that define the first set of time intervals comprise a random sequence of times.

83. The apparatus of claim **59**, wherein each of the actuations comprises an engagement of a respective one of the first and second means for inputting or a disengagement of a respective one of the first and second means for inputting.

84. The apparatus of claim **59**, wherein the first means for inputting comprises a pushbutton, a keypad, a switch, or a touch-screen.

85. The apparatus of claim **59**, further comprising means for activating a pairing mode of the first device prior to acquiring the first indication.

86. The apparatus of claim **59**, further comprising means for generating an indication to initiate the actuation of the first and second means for inputting.

87. The apparatus of claim **86**, wherein the means for generating an indication activates or deactivates a lighting element or provides an output on a display screen.

88. A computer-program product for authenticating comprising:

computer-readable medium comprising codes executable by at least one computer to:

provide a first indication relating to at least one time of actuation of a first user input device that is associated with a first device;

receive a second indication relating to at least one time of actuation of a second user input device that is associated with a second device;

compare the first indication with the second indication to determine whether the at least one time of actuation of the first user input device is sufficiently similar to the at least one time of actuation of the second user input device; and

authenticate the second device based on the comparison.

89. A headset for wireless communication, comprising:

a timing indicator configured to provide a first indication relating to at least one time of actuation of a first user input device that is associated with a first device;

a receiver configured to receive a second indication relating to at least one time of actuation of a second user input device that is associated with a second device;

a comparator configured to compare the first indication with the second indication to determine whether the at least one time of actuation of the first user input device is sufficiently similar to the at least one time of actuation of the second user input device;

an authenticator configured to authenticate the second device based on the comparison; and

a transducer adapted to provide an audio output based on a signal received via the receiver.

90. A watch for wireless communication, comprising:

a timing indicator configured to provide a first indication relating to at least one time of actuation of a first user input device that is associated with a first device;

a receiver configured to receive a second indication relating to at least one time of actuation of a second user input device that is associated with a second device;

a comparator configured to compare the first indication with the second indication to determine whether the at least one time of actuation of the first user input device is sufficiently similar to the at least one time of actuation of the second user input device;

an authenticator configured to authenticate the second device based on the comparison; and

a user interface adapted to provide an indication based on a signal received via the receiver.

91. A sensing device for wireless communication, comprising:

a timing indicator configured to provide a first indication relating to at least one time of actuation of a first user input device that is associated with a first device;

a receiver configured to receive a second indication relating to at least one time of actuation of a second user input device that is associated with a second device;

a comparator configured to compare the first indication with the second indication to determine whether the at least one time of actuation of the first user input device is sufficiently similar to the at least one time of actuation of the second user input device;

an authenticator configured to authenticate the second device based on the comparison; and

a sensor adapted to provide data to be transmitted to the second device.

* * * * *