



- (51) **International Patent Classification:**
H04L 9/08 (2006.01) *H04L 9/32* (2006.01)
- (21) **International Application Number:**
PCT/IB2016/000548
- (22) **International Filing Date:**
1 April 2016 (01.04.2016)
- (25) **Filing Language:** English
- (26) **Publication Language:** English
- (71) **Applicant:** INTEL CORPORATION [US/US]; 2200 Mission College Boulevard, Santa Clara, CA 95054 (US).
- (72) **Inventors:** AFANASYEVA, Alexandra; Trefoleva ul., 11, 40, 198097 Saint Petersburg (RU). BEZZATEEV, Sergey; 193318 Saint Petersburg (RU). PETROV, Vitaly; St. Orjonikidze, 16, 12, 196143 Saint Petersburg (RU). ZHIDANOV, Konstantin; Bukharetskaya St., 192238 Saint Petersburg (RU). VOLOSHINA, Natalia; Dunayskiy Pr., 58-1, 322, Saint Petersburg 192288 (RU). ZYBIN, Vladimir; 30, Turgeneva Street, Nizhny, 603024 Novgorod (RU). BAKUNOVA, Anna; Krylatsjaya, 17, 121614 Moscow (RU).

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

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

Published:

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

(54) **Title:** TECHNOLOGIES FOR MULTIFACTOR THRESHOLD AUTHENTICATION

700

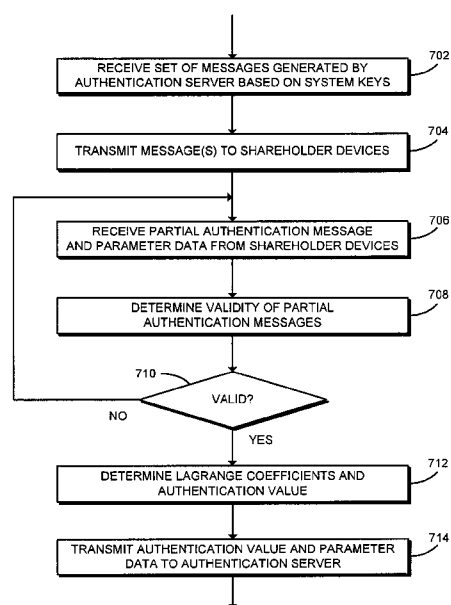


FIG. 7

(57) **Abstract:** Technologies for multifactor threshold authentication include a gateway device to receive, from an authentication server, a message generated by the authentication server based on a set of cryptographic system key. The gateway device transmits the message to a shareholder device receives a partial authentication message, parameter data and validation signature from the shareholder device. The parameter data is based on sensor data generated by the shareholder device and the partial authentication message is based on the parameter data and the message received from the authentication server. The gateway device determines whether the partial authentication message is valid using parameter data and validation signature. The gateway device then aggregates valid partial authentication messages from enough shareholder devices for the threshold scheme to form an authentication value which is sent to the authentication server.

TECHNOLOGIES FOR MULTIFACTOR THRESHOLD AUTHENTICATION

BACKGROUND

[0001] Authentication is a mechanism by which an entity proves that it is the entity it purports to be and is a critical component of many secure systems. For example, authentication systems may include user-level, device-level, and/or component-level authentication mechanisms and may vary in their complexity. For instance, some threshold-based authentication solutions deliver only binary authentication decisions by which basic credentials are provided. Various cryptographic techniques and tools may be employed to ensure data is securely transferred during an authentication procedure including, for example, Machine Authentication Codes (MACs), keyed hashes, cryptographic signatures, key certificates, and/or other suitable mechanisms depending on the particular embodiment and requirements of the system.

BRIEF DESCRIPTION OF THE DRAWINGS

[0002] The concepts described herein are illustrated by way of example and not by way of limitation in the accompanying figures. For simplicity and clarity of illustration, elements illustrated in the figures are not necessarily drawn to scale. Where considered appropriate, reference labels have been repeated among the figures to indicate corresponding or analogous elements.

[0003] FIG. 1 is a simplified block diagram of at least one embodiment of a system for multifactor threshold authentication;

[0004] FIG. 2 is a simplified block diagram of at least one embodiment of a shareholder device of the system of FIG. 1;

[0005] FIG. 3 is a simplified block diagram of at least one embodiment of an environment of the shareholder device of the system of FIG. 1;

[0006] FIG. 4 is a simplified block diagram of at least one embodiment of an environment of a gateway device of the system of FIG. 1;

[0007] FIG. 5 is a simplified block diagram of at least one embodiment of an environment of an authentication server of the system of FIG. 1;

[0008] FIG. 6 is a simplified flow diagram of at least one embodiment of a method for multifactor threshold authentication initialization that may be executed by the gateway device of FIG. 1;

[0009] FIG. 7 is a simplified flow diagram of at least one embodiment of a method for multifactor threshold authentication that may be executed by the gateway device of FIG. 1;

[0010] FIG. 8 is a simplified flow diagram of at least one embodiment of a method for multifactor threshold authentication that may be executed by the shareholder device of FIG. 1;

[0011] FIG. 9 is a simplified flow diagram of at least one embodiment of a method for multifactor threshold authentication that may be executed by the authentication device of FIG. 1;

[0012] FIG. 10 is a simplified data flow diagram of at least one embodiment of a method for multifactor threshold authentication initialization; and

[0013] FIG. 11 is a simplified data flow diagram of at least one embodiment of a method for multifactor threshold authentication.

DETAILED DESCRIPTION OF THE DRAWINGS

[0014] While the concepts of the present disclosure are susceptible to various modifications and alternative forms, specific embodiments thereof have been shown by way of example in the drawings and will be described herein in detail. It should be understood, however, that there is no intent to limit the concepts of the present disclosure to the particular forms disclosed, but on the contrary, the intention is to cover all modifications, equivalents, and alternatives consistent with the present disclosure and the appended claims.

[0015] References in the specification to “one embodiment,” “an embodiment,” “an illustrative embodiment,” etc., indicate that the embodiment described may include a particular feature, structure, or characteristic, but every embodiment may or may not necessarily include that particular feature, structure, or characteristic. Moreover, such phrases are not necessarily referring to the same embodiment. Further, when a particular feature, structure, or characteristic is described in connection with an embodiment, it is submitted that it is within the knowledge of one skilled in the art to effect such feature, structure, or characteristic in connection with other embodiments whether or not explicitly described. Additionally, it should be appreciated that items included in a list in the form of “at least one A, B, and C” can mean (A); (B); (C); (A and

B); (B and C); (A and C); or (A, B, and C). Similarly, items listed in the form of “at least one of A, B, or C” can mean (A); (B); (C); (A and B); (B and C); (A and C); or (A, B, and C).

[0016] The disclosed embodiments may be implemented, in some cases, in hardware, firmware, software, or any combination thereof. The disclosed embodiments may also be implemented as instructions carried by or stored on one or more transitory or non-transitory machine-readable (e.g., computer-readable) storage medium, which may be read and executed by one or more processors. A machine-readable storage medium may be embodied as any storage device, mechanism, or other physical structure for storing or transmitting information in a form readable by a machine (e.g., a volatile or non-volatile memory, a media disc, or other media device).

[0017] In the drawings, some structural or method features may be shown in specific arrangements and/or orderings. However, it should be appreciated that such specific arrangements and/or orderings may not be required. Rather, in some embodiments, such features may be arranged in a different manner and/or order than shown in the illustrative figures. Additionally, the inclusion of a structural or method feature in a particular figure is not meant to imply that such feature is required in all embodiments and, in some embodiments, may not be included or may be combined with other features.

[0018] Referring now to FIG. 1, a system 100 includes one or more shareholder devices 102, a gateway device 104, and an authentication server 106. Although only one gateway device 104 and one authentication server 106 are illustratively shown in FIG. 1, the system 100 may include any number of gateway devices 104 and/or authentication servers 106 in other embodiments. For example, in some embodiments, the same shareholder devices 102 may communicate with multiple different gateway devices 104 (e.g., for different purposes). Further, in some embodiments, one of the shareholder devices 102 may be selected or designated as the gateway device 104.

[0019] As described in detail below, in the illustrative embodiment, the gateway device 104 initializes the system 100 (e.g., the shareholder device 102 and the authentication server 106) with the relevant cryptographic keys, parameters, and/or other relevant data for multifactor threshold authentication. As such, the authentication server 106 may transmit a request for authentication data of the shareholder devices 102 to the gateway device 104 for forwarding to the shareholder devices 102. In the illustrative embodiment, the shareholder devices 102

generate parameter data based on generated sensor data (e.g., biometric parameters) and a partial authentication message based on the parameter data and one or more messages received from the gateway device 104. The gateway device 104 may authenticate the data received from the shareholder devices 102 and transmit valid responses to the authentication server 106 for further authentication.

[0020] It should be appreciated that the techniques described herein allow for a multifactor threshold authentication scheme. For instance, in some embodiments, if the user provides only basic credentials, limited access rights may be granted (e.g., limited amount for an e-commerce transaction or restricted access to certain data). However, in such embodiments, if the user presents additional information from one or more shareholder devices to confirm, for example, the user's identity (e.g., fingerprint scanner, heart rate monitor, and/or other biometric sensors/processors), broader access rights (e.g., full access) may be granted. Of course, the threshold(s) for additional information and corresponding access rights may vary depending on the particular embodiment. For example, the system 100 may include multiple "levels" of access and, therefore, may have different threshold requirements. After receiving the correct basic credentials and additional data regarding the user, the authentication server 106 may make more informed and/or accurate decisions regarding whether to grant or deny access. In particular, in some embodiments, the authentication server 106 may evaluate the risk level of granted or denying access to a particular user (e.g., to a particular collection of shareholder devices 102). For example, in some embodiments, the authentication server 106 may determine the financial risks of access by the user to a particular organization based on a combination of probabilities of false negatives (e.g., refusing service/access to a valid user) and false positives (e.g., granting access to a possible attacker). In other words, in some embodiments, the system 100 may seamlessly integrate a risks analysis function into the authentication process.

[0021] In the illustrative embodiment, each of the shareholder devices 102 is embodied as a wearable computing device. As described below, in the illustrative embodiment, the shareholder devices 102 hold a "shadow" of the user's secret cryptographic key and may reply to authentication requests received from the gateway device 104 in a way that the authentication server 106 can verify the device identity but is unable to obtain the shadow of the user's secret cryptographic key. Further, the gateway device 104 may be embodied as a wearable or handheld computing device (e.g., smartphone, smart watch, etc.) and may be responsible for receiving

authentication requests from the authentication server 106, forwarding the requests to the shareholder devices 102, collecting the responses of the shareholder devices 102, and combining and delivering the responses to the authentication server 106. Although the shareholder devices 102 and the gateway device 104 are described herein as wearable computing device and/or wearable/handheld computing devices, in other embodiments, it should be appreciated that each of the shareholder devices 102 and/or the gateway device 104 may be embodied as any type of computing device capable of performing the functions described herein. For example, each of the shareholder devices 102 and/or the gateway device 104 may be embodied as a wearable computing device, smartphone, cellular phone, personal digital assistant, mobile Internet device, tablet computer, netbook, notebook, Ultrabook™, laptop computer, and/or any other computing/communication device. In the illustrative embodiment, the authentication server 106 acts as a verifying entity/terminal (e.g., an enterprise- or organization-side device/system) responsible for sending authentication requests, receiving replies from the shareholder devices 102 (e.g., the user's wearable computing devices) through the gateway device 104, and determining whether the provided credentials are sufficient enough for authentication (e.g., to permit access).

[0022] Referring now to FIG. 2, the illustrative shareholder device 102 includes a processor 210, an input/output ("I/O") subsystem 212, a memory 214, a data storage 216, a communication circuitry 218, and one or more sensors 120. Of course, the shareholder device 102 may include other or additional components, such as those commonly found in a typical computing device (e.g., various input/output devices and/or other components), in other embodiments. Additionally, in some embodiments, one or more of the illustrative components may be incorporated in, or otherwise form a portion of, another component. For example, the memory 214, or portions thereof, may be incorporated in the processor 210 in some embodiments.

[0023] The processor 210 may be embodied as any type of processor capable of performing the functions described herein. For example, the processor 210 may be embodied as a single or multi-core processor(s), digital signal processor, microcontroller, or other processor or processing/controlling circuit. Similarly, the memory 214 may be embodied as any type of volatile or non-volatile memory or data storage capable of performing the functions described herein. In operation, the memory 214 may store various data and software used during operation

of the shareholder device 102 such as operating systems, applications, programs, libraries, and drivers. The memory 214 is communicatively coupled to the processor 210 via the I/O subsystem 212, which may be embodied as circuitry and/or components to facilitate input/output operations with the processor 210, the memory 214, and other components of the shareholder device 102. For example, the I/O subsystem 212 may be embodied as, or otherwise include, memory controller hubs, input/output control hubs, firmware devices, communication links (i.e., point-to-point links, bus links, wires, cables, light guides, printed circuit board traces, etc.) and/or other components and subsystems to facilitate the input/output operations. In some embodiments, the I/O subsystem 212 may form a portion of a system-on-a-chip (SoC) and be incorporated, along with the processor 210, the memory 214, and other components of the shareholder device 102, on a single integrated circuit chip.

[0024] The data storage 216 may be embodied as any type of device or devices configured for short-term or long-term storage of data such as, for example, memory devices and circuits, memory cards, hard disk drives, solid-state drives, or other data storage devices. The data storage 216 and/or the memory 214 may store various data during operation of the shareholder device 102 as described herein.

[0025] The communication circuitry 218 may be embodied as any communication circuit, device, or collection thereof, capable of enabling communications between the shareholder device 102 and other remote devices (e.g., the gateway device 104) over a network (not shown). The communication circuitry 218 may be configured to use any one or more communication technologies (e.g., wireless or wired communications) and associated protocols (e.g., Ethernet, Bluetooth®, Wi-Fi®, WiMAX, LTE, 5G, etc.) to effect such communication.

[0026] The sensors 220 may be embodied as any sensors configured to generate data/signals indicative of an environment or context of the corresponding shareholder device 102 and/or a user of the corresponding shareholder device 102. For example, in some embodiments, the sensors 220 may be configured to generate data indicative of biometric parameters of the user of the shareholder device 102 (e.g., heart rate, blood pressure, temperature, etc.), data indicative of the location of the shareholder device 102 (e.g., absolute location or location relative to another reference point such as the user), and/or data indicative of inertial characteristics or dynamic interaction patterns (speed, acceleration, direction of movement, tactile patterns, etc.). Of course, the sensors 220 may additionally, or alternatively, generate data indicative of other

environment or contextual characteristics in other embodiments. As such, in various embodiments, the sensors 220 may be embodied as, or otherwise include, for example, inertial sensors, temporal sensors (e.g., clocks), pressure sensors, position sensors, location sensors, proximity sensors, optical sensors, light sensors, audio sensors, temperature sensors, motion sensors, piezoelectric sensors, cameras, and/or other types of sensors. Of course, the shareholder device 102 may also include components and/or devices configured to facilitate the user of the sensor(s) 220. Depending on the particular embodiment, the sensors 220 may include hardware sensors and/or software sensors (e.g., software sensors to identify software applications executed at a particular point in time).

[0027] The authentication server 106 may be embodied as any type of computing device capable of performing the functions described herein. For example, in some embodiments, the authentication server 106 may be embodied as a server, rack-mounted server, blade server, desktop computer, laptop computer, tablet computer, notebook, netbook, Ultrabook™, cellular phone, smartphone, personal digital assistant, mobile Internet device, wearable computing device, Hybrid device, and/or any other computing/communication device.

