US 20070135092A1

(19) United States

(12) Patent Application Publication (10) Pub. No.: US 2007/0135092 A1

Pieronek et al. (43) Pub. Date: Jun. 14, 2007

(54) METHOD AND APPARATUS FOR AUTHENTICATING A MOBILE PHONE ACCESSORY

(76) Inventors: **James V. Pieronek**, San Diego, CA (US); **John P. Taylor**, San Diego, CA (US)

Correspondence Address:
KYOCERA WIRELESS CORP.
P.O. BOX 928289
SAN DIEGO, CA 92192-8289 (US)

(21) Appl. No.: 11/297,077

(22) Filed: Dec. 8, 2005

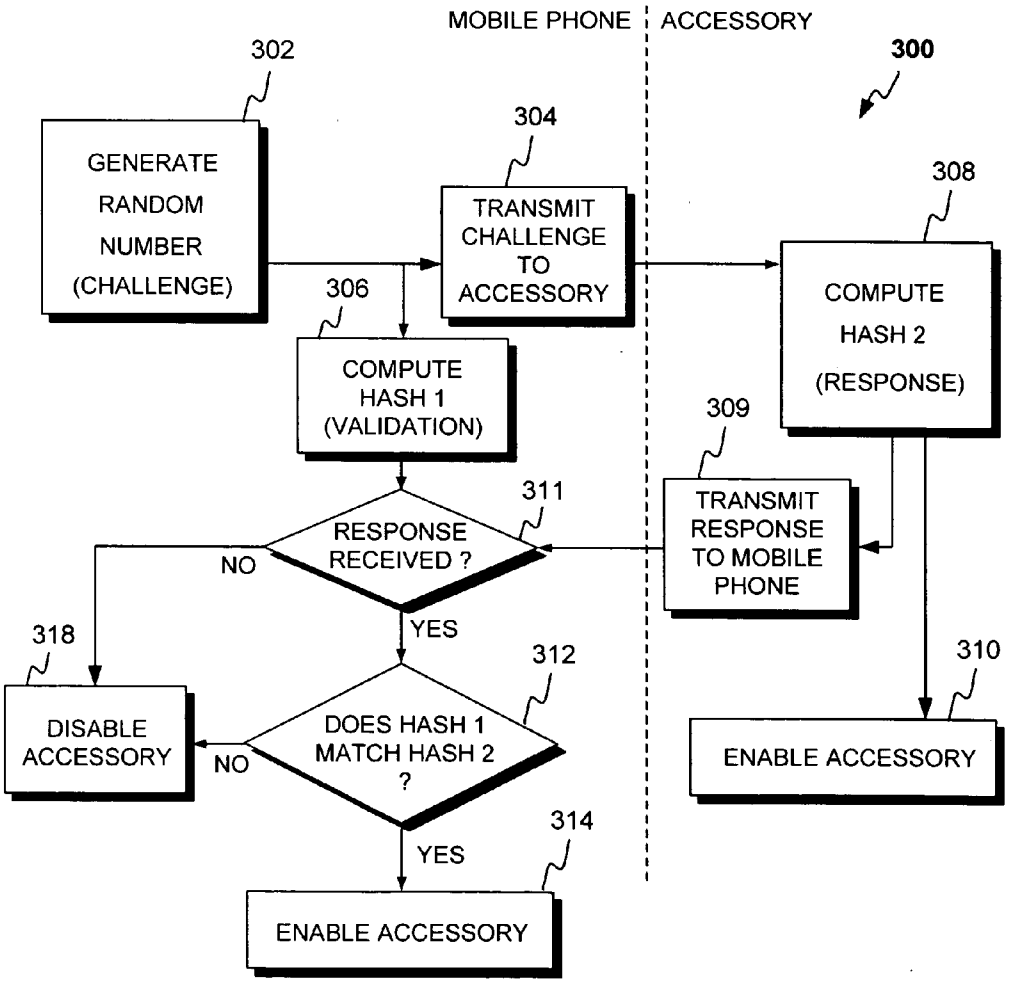
Publication Classification

(51) Int. Cl.
H04M 1/66 (2006.01)

(52) U.S. Cl. 455/411

(57) ABSTRACT

The mobile phone and the accessory communicate over a first line. The mobile phone computes or determines a challenge communication, and transmits the challenge communication over the first line to the accessory. The accessory receives the challenge communication, and computes a response communication based on the challenge communication, a hash algorithm and an electronic key. The response communication is transmitted over the first line to the mobile phone. The accessory also enables the phone accessory for use with the mobile phone. The response communication is received by the mobile phone. The mobile phone computes or determines a validation result based on the challenge communication, a hash algorithm and an electronic key. The mobile phone compares the response communication with the validation result, and enables the phone accessory for use with the mobile phone based on the comparison of the response communication with the validation result.