[0028] It should be appreciated that the gateway device 104 and/or the authentication server 106 may include components similar to those of the shareholder device 102 discussed above. The description of those components of the shareholder device 102 is equally applicable to the description of components of the gateway device 104 and the authentication server 106 and is not repeated herein for clarity of the description. Further, it should be appreciated that the gateway device 104 and/or the authentication server 106 may include other components, sub-components, and devices commonly found in a computing device, which are not discussed above in reference to the shareholder device 102 and not discussed herein for clarity of the description. Additionally, in some embodiments, one or more of the components of the shareholder device 102 may be omitted from the gateway device 104 and/or the authentication server 106 (e.g., the sensors 220).

[0029] Referring now to FIG. 3, in use, one or more of (e.g., each of) the shareholder devices 102 establishes an environment 300 for multifactor threshold authentication. The illustrative environment 300 includes a cryptography module 302, a communication module 304, a key share module 306, and a sensor management module 308. The various modules of the environment 300 may be embodied as hardware, software, firmware, or a combination thereof.

For example, the various modules, logic, and other components of the environment 300 may form a portion of, or otherwise be established by, the processor 210, the I/O subsystem 212, and/or other hardware components of the shareholder device 102. As such, in some embodiments, one or more of the modules of the environment 300 may be embodied as circuitry or collection of electrical devices (e.g., a cryptography circuitry, a communication circuitry, a key share circuitry, and/or a sensor management circuitry). Additionally, in some embodiments, one or more of the illustrative modules may form a portion of another module and/or one or more of the illustrative modules may be independent of one another. Further, in some embodiments, one or more of the modules of the environment 300 may be embodied as virtualized hardware components or emulated architecture, which may be established and maintained by the processor 210 or other components of the shareholder device 102.

[0030] The cryptography module 302, which may be embodied as hardware, firmware, software, virtualized hardware, emulated architecture, and/or a combination thereof as discussed above, is configured to perform various cryptographic and/or security functions on behalf of the shareholder device 102. In some embodiments, the cryptography module 302 may be embodied as a cryptographic engine, an independent security co-processor of the shareholder device 102, a cryptographic accelerator incorporated into the processor 210, or a standalone software/firmware. Depending on the particular embodiment, the cryptography module 302 may generate and/or utilize various cryptographic keys (e.g., symmetric/asymmetric cryptographic keys) for encryption, decryption, signing, and/or signature verification. Additionally, in some embodiments, the cryptography module 302 may establish a secure connection with remote devices (e.g., the gateway device 104) over a network. In the illustrative embodiment, the cryptography module 302 may perform various mathematical, logical, hashing (e.g., keyed hashing), and/or cryptographic operations to data of the shareholder device 102 for generation of a partial authentication message, a validation signature, and/or other data of the multifactor threshold authentication protocol as described herein.

[0031] The communication module 304, which may be embodied as hardware, firmware, software, virtualized hardware, emulated architecture, and/or a combination thereof as discussed above, is configured to handle the communication between the shareholder device 102 and other computing devices of the system 100 (e.g., the gateway device 104). For example, as described herein, the shareholder device 102 may receive messages from the gateway device 104 such as,

for example, various cryptographic system parameters, messages received from the authentication server 106 with an authentication request, and/or other suitable data. Further, the shareholder device 102 may transmit, for example, parameter data, partial authentication messages, and validation signatures to the gateway device 104 as described in greater detail below.

[0032] The key share module 306, which may be embodied as hardware, firmware, software, virtualized hardware, emulated architecture, and/or a combination thereof as discussed above, is configured to generate a partial authentication message based on the parameter data and one or more messages received from the gateway device 104. For example, as described below, in some embodiments, the key share module 306 may receive shareholder key share parameters or a key projection corresponding with the particular shareholder device 102 from the gateway device 104. Based on the shareholder key share parameters and a portion of an authentication challenge message received from the gateway device 104, the key share module 306 may generate the corresponding shareholder key share and a partial authentication message as described below.

[0033] The sensor management module 308, which may be embodied as hardware, firmware, software, virtualized hardware, emulated architecture, and/or a combination thereof as discussed above, is configured to receive, process, and/or otherwise handle sensor data generated by the one or more sensors 220 of the shareholder device 102. For example, in some embodiments, the sensors 220 may generate sensor data indicative of biometric parameters of the user, the location of the shareholder device 102, inertial characteristics, and/or other relevant sensor data. It should be appreciated that the sensor management module 308 may process the sensor data in any suitable way to generate parameter data. As described herein, the parameter data may be transmitted to the gateway device 104 and incorporated in the partial authentication message.

[0034] Referring now to FIG. 4, in use, the gateway device 104 establishes an environment 400 for multifactor threshold authentication. The illustrative environment 400 includes a cryptography module 402, a communication module 404, a protocol initialization module 406, and an authentication module 408. The various modules of the environment 400 may be embodied as hardware, software, firmware, or a combination thereof. For example, the various modules, logic, and other components of the environment 400 may form a portion of, or

otherwise be established by, the processor, the I/O subsystem, and/or other hardware components of the gateway device 104. As such, in some embodiments, one or more of the modules of the environment 400 may be embodied as circuitry or collection of electrical devices (e.g., a cryptography circuitry, a communication circuitry, a protocol initialization circuitry, and/or an authentication circuitry). Additionally, in some embodiments, one or more of the illustrative modules may form a portion of another module and/or one or more of the illustrative modules may be independent of one another. Further, in some embodiments, one or more of the modules of the environment 400 may be embodied as virtualized hardware components or emulated architecture, which may be established and maintained by the processor or other components of the gateway device 104.

[0035] The cryptography module 402, which may be embodied as hardware, firmware, software, virtualized hardware, emulated architecture, and/or a combination thereof as discussed above, is configured to perform various cryptographic and/or security functions on behalf of the gateway device 104. It should be appreciated that, in some embodiments, the cryptography module 402 may be similar to the cryptography module 302 of the shareholder device 102. As such, the cryptography module 402 may be embodied as a cryptographic engine, an independent security co-processor of the gateway device 104, a cryptographic accelerator incorporated into the processor of the gateway device 104, or a standalone software/firmware. Further, depending on the particular embodiment, the cryptography module 402 may generate and/or utilize various cryptographic keys (e.g., symmetric/asymmetric cryptographic keys) for encryption, decryption, signing, and/or signature verification and/or may be configured to establish a secure connection with remote devices (e.g., the shareholder devices 102 and the authentication server 106) over one or more networks. In the illustrative embodiment, the cryptography module 402 may perform various mathematical, logical, hashing (e.g., keyed hashing), and/or cryptographic operations to data of the gateway device 104 for initializing the system 100 with various system key parameters and cryptographic system keys, determining shareholder key share parameters for each of the shareholder devices 102, determining an authenticator key share for the authentication server 106 that corresponds with the shareholder key shares, performing Lagrange interpolation, manipulating algebraic expressions (e.g., bivariate polynomials, vectors, etc.), determining whether a partial authentication message of a shareholder device 102 is valid, and/or performing other functions associated with the multifactor threshold authentication protocol as

described herein. It should be appreciated that the cryptography module 402 may utilize any suitable cryptographic algorithms, techniques, and/or mechanisms for performing the functions described herein. For example, in some embodiments, the system 100 utilizes ElGamal cryptographic keys.

[0036] The communication module 404, which may be embodied as hardware, firmware, software, virtualized hardware, emulated architecture, and/or a combination thereof as discussed above, is configured to handle the communication between the gateway device 104 and other computing devices of the system 100 (e.g., the shareholder devices 102 and the authentication server 106). For example, as described herein, the gateway device 104 may transmit various data to the shareholder devices 102 and the authentication server 106 during initialization of the system 100 for multifactor threshold authentication. Further, the gateway device 104 may receive messages from the authentication server 106 generated based on a set of cryptographic system keys (e.g., established by the gateway device 104), transmit the messages to the shareholder devices 102, receive a partial authentication message and parameter data (e.g., based on sensor data) from each shareholder device 102, and transmit the parameter data with an authentication value to the authentication server 106 as described herein.

[0037] The protocol initialization module 406, which may be embodied as hardware, firmware, software, virtualized hardware, emulated architecture, and/or a combination thereof as discussed above, is configured to initialize the shareholder devices 102 and the authentication server 106 for multifactor threshold authentication as described herein. In particular, as described below, in some embodiments, the protocol initialization module 406 may determine one or more system key parameters and a set of cryptographic system keys (e.g., including a public cryptographic key and a secret cryptographic key), transmit the system key parameters to the shareholder devices 102, transmit the system key parameters and the public cryptographic key (e.g., an ElGamal public key) to the authentication server 106, determine a bivariate polynomial based on the secret cryptographic key, and/or determine shareholder key share parameters for each shareholder device 102 and a corresponding authenticator key share. Of course, the protocol initialization module 406 may utilize other techniques to initialize the system 100 for multifactor threshold authentication in other embodiments.

[0038] The authentication module 408, which may be embodied as hardware, firmware, software, virtualized hardware, emulated architecture, and/or a combination thereof as discussed

above, is configured to perform various authentication techniques on behalf of the gateway device 104. For example, as described below, the authentication module 408 may receive and authenticate the partial authentication messages of the shareholder devices 102 to ensure that the messages are valid. It should be appreciated that the authentication module 408 may utilize any suitable cryptographic algorithms, techniques and/or mechanisms for doing so (e.g., in conjunction with the cryptography module 402) depending on the particular embodiment.

[0039] Referring now to FIG. 5, in use, the authentication server 106 establishes an environment 500 for multifactor threshold authentication. The illustrative environment 500 includes a cryptography module 502, a communication module 504, a request module 506, and an authentication module 508. The various modules of the environment 500 may be embodied as hardware, software, firmware, or a combination thereof. For example, the various modules, logic, and other components of the environment 500 may form a portion of, or otherwise be established by, the processor, the I/O subsystem, and/or other hardware components of the authentication server 106. As such, in some embodiments, one or more of the modules of the environment 500 may be embodied as circuitry or collection of electrical devices (e.g., a cryptography circuitry, a communication circuitry, a request circuitry, and/or an authentication circuitry). Additionally, in some embodiments, one or more of the illustrative modules may form a portion of another module and/or one or more of the illustrative modules may be independent of one another. Further, in some embodiments, one or more of the modules of the environment 500 may be embodied as virtualized hardware components or emulated architecture, which may be established and maintained by the processor or other components of the authentication server 106.

[0040] The cryptography module 502, which may be embodied as hardware, firmware, software, virtualized hardware, emulated architecture, and/or a combination thereof as discussed above, is configured to perform various cryptographic and/or security functions on behalf of the authentication server 106. It should be appreciated that, in some embodiments, the cryptography module 502 may be similar to the cryptography module 302 of the shareholder device 102 and/or the cryptography module 402 of the gateway device 104. As such, the cryptography module 502 may be embodied as a cryptographic engine, an independent security co-processor of the authentication server 106, a cryptographic accelerator incorporated into the processor of the authentication server 106, or a standalone software/firmware. Further, depending on the

particular embodiment, the cryptography module 502 may generate and/or utilize various cryptographic keys (e.g., symmetric/asymmetric cryptographic keys) for encryption, decryption, signing, and/or signature verification and/or may be configured to establish a secure connection with remote devices (e.g., the gateway device 104) over one or more networks. In the illustrative embodiment, the cryptography module 502 may perform various mathematical, logical, hashing (e.g., keyed hashing), and/or cryptographic operations to data of the authentication server 106 for determining the validity (e.g., authenticating) messages received from the gateway device 104, performing or otherwise utilizing Lagrange interpolation, and/or performing other functions associated with the multifactor threshold authentication protocol as described herein.

[0041] The communication module 504, which may be embodied as hardware, firmware, software, virtualized hardware, emulated architecture, and/or a combination thereof as discussed above, is configured to handle the communication between the authentication server 106 and other computing devices of the system 100 (e.g., the gateway device 104). For example, as described herein, the authentication server 106 may receive various data from and transmit various data to the gateway device 104 for multifactor threshold authentication.

[0042] The request module 506, which may be embodied as hardware, firmware, software, virtualized hardware, emulated architecture, and/or a combination thereof as discussed above, is configured to generate authentication request messages for transmittal to the gateway device 104 and subsequent forwarding to the shareholder devices 102. As described herein, the request module 506 may generate an authentication request that includes a set of messages generated based on cryptographic system keys received from the gateway device 104.

[0043] The authentication module 508, which may be embodied as hardware, firmware, software, virtualized hardware, emulated architecture, and/or a combination thereof as discussed above, is configured to perform various authentication techniques on behalf of the authentication server 106. As described below, in some embodiments, the authentication module 508 may determine the validity of one or more messages received from the gateway device 104, for example, based on Lagrange interpolation. In the illustrative embodiment, it should be appreciated that the authentication server 106 does not trust the gateway device 104, so the authentication server 106 performs its own validation of received data. Even if the gateway device 104 is certain that the shareholder devices 102 are secure, there is a possibility of the gateway device 104 or the communication channel (e.g., a wireless communication channel)

between the gateway device 104 and the authentication server 106 becoming compromised. It should be appreciated that the authentication module 508 may utilize any suitable cryptographic algorithms, techniques and/or mechanisms for performing the various authentication functions described herein (e.g., in conjunction with the cryptography module 502) depending on the particular embodiment.

[0044] Referring now to FIG. 6, in use, the gateway device 104 may execute a method 600 for multifactor threshold authentication initialization. It should be appreciated that, in some embodiments, the techniques of the method 600 may be executed by one or more of the modules of the environment 400 of the gateway device 104. The illustrative method 600 begins with block 602 in which the gateway device 104 determines the cryptographic system keys and system parameters for a user of the system 100. In doing so, the gateway device 104 may generate a secret cryptographic key, SK , in block 604 and/or may generate the cryptographic system keys based on an ElGamal cryptographic scheme in block 606. In particular, in the illustrative embodiment, the gateway device 104 selects prime numbers p and q in such a way that $p=2q+1$, and selects a primitive root, g , of the order q modulo the prime number p (i.e., g is a “generator” of the subgroup of order q of integers mod p) as system key parameters. Further, the gateway device 104 generates or otherwise determines an ElGamal public cryptographic key, y , according to $y = g^{SK} \bmod p$, wherein p is the prime number, g is the primitive root of order q mod p , and SK is the secret cryptographic key. In some embodiments, it should be appreciated that the secret key is a symmetric cryptographic key.

[0045] In block 608, the gateway device 104 transmits the system key parameters (or a portion thereof) to the shareholder devices 102. For example, in block 610, the gateway device 104 may transmit the primitive root, g , and the prime number, p , to the shareholder devices 102 (see, for example, flow 1002 of FIG. 10). In block 612, the gateway device 104 transmits the system key parameters and the public cryptographic key to the authentication server 106. In particular, in block 614, the gateway device 104 may transmit the primitive root (g), the prime (p), and the public cryptographic key ($y = g^{SK} \bmod p$) to the authentication server 106 (see, for example, flow 1004 of FIG. 10).

[0046] In block 616, the gateway device 104 determines a bivariate polynomial based on the secret key, SK . In particular, in the illustrative embodiment, the secret key, SK , is distributed

between nodes (e.g., the shareholder devices 102) using a bivariate polynomial, $F(x, z)$, such that $\deg_x(F(x, z)) = k - 1$, $\deg_z(F(x, z)) = 1$, and $F(0, 0) = SK$, where k is the number of shareholder devices 102 involved in the multifactor threshold authentication (e.g., the number of shareholder devices 102 that participate in the authentication protocol). It should be appreciated that the bivariate polynomial may be expressed according to $F(x, z) = f_{k-1,1}x^{k-1}z + f_{k-2,1}x^{k-2}z + \dots + f_{1,1}xz + f_{k-1,0}x^{k-1} + f_{k-2,0}x^{k-2} + \dots + f_{1,0}x + f_{0,1}z + SK$. In order to obtain such a low threshold (k) as a sufficient number of secret shareholders, additional security/authentication values may be stored by the authentication server 106 (e.g., additional values for Lagrange interpolation). In the illustrative embodiment, it should be appreciated that each node/shareholder is initialized by the curve of the first degree of z (not by the point).

[0047] In block 618, the gateway device 104 determines the shareholder key share parameters for each of the shareholder devices 102 participating in the multifactor threshold authentication protocol. To do so, in block 620, the gateway device 104 may determine coefficients of the bivariate polynomial, $F(x, z)$. In particular, in the illustrative embodiment, each shareholder key share, $SS_i(z)$, is determined according to $SS_i(z) = F(x = ID_i, z) = F_i(z) = ss_{i1}z + ss_{i0} \bmod q$ based on the bivariate polynomial, $F(x, z)$, where i is the index of the particular shareholder device 102, ID_i is the identifier of the shareholder device 102, ss_{i1} and ss_{i0} are coefficients, and wherein q is a cryptographic system parameter (e.g., determined/selected by the gateway device 104). It should be appreciated that, in some embodiments, the shareholder key share parameters may be expressed as a representation of the bivariate polynomial, $F(x, z)$, for a particular node (i.e., $x = ID_i$) according to $SS_i(z) = ss_{i1}z + ss_{i0} \bmod q$. In other embodiments, the shareholder key share parameters may be expressed based on the coefficients, ss_{i1} and ss_{i0} . For example, in some embodiments, the shareholder key share parameters may be represented as a vector of the coefficients, ss_{i1} and ss_{i0} . As described below, it should be appreciated that a shareholder device 102 may utilize the shareholder key share parameters in conjunction with the parameter data to generate the shareholder key share, SS_i , for that shareholder device 102.

[0048] In block 622, the gateway device 104 determines the authenticator key shares corresponding with the shareholder key shares. In the illustrative embodiment, the authentication server 106 stores a point of the bivariate polynomial, $F(x, z)$, for every node (e.g., every shareholder device 102) in which $z = L_{Terminal}$, where $L_{Terminal}$ is a portion of the secret retained by the authentication server 106. Accordingly, for each node $x = ID_i$, the authentication server 106 stores the point $SS_{Terminal}^{(i)} = SS_i(L_{Terminal}) = F(ID_i, L_{Terminal}) = ss_{i1}L_{Terminal} + ss_{i0} \bmod q$. It should be appreciated that, in some embodiments, the authenticator key shares involve the same coefficients, ss_{i1} and ss_{i0} , as the shareholder key shares. Accordingly, in some embodiments, a portion of the authenticator key shares determined by the gateway device 104 may be expressed similarly to the shareholder key shares (e.g., as a vector of the coefficients, ss_{i1} and ss_{i0}) and may be used by the authentication server 106 in conjunction with the secret, $L_{Terminal}$, retained by the authentication server 106 to generate the full authenticator key share. In block 624, the gateway device 104 transmits the shareholder key shares to the corresponding shareholder devices 102 (see, for example, flow 1106 of FIG. 10) and the authenticator key shares to the authentication server 106 (see, for example, flow 1108 of FIG. 10).

[0049] In block 626, the gateway device 104 determines a set of verification keys for the each shareholder device 102 based on the bivariate polynomial, $F(x, z)$. In particular, in the illustrative embodiment, the gateway device 104 determines a pair of verification keys, VK_i , such that $VK_i = \{v^{ss_{i1}}, v^{ss_{i0}}\}$, v is a *primitive root of the order $q \bmod p$* , and ss_{i1} and ss_{i0} are the coefficients or key projections described above. In some embodiments, the integer v may be a random constant value and may, for example, be published or stored on the gateway device 104. As described below, the gateway device 104 may utilize the verification keys to determine whether partial authentication messages received from the shareholder devices 102 are valid.

[0050] Referring now to FIG. 7, in use, the gateway device 104 may execute a method 700 for multifactor threshold authentication. It should be appreciated that, in some embodiments, the techniques of the method 700 may be executed by one or more of the modules of the environment 400 of the gateway device 104. The illustrative method 700 begins with block 702 in which the gateway device 104 receives a set of messages from the authentication server 106 (see, for example, flow 1102 of FIG. 11). In the illustrative embodiment, the set of

messages is indicative of a request by the authentication server 106 for authentication of the shareholder devices 102 and generated based on the cryptographic system keys. As described below, in some embodiments, the gateway device 104 receives the set, $\{a, b\}$, of messages a and b in which the message $a = g^k \bmod p$ and the message $b = my^k \bmod p$ such that $p = 2q + 1$, where p and q are the prime numbers for the cryptosystem, g is the determined primitive root of order $q \bmod p$, k is a random session key, m is a challenge message of the authentication server 106, y is the public cryptographic key generated according to $y = g^{SK} \bmod p$, and SK is the secret cryptographic key.

[0051] In block 704, the gateway device 104 transmits one or more of the messages (e.g., a and/or b) to the shareholder devices 102. For example, in the illustrative embodiment, the gateway device 104 transmits the message, a , to each of the shareholder devices 102 involved in the multifactor threshold authentication protocol (see, for example, flow 1104 of FIG. 11).

[0052] In block 706, the gateway device 104 receives a partial authentication message and parameter data from each of the shareholder devices 102 (see, for example, flow 1106 of FIG. 11). As described above, the parameter data, L_i , is based on sensor data generated by the corresponding (e.g., the i -th shareholder device 102). For example, in some embodiments, the parameter data may be based on data sensed from a person's biometric parameters (e.g., heart rate, temperature, etc.), the absolute or relative location of the shareholder device 102 or other entity, dynamic and interaction patterns (e.g., inertial characteristics of the shareholder device 102, touch patterns, etc.), and/or other sensor data. It should be appreciated that the parameter data may be represented in any suitable way and may depend on the particular embodiment. As described below, in the illustrative embodiment, the partial authentication message is based on the parameter data of the corresponding shareholder device 102 and the message, a , received by the shareholder device 102 from the gateway device 104. In particular, the shareholder device 102 may generate the partial authentication message, $Part_i$, according to $Part_i = a^{SS_i(L_i)} \bmod p$, where a is the message received from the gateway device 104, L_i is the parameter data, p is the prime number of the cryptosystem, and $SS_i(\bullet)$ is a shareholder key share of the shareholder device 102 based on an identifier, ID_i , of the shareholder device. Further, in the illustrative embodiment, the shareholder key share, SS_i , may be determined according to

$SS_i(L_i) = F(x = ID_i, z = L_i) \bmod q$. In other words, the shareholder device 102 may determine the shareholder key share based on the parameter data and the shareholder key share parameters received from the gateway device 104.

[0053] As described below, in some embodiments, the shareholder device 102 may obtain an additional cryptographic signature that allows the gateway device 104 to verify the validity of received shares of partially decrypted messages. For example, in the illustrative embodiment, each shareholder device 102 generates a validation signature, VV_i , according to $VV_i = VV_{i,1}, VV_{i,2}$, in which $VV_{i,1} = \text{Hash}(v, a, v^{SS_i(L_i)} \bmod p, Part_i, v^r \bmod p, a' \bmod p)$, where $VV_{i,2} = SS_i(L_i) * VV_{i,1} + r$, where v is a primitive root of the order $q \bmod p$, and where r is an integer mod p . It should be appreciated that any suitable cryptographic hash algorithm may be utilized in determining the validation signature and may depend on the particular embodiment.

[0054] In block 708, the gateway device 104 determines the validity of the partial authentication messages received from the shareholder devices 102. In particular, in some embodiments, the gateway device 104 may compute and determine whether $VV_{i,1} = \text{Hash}(v, a, v'_i, Part_{ai}, v^{VV_{i,2}} * v_i^{r-VV_{i,1}}, a^{VV_{i,2}} Part_{ai}^{-VV_{i,1}})$ where $v'_i = (VK_i^{(1)})^{L_i} * VK_i^{(2)} \bmod p$. In some embodiments, the authentication request received from the authentication server 106 indicates a number of nodes (e.g., shareholder devices 102) necessary for authentication. For example, in an embodiment, the system 100 may include five shareholder devices 102 but the authentication server 106 may require only three shareholder devices 102 to authenticate. In such an embodiment, the gateway device 104 may select, for example, three of the shareholder devices 102 and transmit the authentication request and/or corresponding data to those three shareholder devices 102. If the gateway device 104 receives data from the selected shareholder devices 102 and determines that one of the messages is corrupted (e.g., due to a device malfunction, denial of service attack, etc.), the gateway device 104 may request one of the other two shareholder devices 102 to join the protocol. In the illustrative embodiment, it is unnecessary for the gateway device 104 to inform the authentication server 106 about the issue to restart the protocol, which considerably increases the efficiency of the protocol compared to many other authentication schemes.

[0055] If the gateway device 104 determines that one or more of the partial authentication messages is invalid (e.g., corrupted) in block 710, the method 700 returns to block 706 in which the gateway device 104 selects another shareholder device 102 from which to receive a new partial authentication message and parameter data. However, if the verifications are successful (i.e., the messages are determined to be valid), the method 700 advances to block 712 in which the gateway device 104 determines Lagrange coefficients ($\lambda_{0,x_i}^{(x)}$ and $\lambda_{0,z_j}^{(z)}$) for interpolation of $F(0,0)$ and an authentication value, ret , based on the Lagrange coefficients. In the illustrative embodiment, the Lagrange coefficients may be determined based on $F(0,0) = \sum_{i=1}^k \sum_{j=1}^2 F(x_i, z_j) \lambda_{0,x_i}^{(x)} \lambda_{0,z_j}^{(z)}$, where $x = ID_i$, $z_1 = L_i$, and $z_2 = L_{Terminal}$. Further, in the illustrative embodiment, the gateway device 104 may determine the authentication value, ret , according to determine an authentication value, ret , according to $ret = \frac{b}{a \text{Pr}} \mod p$, where $a \text{Pr} = \prod_{i=1}^k (Part_i)^{(\lambda_{0,ID_i}^{(x)} \lambda_{0,z_1}^{(z)})} \mod p$, where $Part_i$ is the partial authentication message of the corresponding shareholder device 102, and where $\lambda_{0,ID_i}^{(x)}$ and $\lambda_{0,z_1}^{(z)}$ are Lagrange coefficients for interpolation of $F(0,0)$. In block 714, the gateway device 104 transmits the authentication value, ret , and the parameter data of the shareholder devices 102 to the authentication server 106 (see, for example, flow 1108 of FIG. 11). As described herein, in some embodiments, the authentication server 106 performs its own validation of the received data.

[0056] Referring now to FIG. 8, in use, one or more of the shareholder devices 102 (e.g., each shareholder device 102) may execute a method 800 for multifactor threshold authentication initialization. It should be appreciated that, in some embodiments, the techniques of the method 800 may be executed by one or more of the modules of the environment 300 of the shareholder device 102. The illustrative method 800 begins with block 802 in which the shareholder device 102 receives an authentication request message from the gateway device 104 (see, for example, flow 1104 of FIG. 11). As indicated above, the authentication request message received may be the message $a = g^k \mod p$ such that $p=2q+1$, where p and q are the prime numbers for the cryptosystem, g is the determined primitive root of the order $q \mod p$, and k is the random session key used for one round of authentication.

[0057] In block 804, the shareholder device 102 determines parameter data, L_i , based on the sensor data generated by the sensors 220 of the shareholder device 102. As indicated above, it should be appreciated that the number/type of the sensors 220 and the particular parameter data may vary depending on the particular embodiment. For example, the parameter data may be indicative of a biometric parameter of a user of the shareholder device 102, a location of the shareholder device 102 relative to the user, one or more inertial characteristics of the shareholder device 102, and/or other contextual information of the shareholder device 102 or user.

[0058] In block 806, the shareholder device 102 generates a partial authentication messages based on the shareholder key share and parameter data. As described herein, in the illustrative embodiment, the shareholder device 102 generates the partial authentication message, $Part_i$, according to $Part_i = a^{SS_i(L_i)} \bmod p$, where a is the message received from the gateway device 104, L_i is the parameter data, p is a prime number of the cryptosystem, and $SS_i(\bullet)$ is a shareholder key share of the shareholder device 102 based on an identifier of the shareholder device 102. In some embodiments, the shareholder key share, SS_i , may be determined according to $SS_i(L_i) = F(x = ID_i, z = L_i) \bmod q$. In other words, the shareholder device 102 may determine the shareholder key share based on the parameter data and the shareholder key share parameters received from the gateway device 104.

[0059] In block 808, the shareholder device 102 generates or otherwise determines a validation signature of the partial authentication message. As described above, in some embodiments, the shareholder device 102 may generate the validation signature, VV_i , according to $VV_i = VV_{i,1}, VV_{i,2}$, where $VV_{i,1} = Hash(v, a, v^{SS_i(L_i)} \bmod p, Part_i, v^r \bmod p, a^r \bmod p)$, where $VV_{i,2} = SS_i(L_i) * VV_{i,1} + r$, where v is a primitive root of the order $q \bmod p$, and where r is an integer $\bmod p$. In block 810, the shareholder device 102 transmits the partial authentication message, the parameter data, and the validation signature to the gateway device 104 (see, for example, flow 1106 of FIG. 11).

[0060] Referring now to FIG. 9, in use, the authentication server 106 may execute a method 900 for multifactor threshold authentication initialization. It should be appreciated that, in some embodiments, the techniques of the method 900 may be executed by one or more of the modules of the environment 500 of the authentication server 106. The illustrative method 900

begins with block 902 in which the authentication server 106 generates a set of messages based on the cryptographic system keys received from the gateway device 104 (e.g., including an authentication request message). In particular, in the illustrative embodiment, the authentication server 106 generates messages a and b in which the message $a = g^k \bmod p$ and the message $b = my^k \bmod p$ such that $p=2q+1$, where p and q are the prime numbers for the cryptosystem, g is the determined primitive root of order $q \bmod p$, k is a random session key, m is a challenge message of the authentication server 106, y is the public cryptographic key generated according to $y = g^{SK} \bmod p$, and SK is the secret cryptographic key. In block 904, the authentication server 106 transmits the set of messages, $\{a, b\}$, to the gateway device 104 (see, for example, flow 1102 of FIG. 11).

[0061] As described above, the shareholder devices 102 generate partial authentication messages and validation signatures for verification by the gateway device 104. If the shareholder device 102 messages are validated by the gateway device 104, the authentication server 106 receives an authentication value, ret , and parameter data, L_i , from the gateway device 104 in block 906 (see, for example, flow 1108 of FIG. 11). As described above, in some embodiments, the authentication value, ret , is defined according to $ret = \frac{b}{a \Pr} \bmod p$, where

$a \Pr = \prod_{i=1}^k (Part_i)^{(\lambda_{0, ID_i}^{(x)} \lambda_{0, z_1}^{(z)})} \bmod p$, $Part_i$ is a partial authentication message of the corresponding shareholder device 102, and $\lambda_{0, ID_i}^{(x)}$ and $\lambda_{0, z_1}^{(z)}$ are Lagrange coefficients for interpolation of the bivariate polynomial, $F(x, z)$.

[0062] In block 908, the authentication server 106 determines the validity of received data based on Lagrange interpolation. In doing so, in block 910, the authentication server 106 may calculate coefficients of a Lagrange interpolation function based on the received parameter data. In particular, in some embodiments, the authentication server 106 determines whether the challenge message, m , is equal to $ret / \left(\prod_{i=1}^k (a)^{(SS_{terminal}^i \lambda_{0, ID_i}^{(x)} \lambda_{0, z_2}^{(z)})} \right) \bmod p$. If not, the authentication server 106 may determine that the authentication has failed. However, if the computed value matches the initial challenge message, m , the authentication server 106 may utilize the parameter data/values in conjunction with a trust function to determine whether to authorize the user to

have access and the extent of such access. For example, the output values of the trust function may be compared to various threshold values to determine authorized levels of access by the user.