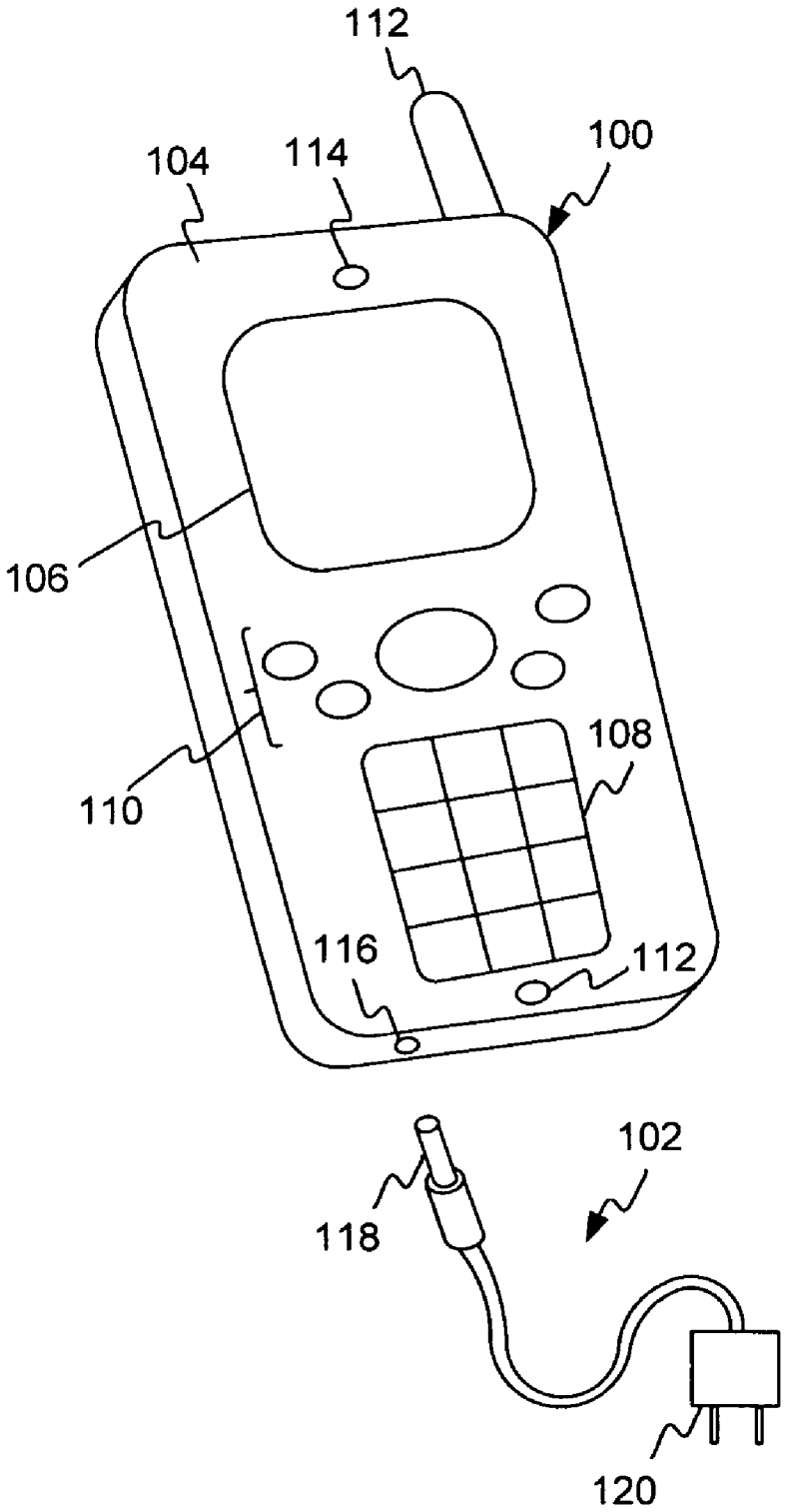


Fig. 1

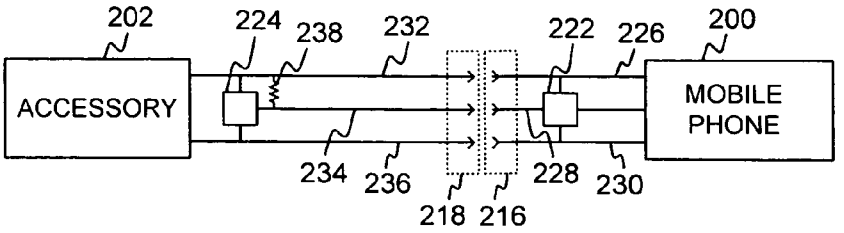

202
224
238
232
222
226
200
ACCESSORY
MOBILE PHONE
234
236
228
230
218
216

Fig. 2

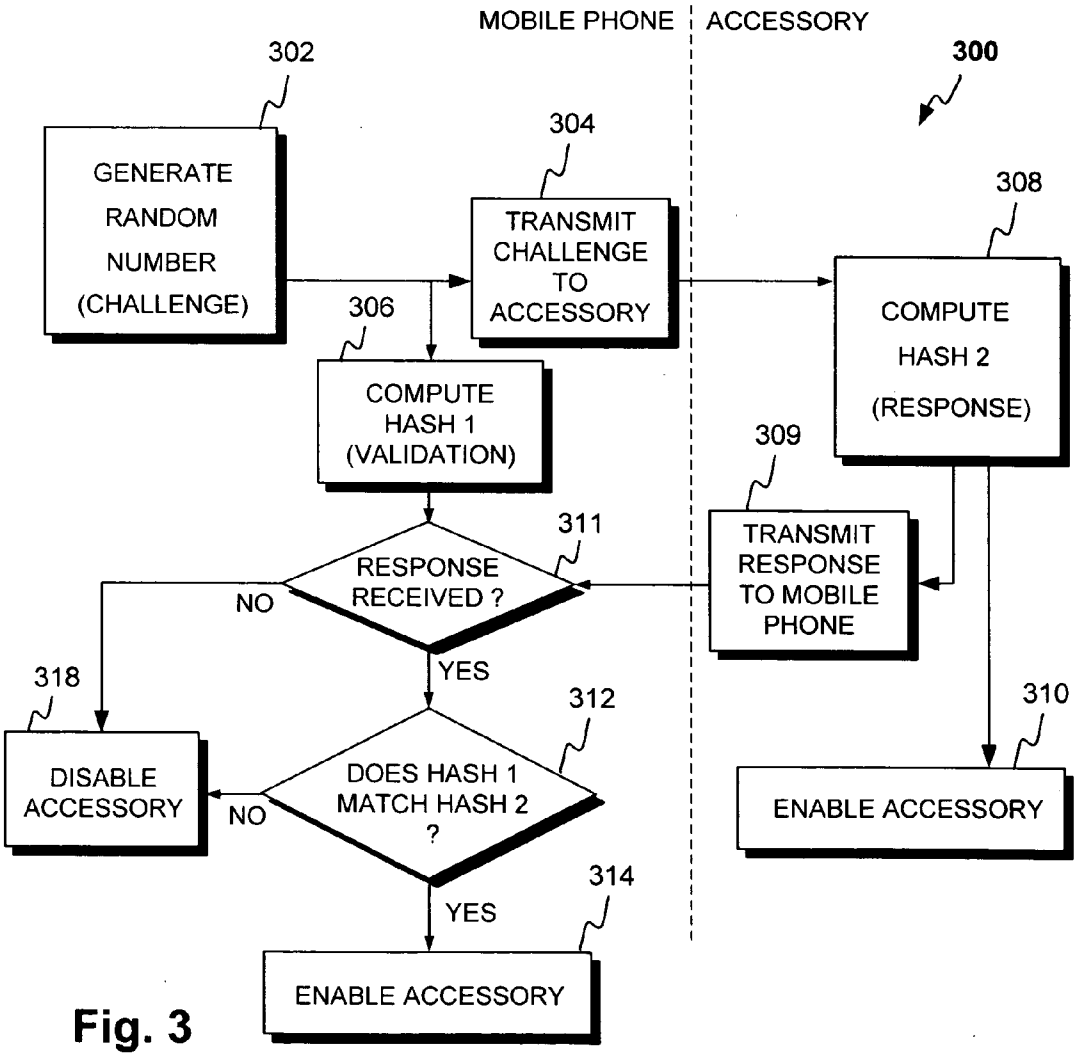

MOBILE PHONE
ACCESSORY
300
302
GENERATE RANDOM NUMBER (CHALLENGE)
304
TRANSMIT CHALLENGE TO ACCESSORY
308
COMPUTE HASH 2 (RESPONSE)
306
COMPUTE HASH 1 (VALIDATION)
309
TRANSMIT RESPONSE TO MOBILE PHONE
311
RESPONSE RECEIVED ?
NO
YES
318
DISABLE ACCESSORY
312
DOES HASH 1 MATCH HASH 2 ?
NO
310
ENABLE ACCESSORY
YES
314
ENABLE ACCESSORY

Fig. 3

METHOD AND APPARATUS FOR AUTHENTICATING A MOBILE PHONE ACCESSORY

FIELD OF THE INVENTION

[0001] The present invention relates to the field of wireless communication devices. More specifically, the invention relates to wireless communication device accessories and related methods of use.

BACKGROUND OF THE INVENTION

[0002] Various peripheral devices, generally referred herein to as "accessories," may be attached and detached from mobile phones, and other wireless communication devices. These accessories, when attached, provide additional functionality and/or otherwise enhance the performance of the phone. In other cases, accessories facilitate the user's ability to productively or comfortably use the mobile phone. A phone battery, though normally thought of as integral with a phone, is also considered an "accessory" for purposes of the present disclosure.

[0003] During the design and development of wireless communication devices, it is common to test the compatibility and/or reliability of accessories anticipated for use with the wireless communication device. Such testing ensures that an accessory will operate with a reasonable level of compatibility with the wireless communication device. Unfortunately, accessories