[0063] It should be appreciated that the gateway device 104 functions as an aggregator of secure data from the shareholder devices 102 (e.g., thereby minimizing channel overhead) and utilizes various zero-knowledge protocols to prevent security risks. As described herein, the system secret key, *SK*, is shared between secret shareholders (e.g., the shareholder devices 102) by a threshold scheme. The shareholder devices 102 prove that they know the secret key by distributed decryption of a random message received from the authentication server 106. During the decryption, each shareholder device 102 includes various information regarding the device status, location, and/or other features (i.e., the parameter data). In the illustrative embodiment, the gateway device 104 does not have any explicit information about the secret key or its shares such that it cannot change parameter data without causing an error in the protocol. However, as described above, the gateway device 104 does include a mechanism to ensure that the shareholder devices 102 follow the protocol, thereby avoiding unnecessary transactions with the authentication server 106. Further, if one of the shareholder devices 102 causes an error, the gateway device 104 may select another shareholder device 102 for authentication without restarting the protocol. If the partial messages from the shareholder devices 102 are validated, the gateway device 104 may combine the partial messages into one common decrypted message and transmit the message and the parameter data to the authentication server 106 for authentication. As described above, the authentication server 106 may evaluate the decrypted message and make a decision regarding the trust level of the user based, for example, on the parameter data of the shareholder devices 102.

EXAMPLES

[0064] Illustrative examples of the technologies disclosed herein are provided below. An embodiment of the technologies may include any one or more, and any combination of, the examples described below.

[0065] Example 1 includes a gateway device for multifactor threshold authentication, the gateway device comprising a communication module to (i) receive, from an authentication server, a message generated by the authentication server based on a set of cryptographic system

key, (ii) transmit the message to a shareholder device, and (iii) receive a partial authentication message and parameter data from the shareholder device, wherein the parameter data is based on sensor data generated by the shareholder device and the partial authentication message is based on the parameter data and the message received from the authentication server; and an authentication module to determine whether the partial authentication message is valid.

[0066] Example 2 includes the subject matter of Example 1, and wherein to receive the message comprises to receive a message generated based on one or more El Gamal cryptographic keys.

[0067] Example 3 includes the subject matter of any of Examples 1 and 2, and wherein to receive the message generated by the authentication server comprises to receive a message, a , generated according to $a = g^k \bmod p$, wherein p and q are prime numbers such that $p=2q+1$; wherein g is a primitive root of order $q \bmod p$; and wherein k is a random session key used for one round of authentication.

[0068] Example 4 includes the subject matter of any of Examples 1-3, and wherein to receive the message generated by the authentication server further comprises to receive a message, b , generated according to $b = my^k \bmod p$, wherein m is a challenge message of the authentication server; wherein y is a public cryptographic key generated according to $y = g^{SK} \bmod p$; and wherein SK is a secret cryptographic key.

[0069] Example 5 includes the subject matter of any of Examples 1-4, and wherein to transmit the message to the shareholder device comprises to transmit the message to each of the shareholder devices involved in the multifactor threshold authentication.

[0070] Example 6 includes the subject matter of any of Examples 1-5, and wherein to receive the partial authentication message comprises to receive a partial authentication message, $Part_i$, determined according to $Part_i = a^{SS_i(L_i)} \bmod p$, wherein a is the message generated by the authentication server; wherein L_i is the parameter data; wherein p is a prime number; and wherein $SS_i(\bullet)$ is a shareholder key share of the shareholder device based on an identifier of the shareholder device.

[0071] Example 7 includes the subject matter of any of Examples 1-6, and wherein to receive the partial authentication message further comprises to receive a cryptographic signature of the partial authentication message.

[0072] Example 8 includes the subject matter of any of Examples 1-7, and wherein to determine whether the partial authentication message is valid comprises to determine whether the partial authentication message is valid based on the cryptographic signature.

[0073] Example 9 includes the subject matter of any of Examples 1-8, and further including a protocol initialization module to initialize the authentication server and the shareholder device for multifactor threshold authentication.

[0074] Example 10 includes the subject matter of any of Examples 1-9, and wherein to initialize the authentication server and the shareholder device comprises to determine one or more system key parameters and the set of cryptographic system keys; transmit the one or more system key parameters to the shareholder device; transmit the one or more system key parameters and a public cryptographic key of the set of cryptographic system keys to the authentication server; determine a bivariate polynomial based on a secret key of the set of cryptographic system keys; determine a shareholder key share parameter of the shareholder device based on the bivariate polynomial and an identifier of the shareholder device; determine an authenticator key share corresponding with the shareholder key share; and transmit the shareholder key share parameter to the shareholder device and the authenticator key share to the authentication device.

[0075] Example 11 includes the subject matter of any of Examples 1-10 and wherein the one or more system key parameters comprises a prime number and a primitive root modulo the prime number.

[0076] Example 12 includes the subject matter of any of Examples 1-11, and wherein to determine the set of cryptographic system keys comprises to determine a secret cryptographic key, SK ; and determine the public cryptographic key, y , according to $y = g^{SK} \bmod p$, wherein p and q are prime numbers such that $p = 2q + 1$; and wherein g is a primitive root of order $q \bmod p$.

[0077] Example 13 includes the subject matter of any of Examples 1-12, and wherein to determine the bivariate polynomial comprises to determine a bivariate polynomial, $F(x, z)$, such

that $\deg_x(F(x, z)) = k - 1$, where k is a number of shareholder devices involved in the multifactor threshold authentication; $\deg_z(F(x, z)) = 1$; and $F(0, 0) = SK$.

[0078] Example 14 includes the subject matter of any of Examples 1-13, and wherein the authentication module is further to (i) determine coefficients for Lagrange interpolation of a bivariate polynomial that involves the parameter data in response to a determination that the partial authentication message is valid and (ii) determine an authentication value based on the coefficients; and wherein the communication module is further to transmit the authentication value to the authentication server.

[0079] Example 15 includes the subject matter of any of Examples 1-14, and wherein to determine the authentication value comprises to determine an authentication value, ret , according to $ret = \frac{b}{aPr} \bmod p$, wherein $aPr = \prod_{i=1}^k (Part_i)^{(\lambda_{0,ID_i}^{(x)} \lambda_{0,z_i}^{(z)})} \bmod p$; wherein $Part_i$ is the partial authentication message; and wherein $\lambda_{0,ID_i}^{(x)}$ and $\lambda_{0,z_i}^{(z)}$ are Lagrange coefficients for interpolation of $F(0, 0)$.

[0080] Example 16 includes the subject matter of any of Examples 1-15, and wherein to determine the shareholder key share parameter comprises to determine a shareholder key share parameter, $SS_i(z)$, according to $SS_i(z) = F(x = ID_i, z) = F_i(z) = ss_{i1}z + ss_{i0} \bmod q$ based on the bivariate polynomial, wherein ID_i is the identifier of the shareholder device; wherein ss_{i1} and ss_{i0} are coefficients; and wherein q is a cryptographic system parameter.

[0081] Example 17 includes the subject matter of any of Examples 1-16, and wherein the shareholder key share parameter is represented as a vector of the coefficients ss_{i1} and ss_{i0} .

[0082] Example 18 includes the subject matter of any of Examples 1-17, and wherein the initialization module is further to determine a set of verification keys for the shareholder device based on the bivariate polynomial.

[0083] Example 19 includes the subject matter of any of Examples 1-18, and wherein to determine the set of verification keys comprises to determine a pair of verification keys, VK_i , such that $VK_i = \{v^{ss_{i1}}, v^{ss_{i0}}\}$ and v is a primitive root of the order $q \bmod p$.

[0084] Example 20 includes the subject matter of any of Examples 1-19, and wherein to determine whether the partial authentication message is valid comprises to determine whether the partial authentication message is valid based on the pair of verification keys.

[0085] Example 21 includes the subject matter of any of Examples 1-20, and wherein the communication module is further to request data from another shareholder device in response to a determination that the partial authentication message of the shareholder device is not valid.

[0086] Example 22 includes the subject matter of any of Examples 1-21, and wherein the gateway device is embodied as a wearable compute device.

[0087] Example 23 includes a method for multifactor threshold authentication by a gateway device, the method comprising receiving, by the gateway device and from an authentication server, a message generated by the authentication server based on a set of cryptographic system keys; transmitting, by the gateway device, the message to a shareholder device; receiving, by the gateway device, a partial authentication message and parameter data from the shareholder device, wherein the parameter data is based on sensor data generated by the shareholder device and the partial authentication message is based on the parameter data and the message received from the authentication server; and determining, by the gateway device, whether the partial authentication message is valid.

[0088] Example 24 includes the subject matter of Example 23, and wherein receiving the message comprises receiving a message generated based on one or more El Gamal cryptographic keys.

[0089] Example 25 includes the subject matter of any of Examples 23 and 24, and wherein receiving the message generated by the authentication server comprises receiving a message, a , generated according to $a = g^k \bmod p$, wherein p and q are prime numbers such that $p=2q+1$; wherein g is a primitive root of order $q \bmod p$; and wherein k is a random session key used for one round of authentication.

[0090] Example 26 includes the subject matter of any of Examples 23-25, and wherein receiving the message generated by the authentication server further comprises receiving a message, b , generated according to $b = my^k \bmod p$, wherein m is a challenge message of the authentication server; wherein y is a public cryptographic key generated according to $y = g^{SK} \bmod p$; and wherein SK is a secret cryptographic key.

[0091] Example 27 includes the subject matter of any of Examples 23-26, and wherein transmitting the message to the shareholder device comprises transmitting the message to each of the shareholder devices involved in the multifactor threshold authentication.

[0092] Example 28 includes the subject matter of any of Examples 23-27, and wherein receiving the partial authentication message comprises receiving a partial authentication message, $Part_i$, determined according to $Part_i = a^{SS_i(L_i)} \bmod p$, wherein a is the message generated by the authentication server; wherein L_i is the parameter data; wherein p is a prime number; and wherein $SS_i(\bullet)$ is a shareholder key share of the shareholder device based on an identifier of the shareholder device.

[0093] Example 29 includes the subject matter of any of Examples 23-28, and wherein receiving the partial authentication message further comprises receiving a cryptographic signature of the partial authentication message.

[0094] Example 30 includes the subject matter of any of Examples 23-29, and wherein determining whether the partial authentication message is valid comprises determining whether the partial authentication message is valid based on the cryptographic signature.

[0095] Example 31 includes the subject matter of any of Examples 23-30, and further including initializing, by the gateway device, the authentication server and the shareholder device for multifactor threshold authentication.

[0096] Example 32 includes the subject matter of any of Examples 23-31, and wherein initializing the authentication server and the shareholder device comprises determining, by the gateway device, one or more system key parameters and the set of cryptographic system keys; transmitting, by the gateway device, the one or more system key parameters to the shareholder device; transmitting, by the gateway device, the one or more system key parameters and a public cryptographic key of the set of cryptographic system keys to the authentication server; determining, by the gateway device, a bivariate polynomial based on a secret key of the set of cryptographic system keys; determining, by the gateway device, a shareholder key share parameter of the shareholder device based on the bivariate polynomial and an identifier of the shareholder device; determining, by the gateway device, an authenticator key share corresponding with the shareholder key share; and transmitting, by the gateway device, the

shareholder key share parameter to the shareholder device and the authenticator key share to the authentication device.

[0097] Example 33 includes the subject matter of any of Examples 23-32, and wherein the one or more system key parameters comprises a prime number and a primitive root modulo the prime number.

[0098] Example 34 includes the subject matter of any of Examples 23-33, and wherein determining the set of cryptographic system keys comprises determining a secret cryptographic key, SK ; and determining the public cryptographic key, y , according to $y = g^{SK} \bmod p$, wherein p and q are prime numbers such that $p=2q+1$; and wherein g is a primitive root of order $q \bmod p$.

[0099] Example 35 includes the subject matter of any of Examples 23-34, and wherein determining the bivariate polynomial comprises determining a bivariate polynomial, $F(x,z)$, such that $\deg_x(F(x,z)) = k-1$, where k is a number of shareholder devices involved in the multifactor threshold authentication; $\deg_z(F(x,z)) = 1$; and $F(0,0) = SK$.

[00100] Example 36 includes the subject matter of any of Examples 23-35, and further including determining, by the gateway device, coefficients for Lagrange interpolation of a bivariate polynomial that involves the parameter data in response to determining the partial authentication message is valid; determining, by the gateway device, an authentication value based on the coefficients; and transmitting, by the gateway device, the authentication value to the authentication server.

[00101] Example 37 includes the subject matter of any of Examples 23-36, and wherein determining the authentication value comprises determining an authentication value, ret , according to $ret = \frac{b}{aPr} \bmod p$, wherein $aPr = \prod_{i=1}^k (Part_i)^{(\lambda_{0,ID_i}^{(x)} \lambda_{0,z_1}^{(z)})} \bmod p$; wherein $Part_i$ is the partial authentication message; and wherein $\lambda_{0,ID_i}^{(x)}$ and $\lambda_{0,z_1}^{(z)}$ are Lagrange coefficients for interpolation of $F(0,0)$.

[00102] Example 38 includes the subject matter of any of Examples 23-37, and wherein determining the shareholder key share parameter comprises determining a shareholder key share parameter, $SS_i(z)$, according to $SS_i(z) = F(x = ID_i, z) = F_i(z) = ss_{i1}z + ss_{i0} \bmod q$ based on the

bivariate polynomial, wherein ID_i is the identifier of the shareholder device; wherein ss_{i1} and ss_{i0} are coefficients; and wherein q is a cryptographic system parameter.

[00103] Example 39 includes the subject matter of any of Examples 23-38, and wherein the shareholder key share parameter is represented as a vector of the coefficients ss_{i1} and ss_{i0} .

[00104] Example 40 includes the subject matter of any of Examples 23-39, and further including determining a set of verification keys for the shareholder device based on the bivariate polynomial.

[00105] Example 41 includes the subject matter of any of Examples 23-40, and wherein determining the set of verification keys comprises determining a pair of verification keys, VK_i , such that $VK_i = \{v^{ss_{i1}}, v^{ss_{i0}}\}$ and v is a primitive root of the order $q \bmod p$.

[00106] Example 42 includes the subject matter of any of Examples 23-41, and wherein determining whether the partial authentication message is valid comprises determining whether the partial authentication message is valid based on the pair of verification keys.

[00107] Example 43 includes the subject matter of any of Examples 23-42, and further including requesting data from another shareholder device in response to determining the partial authentication message of the shareholder device is not valid.

[00108] Example 44 includes the subject matter of any of Examples 23-43, and wherein the gateway device is embodied as a wearable compute device.

[00109] Example 45 includes a computing device comprising a processor; and a memory having stored therein a plurality of instructions that when executed by the processor cause the computing device to perform the method of any of Examples 23-44.

[00110] Example 46 includes one or more machine-readable storage media comprising a plurality of instructions stored thereon that in response to being executed result in a computing device performing the method of any of Examples 23-44.

[00111] Example 47 includes a computing device comprising means for performing the method of any of Examples 23-44.

[00112] Example 48 includes a shareholder device for multifactor threshold authentication, the shareholder device comprising a communication module to receive, from a gateway device, a message determined based on a set of cryptographic system keys; a sensor management module to determine parameter data based on sensor data generated by one or more

sensors of the shareholder device; and a key share module to (i) generate a partial authentication message based on the parameter data and the message received from the gateway device and (ii) generate a validation signature of the partial authentication message; wherein the communication module is further to transmit the partial authentication message, the parameter data, and the validation signature to the gateway device for multifactor threshold authentication.

[00113] Example 49 includes the subject matter of Example 48, and wherein to receive the message comprises to receive a message, a , generated according to $a = g^k \bmod p$, wherein p and q are prime numbers such that $p=2q+1$; wherein g is a primitive root of order $q \bmod p$; and wherein k is a random session key used for one round of authentication.

[00114] Example 50 includes the subject matter of any of Examples 48 and 49, and wherein the communication module is further to receive the prime number, p , and the primitive root, g , from the gateway device.

[00115] Example 51 includes the subject matter of any of Examples 48-50, and wherein to generate the partial authentication message comprises to generate a partial authentication message, $Part_i$, according to $Part_i = a^{SS_i(L_i)} \bmod p$, wherein a is the message received from the gateway device; wherein L_i is the parameter data; wherein p is a prime number; and wherein $SS_i(\bullet)$ is a shareholder key share of the shareholder device based on an identifier of the shareholder device.

[00116] Example 52 includes the subject matter of any of Examples 48-51, and wherein to generate the validation signature comprises to generate a validation signature, VV_i , according to $VV_i = VV_{i,1}, VV_{i,2}$, wherein $VV_{i,1} = Hash(v, a, v^{SS_i(L_i)} \bmod p, Part_i, v^r \bmod p, a^r \bmod p)$; wherein $VV_{i,2} = SS_i(L_i) * VV_{i,1} + r$; and wherein v is a primitive root of the order $q \bmod p$ and r is an integer mod p .

[00117] Example 53 includes the subject matter of any of Examples 48-52, and wherein the communication module is further to receive the shareholder key share parameter, SS_i , from the gateway device, wherein SS_i is determined according to $SS_i(z) = F(x = ID_i, z) = F_i(z) = ss_{i1}z + ss_{i0} \bmod q$ based on a bivariate polynomial, $F(x, z)$;

wherein ID_i is the identifier of the shareholder device; wherein ss_{i1} and ss_{i0} are coefficients; and wherein q is a cryptographic system parameter.

[00118] Example 54 includes the subject matter of any of Examples 48-53, and wherein the bivariate polynomial, $F(x, z)$, is determined such that $\deg_x(F(x, z)) = k - 1$, where k is a number of shareholder devices involved in the multifactor threshold authentication; $\deg_z(F(x, z)) = 1$; and $F(0, 0) = SK$, wherein SK is a secret cryptographic key determined by the gateway device.

[00119] Example 55 includes the subject matter of any of Examples 48-54, and wherein the shareholder key share parameter is represented as a vector of the coefficients ss_{i1} and ss_{i0} .

[00120] Example 56 includes the subject matter of any of Examples 48-55, and wherein the communication module is further to receive one or more initialization messages from the gateway device for initialization of the multifactor threshold authentication.

[00121] Example 57 includes the subject matter of any of Examples 48-56, and wherein to determine the parameter data comprises to determine a biometric parameter of a user of the shareholder device based on the sensor data.

[00122] Example 58 includes the subject matter of any of Examples 48-57, and wherein to determine the parameter data comprises to determine a location of the shareholder device relative to a user of the shareholder device based on the sensor data.

[00123] Example 59 includes the subject matter of any of Examples 48-58, and wherein to determine the parameter data comprises to determine an inertial characteristic of the shareholder device.

[00124] Example 60 includes the subject matter of any of Examples 48-59, and wherein the shareholder device is embodied as a wearable compute device.

[00125] Example 61 includes a method for multifactor threshold authentication by a shareholder device, the method comprising receiving, by the shareholder device and from a gateway device, a message determined based on a set of cryptographic system keys; determining, by the shareholder device, parameter data based on sensor data generated by one or more sensors of the shareholder device; generating, by the shareholder device, a partial authentication message based on the parameter data and the message received from the gateway device; generating, by the shareholder device, a validation signature of the partial authentication message; and

transmitting, by the shareholder device, the partial authentication message, the parameter data, and the validation signature to the gateway device for multifactor threshold authentication.

[00126] Example 62 includes the subject matter of Example 61, and wherein receiving the message comprises receiving a message, a , generated according to $a = g^k \bmod p$, wherein p and q are prime numbers such that $p=2q+1$; wherein g is a primitive root of order $q \bmod p$; and wherein k is a random session key used for one round of authentication.

[00127] Example 63 includes the subject matter of any of Examples 61 and 62, and further including receiving, by the shareholder device, the prime number, p , and the primitive root, g , from the gateway device.

[00128] Example 64 includes the subject matter of any of Examples 61-63, and wherein generating the partial authentication message comprises generating a partial authentication message, $Part_i$, according to $Part_i = a^{SS_i(L_i)} \bmod p$, wherein a is the message received from the gateway device; wherein L_i is the parameter data; wherein p is a prime number; and wherein $SS_i(\bullet)$ is a shareholder key share of the shareholder device based on an identifier of the shareholder device.

[00129] Example 65 includes the subject matter of any of Examples 61-64, and wherein generating the validation signature comprises generating a validation signature, VV_i , according to $VV_i = VV_{i,1}, VV_{i,2}$, wherein $VV_{i,1} = Hash(v, a, v^{SS_i(L_i)} \bmod p, Part_i, v^r \bmod p, a^r \bmod p)$; wherein $VV_{i,2} = SS_i(L_i) * VV_{i,1} + r$; and wherein v is a primitive root of the order $q \bmod p$ and r is an integer mod p .

[00130] Example 66 includes the subject matter of any of Examples 61-65, and further including receiving, by the shareholder device, the shareholder key share parameter, SS_i , from the gateway device, wherein SS_i is determined according to $SS_i(z) = F(x = ID_i, z) = F_i(z) = ss_{i1}z + ss_{i0} \bmod q$ based on a bivariate polynomial, $F(x, z)$; wherein ID_i is the identifier of the shareholder device; wherein ss_{i1} and ss_{i0} are coefficients; and wherein q is a cryptographic system parameter.

[00131] Example 67 includes the subject matter of any of Examples 61-66, and wherein the bivariate polynomial, $F(x, z)$, is determined such that $\deg_x(F(x, z)) = k - 1$, where k is a

number of shareholder devices involved in the multifactor threshold authentication; $\deg_z(F(x,z)) = 1$; and $F(0,0) = SK$, wherein SK is a secret cryptographic key determined by the gateway device.

[00132] Example 68 includes the subject matter of any of Examples 61-67, and wherein the shareholder key share parameter is represented as a vector of the coefficients ss_{i1} and ss_{i0} .

[00133] Example 69 includes the subject matter of any of Examples 61-68, and further including receiving, by the shareholder device, one or more initialization messages from the gateway device for initialization of the multifactor threshold authentication.

[00134] Example 70 includes the subject matter of any of Examples 61-69, and wherein determining the parameter data comprises determining a biometric parameter of a user of the shareholder device based on the sensor data.

[00135] Example 71 includes the subject matter of any of Examples 61-70, and wherein determining the parameter data comprises determining a location of the shareholder device relative to a user of the shareholder device based on the sensor data.

[00136] Example 72 includes the subject matter of any of Examples 61-71, and wherein determining the parameter data comprises determining an inertial characteristic of the shareholder device.

[00137] Example 73 includes the subject matter of any of Examples 61-72, and wherein the shareholder device is embodied as a wearable compute device.

[00138] Example 74 includes a computing device comprising a processor; and a memory having stored therein a plurality of instructions that when executed by the processor cause the computing device to perform the method of any of Examples 61-73.

[00139] Example 75 includes one or more machine-readable storage media comprising a plurality of instructions stored thereon that in response to being executed result in a computing device performing the method of any of Examples 61-73.

[00140] Example 76 includes a computing device comprising means for performing the method of any of Examples 61-73.

[00141] Example 77 includes an authentication server for multifactor threshold authentication, the authentication server comprising a request module to generate a set of messages based on a set of cryptographic system keys; a communication module to (i) transmit the set of messages to a gateway device and (ii) receive an authentication value and parameter

data from the gateway device in response to transmittal of the set of messages to the gateway device, wherein the parameter data is based on sensor data generated by a shareholder device; and an authentication module to determine a validity of one or more messages received from the gateway device based on Lagrange interpolation.

[00142] Example 78 includes the subject matter of Example 77, and wherein to generate the set of messages comprises to generate a message, a , generated according to $a = g^k \bmod p$, wherein p and q are prime numbers such that $p=2q+1$; wherein g is a primitive root of order $q \bmod p$; and wherein k is a random session key used for one round of authentication.

[00143] Example 79 includes the subject matter of any of Examples 77 and 78, and wherein to generate the set of messages comprises to generate a message, b , generated according to $b = my^k \bmod p$, wherein m is a challenge message of the authentication server; wherein y is a public cryptographic key generated according to $y = g^{SK} \bmod p$; and wherein SK is a secret cryptographic key.

[00144] Example 80 includes the subject matter of any of Examples 77-79, and wherein to generate the set of message comprises to generate a set of messages in response to receiving the prime number, p , the primitive root, g , and the public cryptographic key, y , from the gateway device.

[00145] Example 81 includes the subject matter of any of Examples 77-80, and wherein to receive the authentication value comprises to receive an authentication value, ret , determined according to $ret = \frac{b}{a \text{Pr}} \bmod p$, wherein $a \text{Pr} = \prod_{i=1}^k (Part_i)^{(\lambda_{0,ID_i}^{(x)} \lambda_{0,z_1}^{(z)})} \bmod p$; wherein $Part_i$ is a partial authentication message of the shareholder device; and wherein $\lambda_{0,ID_i}^{(x)}$ and $\lambda_{0,z_1}^{(z)}$ are Lagrange coefficients for interpolation of a bivariate polynomial.

[00146] Example 82 includes the subject matter of any of Examples 77-81, and wherein the bivariate polynomial, $F(x,z)$, is such that $\deg_x(F(x,z)) = k-1$, where k is a number of shareholder devices involved in the multifactor threshold authentication; $\deg_z(F(x,z)) = 1$; and $F(0,0) = SK$.

[00147] Example 83 includes the subject matter of any of Examples 77-82, and wherein the communication module is further to receive an authenticator key share, $SS_{Terminal}^{(i)}$,

determined according to $SS_{Terminal}^{(i)} = SS_i(L_{Terminal}) = F(ID_i, L_{Terminal}) = ss_{i1}L_{Terminal} + ss_{i0} \bmod q$, wherein $L_{Terminal}$ is a secret of the authentication server, wherein ID_i is an identifier of the shareholder device; wherein ss_{i1} and ss_{i0} are coefficients; and wherein q is a cryptographic system parameter.

[00148] Example 84 includes the subject matter of any of Examples 77-83, and wherein to determine the validity of the one or more messages comprises to determine whether the challenge message, m , is equal to $ret / \left(\prod_{i=1}^k (a)^{(SS_{Terminal}^i \lambda_{0,ID_i}^{(x)} \lambda_{0,z_2}^{(z)})} \right) \bmod p$.

[00149] Example 85 includes the subject matter of any of Examples 77-84, and wherein at least one of the gateway device or the shareholder device is embodied as a wearable compute device.

[00150] Example 86 includes a method for multifactor threshold authentication by an authentication server, the method comprising generating, by the authentication server, a set of messages based on a set of cryptographic system keys; transmitting, by the authentication server, the set of messages to a gateway device; receiving, by the authentication server, an authentication value and parameter data from the gateway device in response to transmitting the set of messages to the gateway device, wherein the parameter data is based on sensor data generated by a shareholder device; and determining, by the authentication server, a validity of one or more messages received from the gateway device based on Lagrange interpolation.

[00151] Example 87 includes the subject matter of Example 86, and wherein generating the set of messages comprises generating a message, a , generated according to $a = g^k \bmod p$, wherein p and q are prime numbers such that $p=2q+1$; wherein g is a primitive root of order $q \bmod p$; and wherein k is a random session key used for one round of authentication..

[00152] Example 88 includes the subject matter of any of Examples 86 and 87, and wherein generating the set of messages comprises generating a message, b , generated according to $b = my^k \bmod p$, wherein m is a challenge message of the authentication server; wherein y is a public cryptographic key generated according to $y = g^{SK} \bmod p$; and wherein SK is a secret cryptographic key.

[00153] Example 89 includes the subject matter of any of Examples 86-88, and wherein generating the set of message comprises generating a set of messages in response to receiving the

prime number, p , the primitive root, g , and the public cryptographic key, y , from the gateway device.

[00154] Example 90 includes the subject matter of any of Examples 86-89, and wherein receiving the authentication value comprises receiving an authentication value, ret , determined according to $ret = \frac{b}{a \text{Pr}} \bmod p$, wherein $a \text{Pr} = \prod_{i=1}^k (Part_i)^{(\lambda_{0,ID_i}^{(x)} \lambda_{0,z_1}^{(z)})} \bmod p$; wherein $Part_i$ is a partial authentication message of the shareholder device; and wherein $\lambda_{0,ID_i}^{(x)}$ and $\lambda_{0,z_1}^{(z)}$ are Lagrange coefficients for interpolation of a bivariate polynomial.

[00155] Example 91 includes the subject matter of any of Examples 86-90, and wherein the bivariate polynomial, $F(x,z)$, is such that $\deg_x(F(x,z)) = k-1$, where k is a number of shareholder devices involved in the multifactor threshold authentication; $\deg_z(F(x,z)) = 1$; and $F(0,0) = SK$.

[00156] Example 92 includes the subject matter of any of Examples 86-91, and further including receiving, by the authentication server, an authenticator key share, $SS_{Terminal}^{(i)}$, determined according to $SS_{Terminal}^{(i)} = SS_i(L_{Terminal}) = F(ID_i, L_{Terminal}) = ss_{i1}L_{Terminal} + ss_{i0} \bmod q$, wherein $L_{Terminal}$ is a secret of the authentication server, wherein ID_i is an identifier of the shareholder device; wherein ss_{i1} and ss_{i0} are coefficients; and wherein q is a cryptographic system parameter.

[00157] Example 93 includes the subject matter of any of Examples 86-92, and wherein determining the validity of the one or more messages comprises determining whether the challenge message, m , is equal to $ret / \left(\prod_{i=1}^k (a)^{(SS_{Terminal}^{(i)} \lambda_{0,ID_i}^{(x)} \lambda_{0,z_2}^{(z)})} \right) \bmod p$.

[00158] Example 94 includes the subject matter of any of Examples 86-93, and wherein at least one of the gateway device or the shareholder device is embodied as a wearable compute device.

[00159] Example 95 includes a computing device comprising a processor; and a memory having stored therein a plurality of instructions that when executed by the processor cause the computing device to perform the method of any of Examples 86-94.

[00160] Example 96 includes one or more machine-readable storage media comprising a plurality of instructions stored thereon that in response to being executed result in a computing device performing the method of any of Examples 86-94.

[00161] Example 97 includes a computing device comprising means for performing the method of any of Examples 86-94.

[00162] Example 98 includes a gateway device for multifactor threshold authentication, the gateway device comprising means for receiving, from an authentication server, a message generated by the authentication server based on a set of cryptographic system keys; means for transmitting the message to a shareholder device; means for receiving a partial authentication message and parameter data from the shareholder device, wherein the parameter data is based on sensor data generated by the shareholder device and the partial authentication message is based on the parameter data and the message received from the authentication server; and means for determining whether the partial authentication message is valid.

[00163] Example 99 includes the subject matter of Example 98, and wherein the means for receiving the message comprises means for receiving a message generated based on one or more El Gamal cryptographic keys.

[00164] Example 100 includes the subject matter of any of Examples 98 and 99, and wherein the means for receiving the message generated by the authentication server comprises means for receiving a message, a , generated according to $a = g^k \bmod p$, wherein p and q are prime numbers such that $p=2q+1$; wherein g is a primitive root of order $q \bmod p$; and wherein k is a random session key used for one round of authentication.