made available by third parties for use with wireless communication devices are often not tested or, even if tested, fall below the standards defined by manufacturers of wireless communication devices and/or other standards, e.g., defined by government bodies. Such accessories (referred to herein as "unauthorized accessories") have the capability of damaging the wireless communication device and/or pose a safety threat to a consumer.

[0004] Existing techniques for preventing unauthorized accessories to be employed with wireless communication devices have been relatively easy to circumvent. For example, connectors employing unique mechanical keying arrangements can be overcome with mechanical modifications to the connectors. Electrical arrangements employing resistors for authentication are likewise easily circumvented with appropriate circuitry. Finally, digital communication techniques employing fixed passwords or rolling codes are relatively easy to defeat or mimic.

[0005] Accordingly, there remains a strong need in the art for an effective and secure authentication method and apparatus for wireless communication devices.

SUMMARY OF THE INVENTION

[0006] A method and apparatus for authenticating a mobile phone accessory is disclosed. According to one embodiment, the mobile phone and the accessory are capable of being coupled for communication over a first line via an interface.

[0007] In an exemplary embodiment, the mobile phone computes a challenge communication, such as a random number or pseudo random number, and transmits the challenge communication over the first line to the accessory. In response, the accessory receives the challenge communication over the first line, and computes a response communication based on the challenge communication, a hash algorithm and an electronic key. The response communication is transmitted over the first line to the mobile phone. In some embodiments, the accessory also optionally enables the phone accessory for use with the mobile phone, such as by making the requisite electrical connections, for example.

[0008] The response communication generated by the accessory is received by the mobile phone over the first line. The mobile phone computes a validation result based on the challenge communication, a hash algorithm and an electronic key. The mobile phone compares the response communication with the validation result, and enables the phone accessory for use with the mobile phone based on the comparison of the response communication with the validation result. In the case where the accessory is authorized for use with the mobile phone, the response communication generated by the accessory will match the validation result, and the accessory is enabled for use with the mobile phone. Otherwise, the accessory is not enabled for use with the mobile phone.

[0009] As discussed below, the particular mobile phone accessory authentication arrangement and technique disclosed herein result in significantly improved security, thereby significantly reducing the misuse of unauthorized accessories with mobile phones.

[0010] Other features and advantages of the present invention will become more readily apparent to those of ordinary skill in the art after reviewing the following detailed description and accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] FIG. **1** illustrates an exemplary mobile phone and accessory according to one embodiment of the present invention.

[0012] FIG. **2** illustrates an exemplary mobile phone and accessory according to one embodiment of the present invention.