[00165] Example 101 includes the subject matter of any of Examples 98-100, and wherein the means for receiving the message generated by the authentication server further comprises means for receiving a message, b , generated according to $b = my^k \bmod p$, wherein m is a challenge message of the authentication server; wherein y is a public cryptographic key generated according to $y = g^{SK} \bmod p$; and wherein SK is a secret cryptographic key.

[00166] Example 102 includes the subject matter of any of Examples 98-101, and wherein the means for transmitting the message to the shareholder device comprises means for transmitting the message to each of the shareholder devices involved in the multifactor threshold authentication.

[00167] Example 103 includes the subject matter of any of Examples 98-102, and wherein the means for receiving the partial authentication message comprises means for receiving a partial authentication message, $Part_i$, determined according to $Part_i = a^{SS_i(L_i)} \bmod p$, wherein a is the message generated by the authentication server; wherein L_i is the parameter data; wherein p is a prime number; and wherein $SS_i(\bullet)$ is a shareholder key share of the shareholder device based on an identifier of the shareholder device.

[00168] Example 104 includes the subject matter of any of Examples 98-103, and wherein the means for receiving the partial authentication message further comprises means for receiving a cryptographic signature of the partial authentication message.

[00169] Example 105 includes the subject matter of any of Examples 98-104, and wherein the means for determining whether the partial authentication message is valid comprises means for determining whether the partial authentication message is valid based on the cryptographic signature.

[00170] Example 106 includes the subject matter of any of Examples 98-105, and further including means for initializing the authentication server and the shareholder device for multifactor threshold authentication.

[00171] Example 107 includes the subject matter of any of Examples 98-106, and wherein the means for initializing the authentication server and the shareholder device comprises means for determining one or more system key parameters and the set of cryptographic system keys; means for transmitting the one or more system key parameters to the shareholder device; means for transmitting the one or more system key parameters and a public cryptographic key of the set of cryptographic system keys to the authentication server; means for determining a bivariate polynomial based on a secret key of the set of cryptographic system keys; means for determining a shareholder key share parameter of the shareholder device based on the bivariate polynomial and an identifier of the shareholder device; means for determining an authenticator key share corresponding with the shareholder key share; and means for transmitting the shareholder key share parameter to the shareholder device and the authenticator key share to the authentication device.

[00172] Example 108 includes the subject matter of any of Examples 98-107, and wherein the one or more system key parameters comprises a prime number and a primitive root modulo the prime number.

[00173] Example 109 includes the subject matter of any of Examples 98-108, and wherein the means for determining the set of cryptographic system keys comprises means for determining a secret cryptographic key, SK ; and means for determining the public cryptographic key, y , according to $y = g^{SK} \bmod p$, wherein p and q are prime numbers such that $p=2q+1$; and wherein g is a primitive root of order $q \bmod p$.

[00174] Example 110 includes the subject matter of any of Examples 98-109, and wherein the means for determining the bivariate polynomial comprises means for determining a bivariate polynomial, $F(x, z)$, such that $\deg_x(F(x, z)) = k - 1$, where k is a number of shareholder devices involved in the multifactor threshold authentication; $\deg_z(F(x, z)) = 1$; and $F(0, 0) = SK$.

[00175] Example 111 includes the subject matter of any of Examples 98-110, and further including means for determining coefficients for Lagrange interpolation of a bivariate polynomial that involves the parameter data in response to determining the partial authentication message is valid; means for determining an authentication value based on the coefficients; and means for transmitting the authentication value to the authentication server.

[00176] Example 112 includes the subject matter of any of Examples 98-111, and wherein the means for determining the authentication value comprises means for determining an authentication value, ret , according to $ret = \frac{b}{aPr} \bmod p$, wherein

$aPr = \prod_{i=1}^k (Part_i)^{(\lambda_{0, ID_i}^{(x)} \lambda_{0, z_1}^{(z)})} \bmod p$; wherein $Part_i$ is the partial authentication message; and wherein $\lambda_{0, ID_i}^{(x)}$ and $\lambda_{0, z_1}^{(z)}$ are Lagrange coefficients for interpolation of $F(0, 0)$.

[00177] Example 113 includes the subject matter of any of Examples 98-112, and wherein the means for determining the shareholder key share parameter comprises means for determining a shareholder key share parameter, $SS_i(z)$, according to $SS_i(z) = F(x = ID_i, z) = F_i(z) = ss_{i1}z + ss_{i0} \bmod q$ based on the bivariate polynomial, wherein ID_i is the identifier of the shareholder device; wherein ss_{i1} and ss_{i0} are coefficients; and wherein q is a cryptographic system parameter.

[00178] Example 114 includes the subject matter of any of Examples 98-113, and wherein the shareholder key share parameter is represented as a vector of the coefficients ss_{i1} and ss_{i0} .

[00179] Example 115 includes the subject matter of any of Examples 98-114, and further including means for determining a set of verification keys for the shareholder device based on the bivariate polynomial.

[00180] Example 116 includes the subject matter of any of Examples 98-115, and wherein the means for determining the set of verification keys comprises means for determining a pair of verification keys, VK_i , such that $VK_i = \{v^{ss_{i1}}, v^{ss_{i0}}\}$ and v is a primitive root of the order $q \bmod p$.

[00181] Example 117 includes the subject matter of any of Examples 98-116, and wherein the means for determining whether the partial authentication message is valid comprises means for determining whether the partial authentication message is valid based on the pair of verification keys.

[00182] Example 118 includes the subject matter of any of Examples 98-117, and further including means for requesting data from another shareholder device in response to a determination that the partial authentication message of the shareholder device is not valid.

[00183] Example 119 includes the subject matter of any of Examples 98-118, and wherein the gateway device is embodied as a wearable compute device.

[00184] Example 120 includes a shareholder device for multifactor threshold authentication, the shareholder device comprising means for receiving, from a gateway device, a message determined based on a set of cryptographic system keys; means for determining parameter data based on sensor data generated by one or more sensors of the shareholder device; means for generating a partial authentication message based on the parameter data and the message received from the gateway device; means for generating a validation signature of the partial authentication message; and means for transmitting the partial authentication message, the parameter data, and the validation signature to the gateway device for multifactor threshold authentication.

[00185] Example 121 includes the subject matter of Example 120, and wherein the means for receiving the message comprises means for receiving a message, a , generated according to $a = g^k \bmod p$, wherein p and q are prime numbers such that $p=2q+1$; wherein g is a primitive

root of order $q \bmod p$; and wherein k is a random session key used for one round of authentication.

[00186] Example 122 includes the subject matter of any of Examples 120 and 121, and further including means for receiving the prime number, p , and the primitive root, g , from the gateway device.

[00187] Example 123 includes the subject matter of any of Examples 120-122, and wherein the means for generating the partial authentication message comprises means for generating a partial authentication message, $Part_i$, according to $Part_i = a^{SS_i(L_i)} \bmod p$, wherein a is the message received from the gateway device; wherein L_i is the parameter data; wherein p is a prime number; and wherein $SS_i(\bullet)$ is a shareholder key share of the shareholder device based on an identifier of the shareholder device.

[00188] Example 124 includes the subject matter of any of Examples 120-123, and wherein the means for generating the validation signature comprises means for generating a validation signature, VV_i , according to $VV_i = VV_{i,1}, VV_{i,2}$, wherein $VV_{i,1} = Hash(v, a, v^{SS_i(L_i)} \bmod p, Part_i, v^r \bmod p, a^r \bmod p)$; wherein $VV_{i,2} = SS_i(L_i) * VV_{i,1} + r$; and wherein v is a primitive root of the order $q \bmod p$ and r is an integer mod p .

[00189] Example 125 includes the subject matter of any of Examples 120-124, and further including means for receiving the shareholder key share parameter, SS_i , from the gateway device, wherein SS_i is determined according to $SS_i(z) = F(x = ID_i, z) = F_i(z) = ss_{i1}z + ss_{i0} \bmod q$ based on a bivariate polynomial, $F(x, z)$; wherein ID_i is the identifier of the shareholder device; wherein ss_{i1} and ss_{i0} are coefficients; and wherein q is a cryptographic system parameter.

[00190] Example 126 includes the subject matter of any of Examples 120-125, and wherein the bivariate polynomial, $F(x, z)$, is determined such that $\deg_x(F(x, z)) = k - 1$, where k is a number of shareholder devices involved in the multifactor threshold authentication; $\deg_z(F(x, z)) = 1$; and $F(0, 0) = SK$, wherein SK is a secret cryptographic key determined by the gateway device.

[00191] Example 127 includes the subject matter of any of Examples 120-126, and wherein the shareholder key share parameter is represented as a vector of the coefficients ss_{i1} and ss_{i0} .

[00192] Example 128 includes the subject matter of any of Examples 120-127, and further including means for receiving one or more initialization messages from the gateway device for initialization of the multifactor threshold authentication.

[00193] Example 129 includes the subject matter of any of Examples 120-128, and wherein the means for determining the parameter data comprises means for determining a biometric parameter of a user of the shareholder device based on the sensor data.

[00194] Example 130 includes the subject matter of any of Examples 120-129, and wherein the means for determining the parameter data comprises means for determining a location of the shareholder device relative to a user of the shareholder device based on the sensor data.

[00195] Example 131 includes the subject matter of any of Examples 120-130, and wherein the means for determining the parameter data comprises means for determining an inertial characteristic of the shareholder device.

[00196] Example 132 includes the subject matter of any of Examples 120-131, and wherein the shareholder device is embodied as a wearable compute device.

[00197] Example 133 includes an authentication server for multifactor threshold authentication, the authentication server comprising means for generating a set of messages based on a set of cryptographic system keys; means for transmitting the set of messages to a gateway device; means for receiving an authentication value and parameter data from the gateway device in response to transmittal of the set of messages to the gateway device, wherein the parameter data is based on sensor data generated by a shareholder device; and means for determining a validity of one or more messages received from the gateway device based on Lagrange interpolation.

[00198] Example 134 includes the subject matter of Example 133, and wherein the means for generating the set of messages comprises means for generating a message, a , generated according to $a = g^k \bmod p$, wherein p and q are prime numbers such that $p=2q+1$; wherein g is a

primitive root of order $q \bmod p$; and wherein k is a random session key used for one round of authentication..

[00199] Example 135 includes the subject matter of any of Examples 133 and 134, and wherein the means for generating the set of messages comprises means for generating a message, b , generated according to $b = my^k \bmod p$, wherein m is a challenge message of the authentication server; wherein y is a public cryptographic key generated according to $y = g^{SK} \bmod p$; and wherein SK is a secret cryptographic key.

[00200] Example 136 includes the subject matter of any of Examples 133-135, and wherein the means for generating the set of message comprises means for generating a set of messages in response to receiving the prime number, p , the primitive root, g , and the public cryptographic key, y , from the gateway device.

[00201] Example 137 includes the subject matter of any of Examples 133-136, and wherein the means for receiving the authentication value comprises means for receiving an authentication value, ret , determined according to $ret = \frac{b}{a \text{Pr}} \bmod p$, wherein

$a \text{Pr} = \prod_{i=1}^k (Part_i)^{(\lambda_{0,ID_i}^{(x)} \lambda_{0,z_1}^{(z)})} \bmod p$; wherein $Part_i$ is a partial authentication message of the shareholder device; and wherein $\lambda_{0,ID_i}^{(x)}$ and $\lambda_{0,z_1}^{(z)}$ are Lagrange coefficients for interpolation of a bivariate polynomial.

[00202] Example 138 includes the subject matter of any of Examples 133-137, and wherein the bivariate polynomial, $F(x, z)$, is such that $\deg_x(F(x, z)) = k - 1$, where k is a number of shareholder devices involved in the multifactor threshold authentication; $\deg_z(F(x, z)) = 1$; and $F(0, 0) = SK$.

[00203] Example 139 includes the subject matter of any of Examples 133-138, and further including means for receiving an authenticator key share, $SS_{Terminal}^{(i)}$, determined according to $SS_{Terminal}^{(i)} = SS_i(L_{Terminal}) = F(ID_i, L_{Terminal}) = ss_{i1}L_{Terminal} + ss_{i0} \bmod q$, wherein $L_{Terminal}$ is a secret of the authentication server, wherein ID_i is an identifier of the shareholder device; wherein ss_{i1} and ss_{i0} are coefficients; and wherein q is a cryptographic system parameter.

[00204] Example 140 includes the subject matter of any of Examples 133-139, and wherein the means for determining the validity of the one or more messages comprises means for determining whether the challenge message, m , is equal to $ret / \left(\prod_{i=1}^k (a)^{(SS_{Terminal}^i \lambda_{0, ID_i}^{(x)} \lambda_{0, z_2}^{(z)})} \right) \bmod p$.

[00205] Example 141 includes the subject matter of any of Examples 133-140, and wherein at least one of the gateway device or the shareholder device is embodied as a wearable compute device.

CLAIMS:

1. A gateway device for multifactor threshold authentication, the gateway device comprising:

a communication module to (i) receive, from an authentication server, a message generated by the authentication server based on a set of cryptographic system key, (ii) transmit the message to a shareholder device, and (iii) receive a partial authentication message and parameter data from the shareholder device, wherein the parameter data is based on sensor data generated by the shareholder device and the partial authentication message is based on the parameter data and the message received from the authentication server; and

an authentication module to determine whether the partial authentication message is valid.

2. The gateway device of claim 1, wherein to receive the message generated by the authentication server comprises to receive a message, a , generated according to $a = g^k \bmod p$,

wherein p and q are prime numbers such that $p=2q+1$;

wherein g is a primitive root of order $q \bmod p$; and

wherein k is a random session key used for one round of authentication.

3. The gateway device of claim 2, wherein to receive the message generated by the authentication server further comprises to receive a message, b , generated according to $b = my^k \bmod p$,

wherein m is a challenge message of the authentication server;

wherein y is a public cryptographic key generated according to $y = g^{SK} \bmod p$;

and

wherein SK is a secret cryptographic key.

4. The gateway device of claim 2, wherein to transmit the message to the shareholder device comprises to transmit the message to each of the shareholder devices involved in the multifactor threshold authentication.

5. The gateway device of claim 1, wherein to receive the partial authentication message comprises to receive a partial authentication message, $Part_i$, determined according to $Part_i = a^{SS_i(L_i)} \bmod p$,

wherein a is the message generated by the authentication server;

wherein L_i is the parameter data;

wherein p is a prime number; and

wherein $SS_i(\bullet)$ is a shareholder key share of the shareholder device based on an identifier of the shareholder device.

6. The gateway device of claim 1, wherein to receive the partial authentication message further comprises to receive a cryptographic signature of the partial authentication message.

7. The gateway device of claim 6, wherein to determine whether the partial authentication message is valid comprises to determine whether the partial authentication message is valid based on the cryptographic signature; and

wherein the gateway device is embodied as a wearable compute device.

8. A method for multifactor threshold authentication by a gateway device, the method comprising:

receiving, by the gateway device and from an authentication server, a message generated by the authentication server based on a set of cryptographic system keys;

transmitting, by the gateway device, the message to a shareholder device;

receiving, by the gateway device, a partial authentication message and parameter data from the shareholder device, wherein the parameter data is based on sensor data generated by the shareholder device and the partial authentication message is based on the parameter data and the message received from the authentication server; and

determining, by the gateway device, whether the partial authentication message is valid.

9. The method of claim 8, further comprising initializing, by the gateway device, the authentication server and the shareholder device for multifactor threshold authentication by:

determining, by the gateway device, one or more system key parameters and the set of cryptographic system keys;

transmitting, by the gateway device, the one or more system key parameters to the shareholder device;

transmitting, by the gateway device, the one or more system key parameters and a public cryptographic key of the set of cryptographic system keys to the authentication server;

determining, by the gateway device, a bivariate polynomial based on a secret key of the set of cryptographic system keys;

determining, by the gateway device, a shareholder key share parameter of the shareholder device based on the bivariate polynomial and an identifier of the shareholder device;

determining, by the gateway device, an authenticator key share corresponding with the shareholder key share; and

transmitting, by the gateway device, the shareholder key share parameter to the shareholder device and the authenticator key share to the authentication device.

10. The method of claim 9, wherein the one or more system key parameters comprises a prime number and a primitive root modulo the prime number;

wherein determining the set of cryptographic system keys comprises (i) determining a secret cryptographic key, SK , and (ii) determining the public cryptographic key, y , according to $y = g^{SK} \bmod p$,

wherein p and q are prime numbers such that $p=2q+1$; and

wherein g is a primitive root of order $q \bmod p$.

11. The method of claim 10, wherein determining the bivariate polynomial comprises determining a bivariate polynomial, $F(x, z)$, such that:

$\deg_x(F(x, z)) = k - 1$, where k is a number of shareholder devices involved in the multifactor threshold authentication;

$\deg_z(F(x, z)) = 1$; and

$F(0, 0) = SK$.

12. The method of claim 11, further comprising:

determining, by the gateway device, coefficients for Lagrange interpolation of a bivariate polynomial that involves the parameter data in response to determining the partial authentication message is valid;

determining, by the gateway device, an authentication value based on the coefficients; and

transmitting, by the gateway device, the authentication value to the authentication server.

13. The method of claim 12, wherein determining the authentication value comprises determining an authentication value, ret , according to $ret = \frac{b}{a \text{ Pr}} \bmod p$,

wherein $a \text{ Pr} = \prod_{i=1}^k (Part_i)^{(\lambda_{0, ID_i}^{(x)} \lambda_{0, z_1}^{(z)})} \bmod p$;

wherein $Part_i$ is the partial authentication message; and

wherein $\lambda_{0, ID_i}^{(x)}$ and $\lambda_{0, z_1}^{(z)}$ are Lagrange coefficients for interpolation of $F(0, 0)$.

14. The method of claim 11, wherein determining the shareholder key share parameter comprises determining a shareholder key share parameter, $SS_i(z)$, according to $SS_i(z) = F(x = ID_i, z) = F_i(z) = ss_{i1}z + ss_{i0} \bmod q$ based on the bivariate polynomial,

wherein ID_i is the identifier of the shareholder device;

wherein ss_{i1} and ss_{i0} are coefficients; and

wherein q is a cryptographic system parameter.

15. The method of claim 14, further comprising determining a pair of verification keys, VK_i , for the shareholder device based on the bivariate polynomial such that $VK_i = \{v^{ss_{i1}}, v^{ss_{i0}}\}$ and v is a primitive root of the order $q \bmod p$; and

wherein determining whether the partial authentication message is valid comprises determining whether the partial authentication message is valid based on the pair of verification keys.

16. One or more machine-readable storage media comprising a plurality of instructions stored thereon that in response to being executed result in a computing device performing the method of any of claims 9-15.

17. A method for multifactor threshold authentication by a shareholder device, the method comprising:

receiving, by the shareholder device and from a gateway device, a message determined based on a set of cryptographic system keys;

determining, by the shareholder device, parameter data based on sensor data generated by one or more sensors of the shareholder device;

generating, by the shareholder device, a partial authentication message based on the parameter data and the message received from the gateway device;

generating, by the shareholder device, a validation signature of the partial authentication message; and

transmitting, by the shareholder device, the partial authentication message, the parameter data, and the validation signature to the gateway device for multifactor threshold authentication.

18. The method of claim 17, wherein generating the partial authentication message comprises generating a partial authentication message, $Part_i$, according to $Part_i = a^{ss_i(L_i)} \bmod p$,

wherein a is the message received from the gateway device;

wherein L_i is the parameter data;

wherein p is a prime number; and

wherein $SS_i(\bullet)$ is a shareholder key share of the shareholder device based on an identifier of the shareholder device.

19. The method of claim 18, wherein generating the validation signature comprises generating a validation signature, VV_i , according to $VV_i = VV_{i,1}, VV_{i,2}$,

wherein $VV_{i,1} = \text{Hash}(v, a, v^{SS_i(L_i)} \bmod p, Part_i, v^r \bmod p, a^r \bmod p)$;

wherein $VV_{i,2} = SS_i(L_i) * VV_{i,1} + r$; and

wherein v is a primitive root of the order $q \bmod p$ and r is an integer $\bmod p$.

20. The method of claim 18, further comprising receiving, by the shareholder device, the shareholder key share parameter, SS_i , from the gateway device, wherein SS_i is determined according to $SS_i(z) = F(x = ID_i, z) = F_i(z) = ss_{i1}z + ss_{i0} \bmod q$ based on a bivariate polynomial, $F(x, z)$;

wherein ID_i is the identifier of the shareholder device;

wherein ss_{i1} and ss_{i0} are coefficients; and

wherein q is a cryptographic system parameter.

21. The method of claim 20, wherein the bivariate polynomial, $F(x, z)$, is determined such that:

$\deg_x(F(x, z)) = k - 1$, where k is a number of shareholder devices involved in the multifactor threshold authentication;

$\deg_z(F(x, z)) = 1$; and

$F(0, 0) = SK$, wherein SK is a secret cryptographic key determined by the gateway device.

22. The method of claim 17, wherein determining the parameter data comprises determining, based on the sensor data, at least one of (i) a biometric parameter of a

user of the shareholder device, (ii) a location of the shareholder device relative to a user of the shareholder device, or (iii) an inertial characteristic of the shareholder device.

23. One or more machine-readable storage media comprising a plurality of instructions stored thereon that in response to being executed result in a computing device performing the method of any of claims 17-22.

24. A method for multifactor threshold authentication by an authentication server, the method comprising:

generating, by the authentication server, a set of messages based on a set of cryptographic system keys;

transmitting, by the authentication server, the set of messages to a gateway device;

receiving, by the authentication server, an authentication value and parameter data from the gateway device in response to transmitting the set of messages to the gateway device, wherein the parameter data is based on sensor data generated by a shareholder device; and

determining, by the authentication server, a validity of one or more messages received from the gateway device based on Lagrange interpolation.

25. The method of claim 24, wherein generating the set of messages comprises (i) generating a message, a , generated according to $a = g^k \bmod p$ and (ii) generating a message, b , generated according to $b = my^k \bmod p$,

wherein p and q are prime numbers such that $p=2q+1$;

wherein g is a primitive root of order $q \bmod p$;

wherein k is a random session key used for one round of authentication;

wherein m is a challenge message of the authentication server;

wherein y is a public cryptographic key generated according to $y = g^{SK} \bmod p$;

and

wherein SK is a secret cryptographic key.

26. The method of claim 25, wherein receiving the authentication value comprises receiving an authentication value, ret , determined according to $ret = \frac{b}{a \text{Pr}} \bmod p$,

$$\text{wherein } a \text{Pr} = \prod_{i=1}^k (Part_i)^{(\lambda_{0,ID_i}^{(x)} \lambda_{0,z_1}^{(z)})} \bmod p;$$

wherein $Part_i$ is a partial authentication message of the shareholder device; and

wherein $\lambda_{0,ID_i}^{(x)}$ and $\lambda_{0,z_1}^{(z)}$ are Lagrange coefficients for interpolation of a bivariate polynomial.

27. The method of claim 26, wherein the bivariate polynomial, $F(x,z)$, is such that:

$\deg_x(F(x,z)) = k-1$, where k is a number of shareholder devices involved in the multifactor threshold authentication;

$$\deg_z(F(x,z)) = 1; \text{ and}$$

$$F(0,0) = SK.$$

28. The method of claim 27, further comprising receiving, by the authentication server, an authenticator key share, $SS_{Terminal}^{(i)}$, determined according to $SS_{Terminal}^{(i)} = SS_i(L_{Terminal}) = F(ID_i, L_{Terminal}) = ss_{i1}L_{Terminal} + ss_{i0} \bmod q$,

wherein $L_{Terminal}$ is a secret of the authentication server,

wherein ID_i is an identifier of the shareholder device;

wherein ss_{i1} and ss_{i0} are coefficients; and

wherein q is a cryptographic system parameter.

29. The method of claim 28, wherein determining the validity of the one or more messages comprises determining whether the challenge message, m , is equal to

$$ret / \left(\prod_{i=1}^k (a)^{(SS_{Terminal}^{(i)} \lambda_{0,ID_i}^{(x)} \lambda_{0,z_2}^{(z)})} \right) \bmod p.$$

30. One or more machine-readable storage media comprising a plurality of instructions stored thereon that in response to being executed result in a computing device performing the method of any of claims 24-29.