[0013] FIG. **3** illustrates a flow chart depicting an exemplary method for authenticating a mobile phone accessory according to one embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

[0014] Referring first to FIG. **1**, there is shown mobile phone **100** and mobile phone accessory **102** capable of being connected to mobile phone **100** according to one embodiment of the invention. Mobile phone **100** may be any wireless F communication device capable of transmitting and receiving electromagnetic ("EM") energy in the radio frequency ("RF") band via an antenna coupled to the transceiver. Although the exemplary authentication method described herein is carried out by a mobile phone device for authenticating a mobile phone accessory, the method can also be used to authenticate battery packs or accessories for video cameras, notebook computers, ipods, and other electronic devices.

[0015] Although not shown in FIG. **1** for ease of illustration, mobile phone **100** typically includes a processor coupled to a memory enclosed within housing **104** for

carrying out a number of functions related to operating mobile phone **100**. The processor is further coupled to a transceiver for communication RF signals via antenna **112**. A power supply, such as a battery, supplies power to the processor, memory, transceiver, and other mobile phone **100** components.

[**0016**] Mobile phone **100** further includes a number of input/output ("I/O") devices for receiving and transmitting information to the user. For example, mobile phone **100** includes display **106**, keys **108** and **110**, microphone **112** and speaker **114**, each typically coupled to the processor via an appropriate I/O interface.

[**0017**] Continuing with FIG. **1**, mobile phone **100** further includes one or more accessory interfaces for connecting an accessory to the mobile phone **100**. Although the techniques described herein may be used with a wide variety of accessories and accessory interfaces, FIG. **1** illustrates an example arrangement involving power adapter accessory **102** having charging unit **120** connected to mobile phone interface **118**. The mobile phone interface **118** is capable of being connecting to accessory interface **116** of mobile phone **100**.

[**0018**] Referring now to FIG. **2**, there is shown a simplified block diagram illustrating mobile phone **200** connected to accessory **202** according to one embodiment of the invention. For example, mobile phone **200**, accessory interface **216**, accessory **202**, and mobile phone interface **218** in FIG. **2** may correspond to mobile phone **100**, accessory interface **116**, accessory **102**, and mobile phone interface **118**, respectively, in FIG. **1**.

[**0019**] As shown in FIG. **2**, accessory interface **216** of mobile phone **200** includes lines **226228** and **230**, and mobile phone interface **218** of accessory **202** includes lines **232**, **234** and **236**. By way of illustration, when mobile phone **200** and accessory **202** are connected, line **226** may be connected to line **232** for providing a supply voltage, line **230** may be connected to line **236** for providing a reference voltage, e.g., such as ground, and line **228** may be connected to line **234** for providing bi-directional communication between mobile phone **200** and accessory **202**.

[**0020**] According to another embodiment, signaling lines **228** and **234** may be omitted, and, thus, communication as described herein over lines **228** and **234** may be carried out over supply voltage lines **226** and **232**, respectively. For example, bi-directional signaling may be employed over lines **226** and **232** via modulation over lines **226** and **232**. As another example, bi-directional signaling may be employed over lines **226** and **232** by employing switches to enable lines **226** and **232** to operate in a first bi-directional signaling mode during the authentication process and to enable lines **226** and **232** to operate in a second voltage supplying mode after accessory **202** is authenticated. A benefit of enabling communication over existing supply voltage lines **226** and **232** is that dedicated communication lines **228** and **234** is not required, and thus, the interface and connectors between the mobile phone **200** and accessory **202** need not be modified from previous arrangements that do not employ the authentication method described herein.

[**0021**] Continuing with FIG. **2**, processor **222** of mobile phone **200** is connected to lines **226**, **228** and **230** of interface **216**, and processor **224** of accessory **202** is connected to lines **232**, **234** and **236**. Processor **222** may be the main processor of mobile phone **200** or may be an auxiliary processor within mobile phone **200**. Resistive element **238** is connected across lines **232** and **234** to provide an appropriate impedance to mobile phone **200**. The operations of processors **222** and **224** to authenticate accessory **202** will now be described in conjunction with FIG. **3**.

[**0022**] FIG. **3** depicts flowchart **300** illustrating a method for authenticating a mobile phone accessory according to one embodiment of the invention. Certain details and features have been left out of flow chart **300** of FIG. **3** that are apparent to a person of ordinary skill in the art. For example, a step may consist of one or more sub-steps, as known in the art. While steps **302** through **318** shown in flow chart **300** are sufficient to describe one embodiment of the present invention, other embodiments of the invention may utilize steps different from those shown in flow chart **300**.

[**0023**] According to one embodiment, the method of flow chart **300** is initiated when an accessory is connected to a mobile phone, e.g., when accessory **202** in FIG. **2** is connected to mobile phone **200**. At block **302**, processor **222** senses the connection of accessory **202** and generates a challenge communication. According to one embodiment, the challenge communication is a string of digits comprising a random number. For example, the challenge communication may be a 64-bit random number having more than 18 quintillion (18,000,000,000,000,000,000) possible values. The challenge response can also be a pseudo random number that may be unique for each mobile phone for each authenticating event. For example, the pseudo random number may be based on the mobile phone's electronic serial number ("ESN") and a counter incremented on every authentication attempt.

[**0024**] At block **304**, the challenge communication is transmitted from the mobile phone to the accessory for processing. For example, in FIG. **2**, the challenge communication is transmitted by processor **222** to processor **224** via lines **228** and **234**.

[**0025**] At block **306**, processor **222** of mobile phone **200** computes a first hash value ("Hash **1**") based on the challenge communication generated during block **302**. Hash **1** may be generated by a first hash algorithm employing a first electronic key, and further using the challenge communication as its input data. For example, the first hash algorithm may be a one-way hash algorithm. In general, for every unique input string, a different output string is produced. For purposes of the present disclosure, Hash **1** is referred to as a validation result, which is used to compare against a response communication generated by an accessory for authenticating the accessory, as discussed below.

[**0026**] At block **308**, processor **224** of accessory **202** receives the challenge communication transmitted during block **304** and computes a second hash value ("Hash **2**") based on the received challenge communication. Hash **2** is also known as a response communication, since Hash **2** is generated in response to the received challenge communication. Like Hash **1**, Hash **2** may be generated by a second hash algorithm employing a second electronic key, and further using the challenge communication as its input data. In a case where accessory **202** is authorized for use with mobile phone **200**, the second hash algorithm and/or the second electronic key would be supplied to the manufacturer of accessory **202** for storage in a memory used by processor

224 during the authentication process. As such, Hash 2, generated by the second hash algorithm and the second electronic key, can be authenticated by mobile phone 200, as discussed below. Unauthorized accessories, lacking either the second hash algorithm or the second electronic key would fail to generate the requisite Hash 2 for proper authentication, also discussed below.

[0027] At block 309, Hash 2 is transmitted by the mobile accessory to the mobile phone for processing. For example, in FIG. 2, the Hash 2 is transmitted by processor 224 to processor 222 via lines 234 and 228. As discussed below, authentication by mobile phone 200 is still required before accessory 202 is completely enabled for operation with mobile phone 200. Upon validating accessory 202, mobile phone 200 may allow certain portions of mobile phone 200 to communicate with or otherwise utilize accessory 202. Mobile phone 20 may command the accessory to change its configuration or connection (represented by block 310) or may cause the configuration to occur in mobile phone 20 (represented by block 314 as discussed below).

[0028] At decision block 311, a determination is made as to whether processor 222 has or has not received a response communication (Hash 2) from accessory 202. By way of illustration, Processor 222 will not receive a response communication where accessory 202 is not configured to transmit the response communication in response to the challenge communication transmitted during block 304. In such case, accessory 202 is considered unauthorized, and mobile phone 200 disables accessory 202 from operating with mobile phone 200 at step 318, as discussed below. If a response communication is received, method 300 continues to decision block 312.

[0029] At decision block 312, processor 222 has received the response communication (Hash 2) from processor 224 and compares Hash 1 generated during block 306 with Hash 2 received from accessory 202. In the case where accessory 202 is an authorized accessory, Hash 1 will match Hash 2, in which case processor 222 enables accessory 202 for operation with mobile phone 200 at step 314. As discussed above, upon validating accessory 202, mobile phone 200 may allow certain portions of mobile phone 200 to communicate with or otherwise utilize accessory 202. Mobile phone 20 may command the accessory to change its configuration or connection (represented by block 310) or may cause the configuration to occur in mobile phone 20 (represented by block 314 as discussed below). By way of illustration, enabling accessory 202 may involve, among other things, providing the requisite electrical connections, e.g., via lines 226 and 230 to mobile phone components of mobile phone 200. Accessory 202 is thereby authenticated and is enabled for use with mobile phone 200. In the case where accessory 202 is not an authorized accessory, Hash 1 will not match Hash 2, in which case processor 222 disables accessory 202 from operating with mobile phone 200 at step 318. For example, disabling accessory 202 can be carried out by preventing line 226 and/or line 230 of accessory interface 216 from connecting to respective mobile phone components of mobile phone 200.

[0030] When an accessory is disabled, a message may be communicated to the user, e.g., via a display message or audible message, to indicate that the accessory is not compatible with the mobile phone. Other appropriate messages may further include a warning that the accessory may damage the mobile phone.

[0031] Due to the particular arrangement and operation of mobile phone 200 and accessory 202, authentication of accessories for use with mobile phone 200 is significantly improved. For example, the hashing functions and the challenge and response technique employed in method 300 are extremely difficult and expensive to analyze and undermine. As a result, the ability for an unauthorized manufacturer of accessories to bypass the authentication arrangement of mobile phone 200 is significantly reduced. Benefits are realized by manufacturers of mobile phone 202, since use of unauthorized accessories which may damage mobile phone 202 is significantly reduced. In addition, users of the mobile phone 202 are benefited since the reduced likelihood for damage will result in reducing the loss of usage of the mobile phone during the repair period.

[0032] According to another embodiment of the invention, the processes associated with blocks 302 and 306 of method 300 depicted in FIG. 3 are replaced by one or more "challenge-response" pairs which are stored in memory on the mobile phone. According to this particular embodiment, the challenge communication need not be generated at block 302. Instead, the challenge component of a challenge-response pair is transmitted to the accessory at block 304. The accessory processes the challenge communication as discussed above in connection with block 308 of FIG. 3 and transmits the "Hash 2" response as discussed above in connection with block 309. According to this particular embodiment, the "Hash 1" validation result need not be generated at block 306. Instead the response component of the associated challenge-response pair (transmitted at block 304) may be used as the "Hash 1" validation result for comparison at block 312 as discussed above. Furthermore, according to this particular embodiment, each mobile phone will have unique or substantially unique challenge-response pair(s). By way of example, the unique or substantially unique challenge-response pair(s) may be provisioned when customers receive their product and are assigned an ESN. The benefit of this particular approach is that the encryption algorithm need not be stored on the mobile phone, where the algorithm could be illegitimately acquired for producing counterfeit accessories. Since the challenge-response pair(s) assigned to mobile phones are unique or substantially unique, even if a counterfeiter were to analyze the protocol of a particular mobile phone to mimic the response generated by an authorized accessory for authentication, the counterfeiter would be limited to making accessories for only that particular mobile phone, thereby rendering the ability of a counterfeiter to produce counterfeit accessories impractical.

[0033] From the above description of exemplary embodiments of the invention, it is manifest that various techniques can be used for implementing the concepts of the present invention without departing from its scope. Moreover, while the invention has been described with specific reference to certain embodiments, a person of ordinary skill in the art would recognize that changes could be made in form and detail without departing from the spirit and the scope of the invention. The described exemplary embodiments are to be considered in all respects as illustrative and not restrictive. It should also be understood that the invention is not limited

to the particular exemplary embodiments described herein, but is capable of many rearrangements, modifications, and substitutions without departing from the scope of the invention.

What is claimed is:

1. A method for authenticating a phone accessory, the phone accessory capable of being electrically connected to a mobile phone via a first line, the method comprising:

receiving a challenge communication over the first line;

computing a response communication based on the challenge communication, a hash algorithm and an electronic key;

transmitting the response communication over the first line;

enabling the phone accessory for use with the mobile phone.

2. The method of claim 1 wherein the phone accessory is enabled for use with the mobile phone over the first line.

3. The method of claim 2 wherein the first line is a supply voltage line.

4. The method of claim 1 wherein the phone accessory is enabled for use with the mobile phone over a second line, the second line electrically connecting the mobile phone and the phone accessory.

5. The method of claim 4 wherein the second line is a bi-directional communication line.

6. The method of claim 1 wherein the challenge communication is one of a random number and a pseudo random number.

7. A method for authenticating a phone accessory, the phone accessory capable of being electrically connected to a mobile phone via a first line, the method comprising:

computing a challenge communication;

transmitting the challenge communication over the first line;

receiving a response communication over the first line;

computing a validation result based on the challenge communication, a hash algorithm and an electronic key;

comparing the response communication with the validation result;

enabling the phone accessory for use with the mobile phone based on the comparing step.

8. The method of claim 7 wherein the phone accessory is enabled for use with the mobile phone over the first line.

9. The method of claim 8 wherein the first line is a supply voltage line.

10. The method of claim 7 wherein the phone accessory is enabled for use with the mobile phone over a second line, the second line electrically connecting the mobile phone and the phone accessory.

11. The method of claim 10 wherein the second line is a bi-directional communication line.

12. The method of claim 7 wherein the challenge communication is one of a random number and a pseudo random number.

13. The method of claim 7 further comprising disabling the phone accessory from use with the mobile phone if the response communication does not match the validation result.

14. The method of claim 7 further comprising disabling the phone accessory from use with the mobile phone if the response communication is not received during the receiving step.

15. A wireless accessory capable of being electrically connected to a mobile phone via a first line, the wireless accessory comprising:

a mobile phone interface including a first line;

a processor configured to:

receive a challenge communication over the first line;

calculate a response communication based on the challenge communication, a hash algorithm and an electronic key;

transmit the response communication over the first line; and

enable the phone accessory for use with the mobile phone.

16. The wireless accessory of claim 15 wherein the phone accessory is enabled for use with the mobile phone over the first line.

17. The wireless accessory of claim 16 wherein the first line is a supply voltage line.

18. The wireless accessory of claim 15 wherein mobile phone interface further includes a second line, the phone accessory being enabled for use with the mobile phone over the second line, the second line electrically connecting the mobile phone and the phone accessory.

19. The wireless accessory of claim 18 wherein the second line is a bi-directional communication line.

20. The wireless accessory of claim 15 wherein the challenge communication is one of a random number and a pseudo random number.

21. A mobile phone capable of being electrically connected to a phone accessory, the mobile phone comprising:

a first processor;

a transceiver coupled to the processor;

an antenna coupled to the transceiver;

a housing enclosing the first processor and the transceiver;

an accessory interface on the housing, the accessory interface including a first line;

a second processor communicably coupled to the first line, the second processor configured to:

compute a challenge communication;

transmit the challenge communication over the first line;

receive a response communication over the first line;

compute a validation result based on the challenge communication, a hash algorithm and an electronic key;

compare the response communication with the validation result;

enable the phone accessory for use with the mobile phone based on a comparison of the response communication with the validation result.

22. The mobile phone of claim 21 wherein the phone accessory is enabled for use with the mobile phone over the first line.

23. The mobile phone of claim 22 wherein the first line is a supply voltage line.

24. The mobile phone of claim 21 wherein **15** wherein accessory interface further includes a second line, the phone accessory is enabled for use with the mobile phone over the second line, the second line electrically connecting the mobile phone and the phone accessory.

25. The mobile phone of claim 24 wherein the second line is a bi-directional communication line.

26. The mobile phone of claim 21 wherein the challenge communication is one of a random number and a pseudo random number.

27. The mobile phone of claim 21 wherein the second processor is further configured to disable the phone accessory from use with the mobile phone if the response communication does not match the validation result.

28. The mobile phone of claim 21 wherein the second processor is further configured to disable the phone accessory from use with the mobile phone if the response communication is not received.

29. A method for authenticating a phone accessory, the phone accessory capable of being electrically connected to a mobile phone via a first line, the method comprising:

storing a substantially unique challenge-response pair in the mobile phone, the challenge-response pair including a challenge component and a response component;

transmitting the challenge component of the challenge-response pair as a challenge communication over the first line;

receiving a response communication over the first line;

comparing the response communication with the response component;

enabling the phone accessory for use with the mobile phone based on the comparing step.

30. The method of claim 27 wherein the phone accessory is enabled for use with the mobile phone over the first line.

31. The method of claim 28 wherein the first line is a supply voltage line.

32. The method of claim 27 wherein the phone accessory is enabled for use with the mobile phone over a second line, the second line electrically connecting the mobile phone and the phone accessory.

33. The method of claim 30 wherein the second line is a bi-directional communication line.

34. The method of claim 27 further comprising disabling the phone accessory from use with the mobile phone if the response communication does not match the response component.

35. The method of claim 27 further comprising disabling the phone accessory from use with the mobile phone if the response communication is not received during the receiving step.

* * * * *