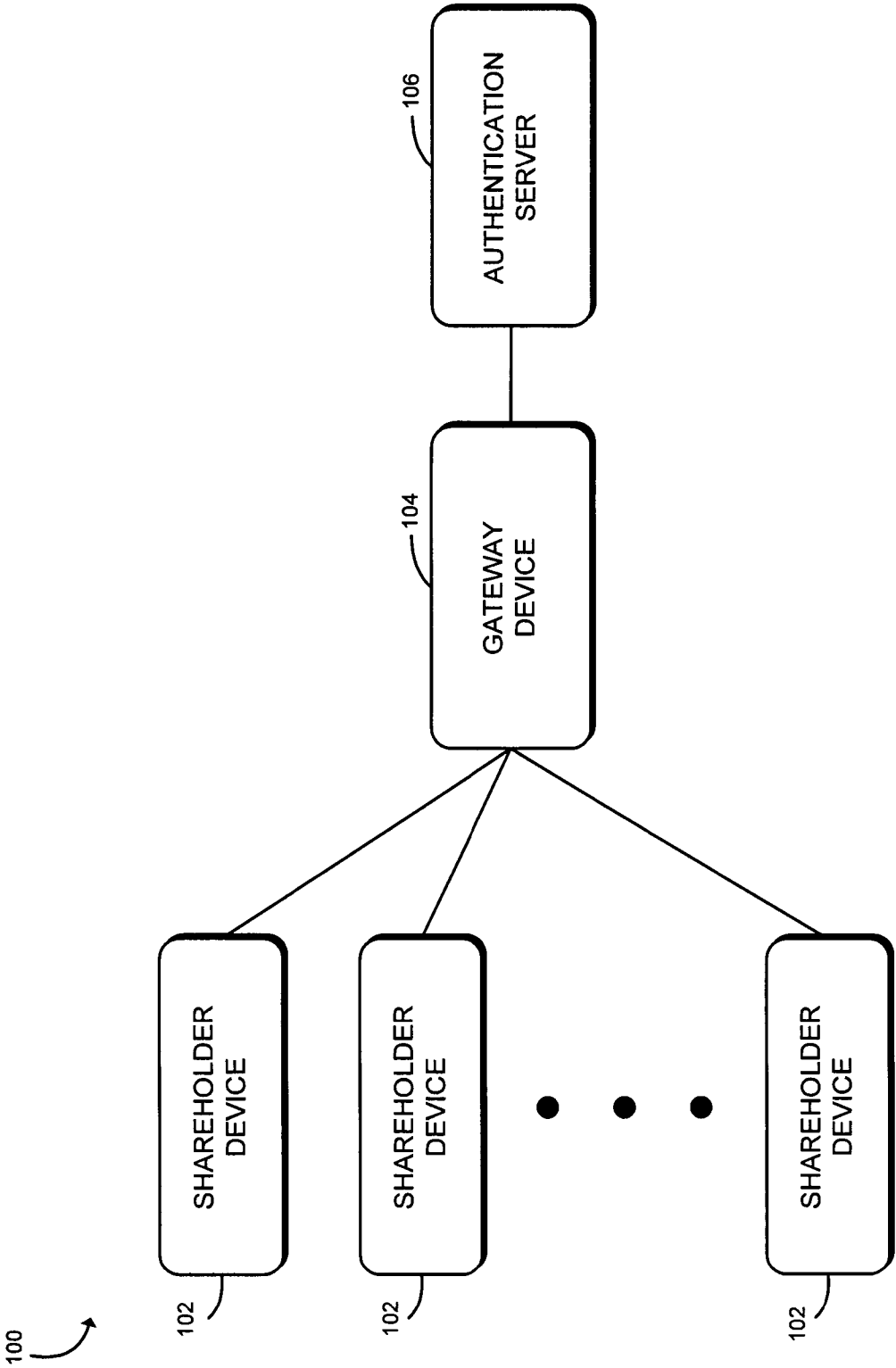


FIG. 1

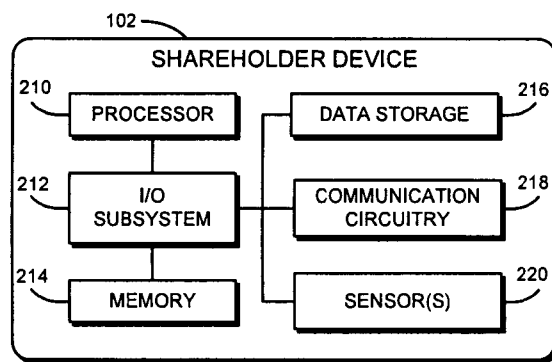


FIG. 2

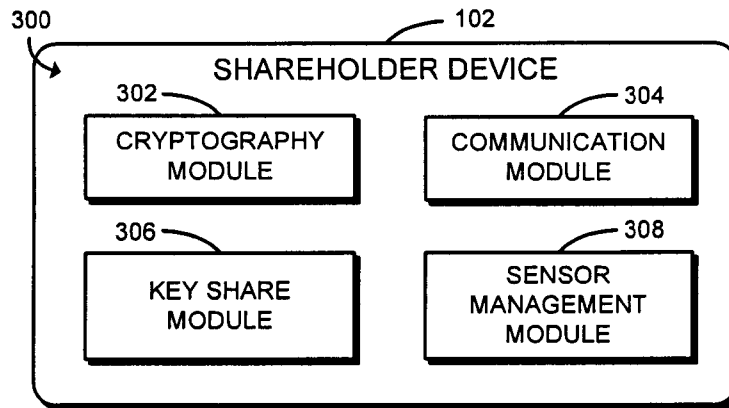


FIG. 3

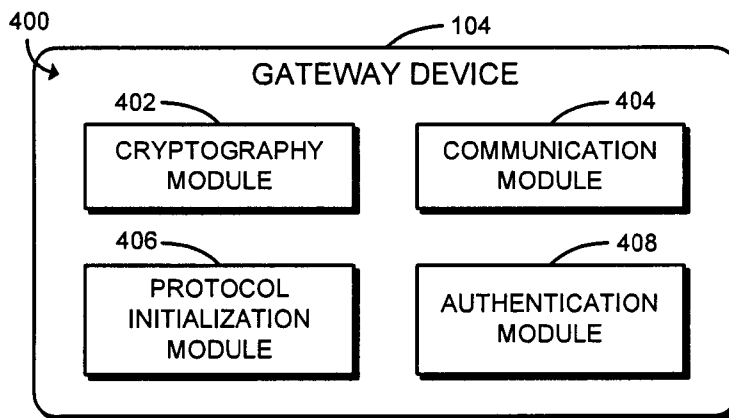


FIG. 4

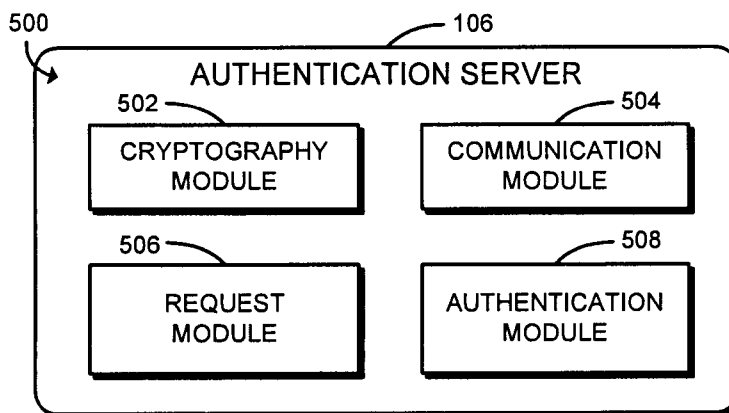


FIG. 5

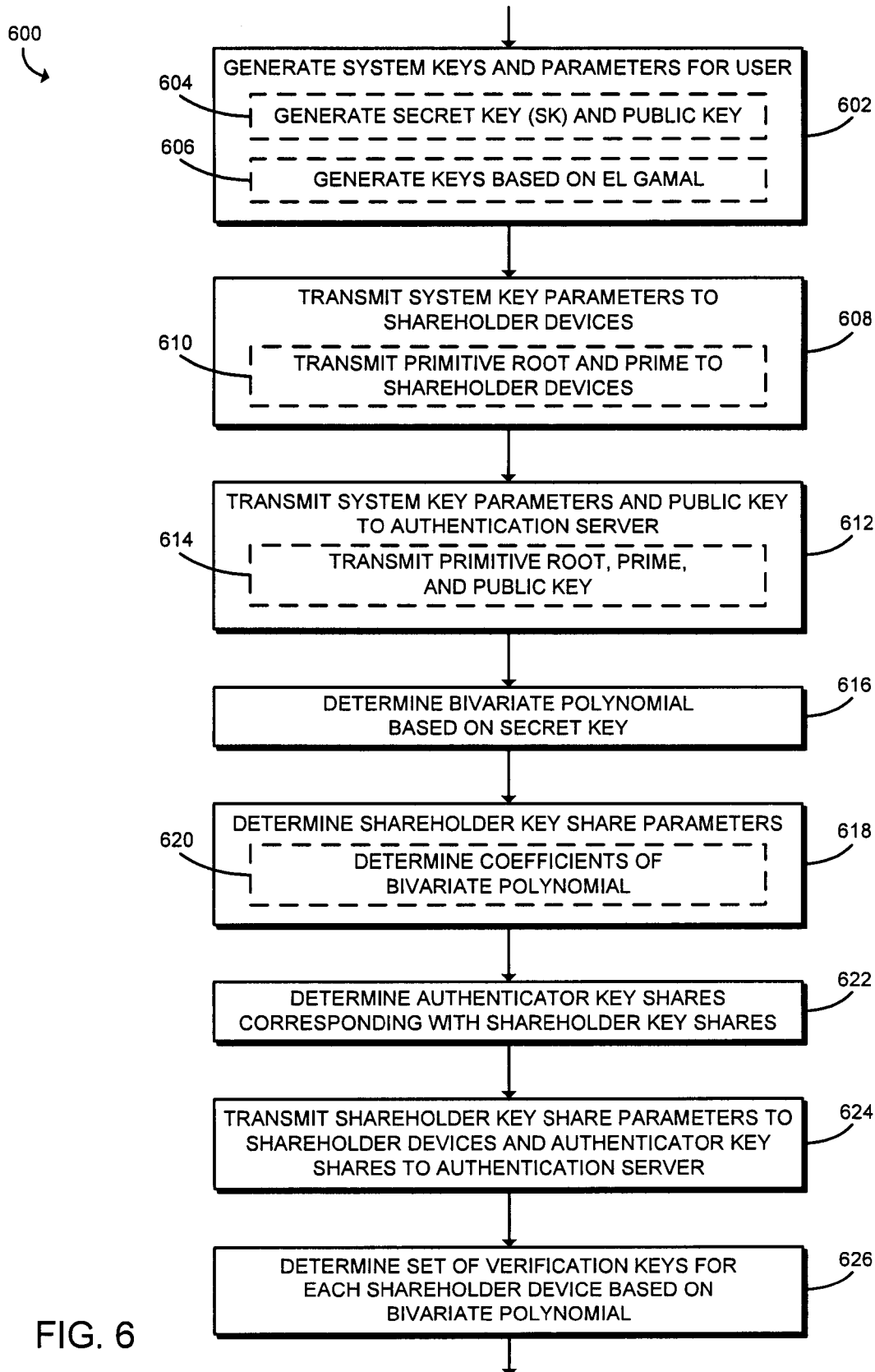


FIG. 6

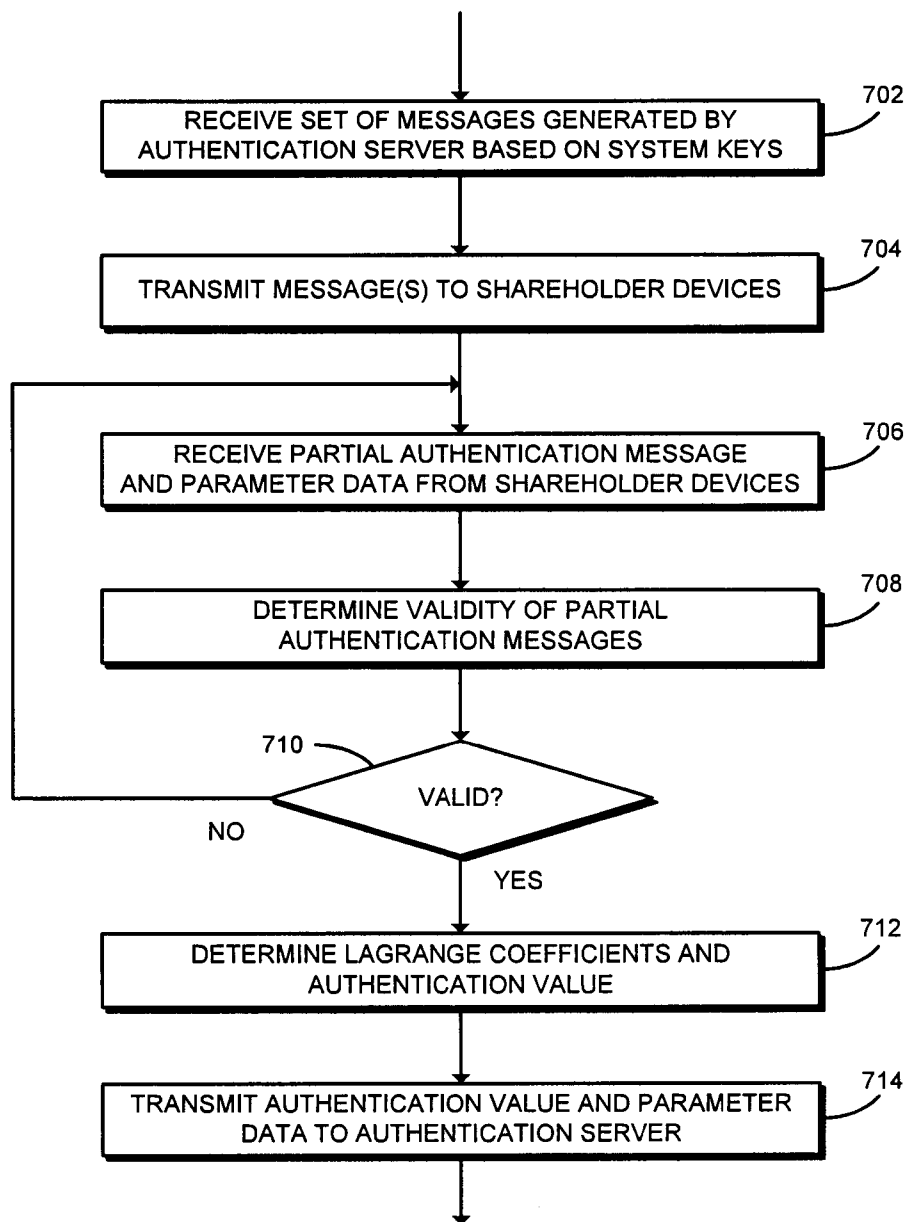
700
↘

FIG. 7

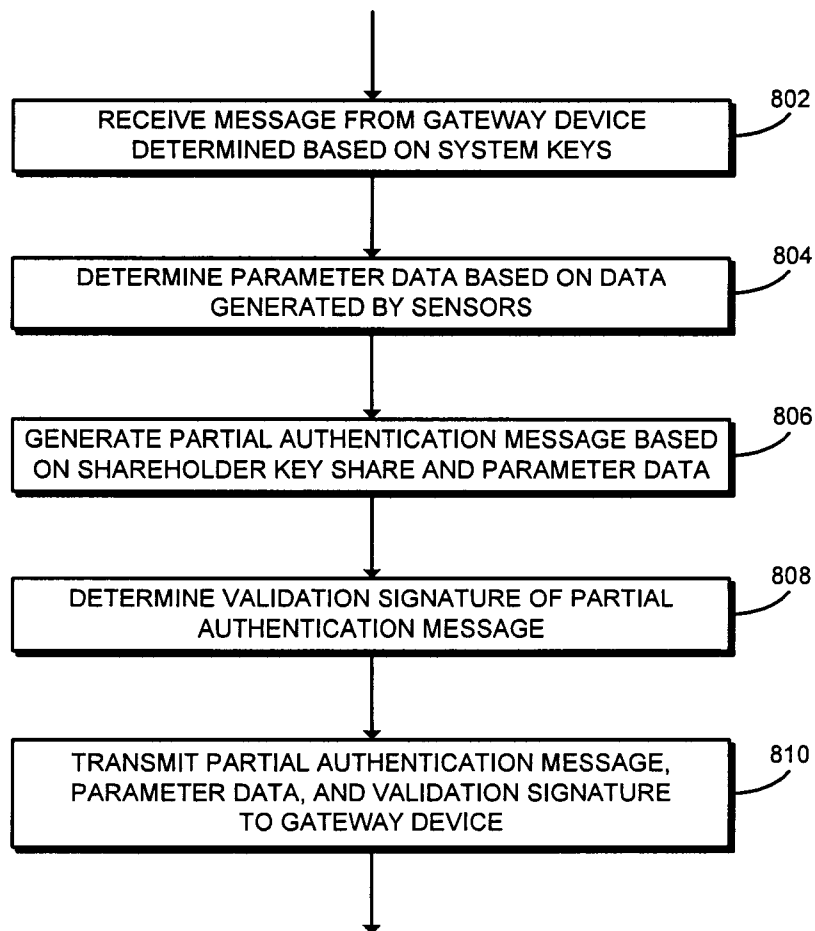
800
↓

FIG. 8

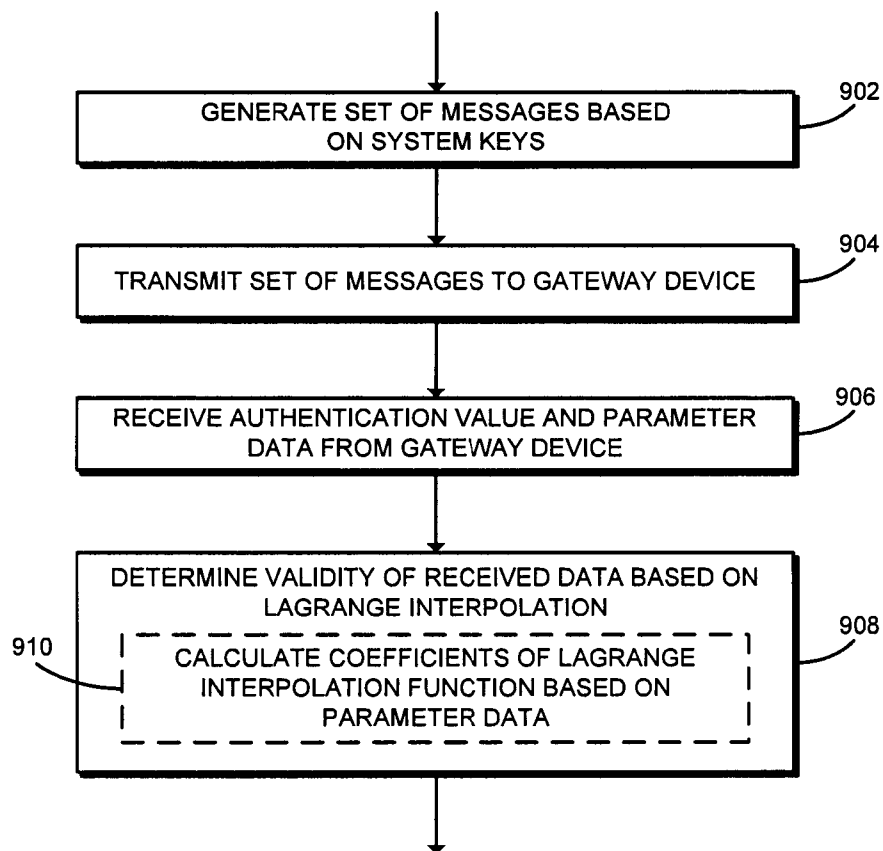
900
↘

FIG. 9

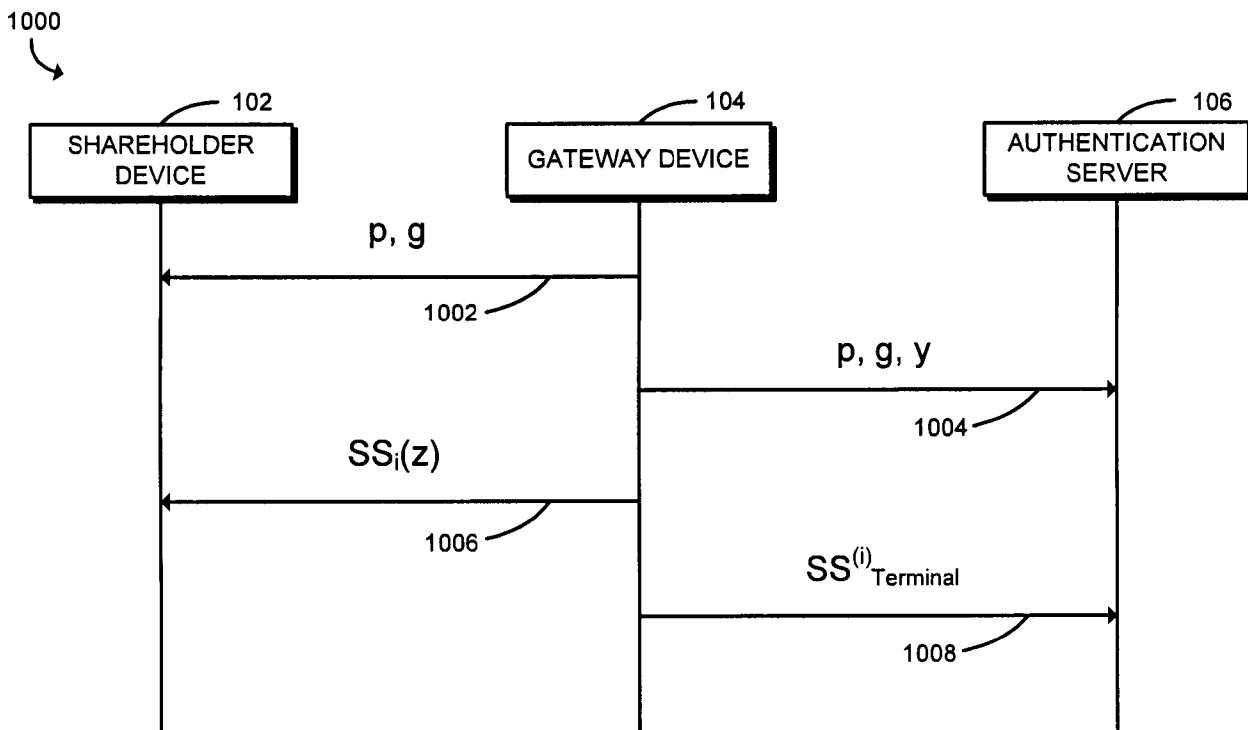


FIG. 10

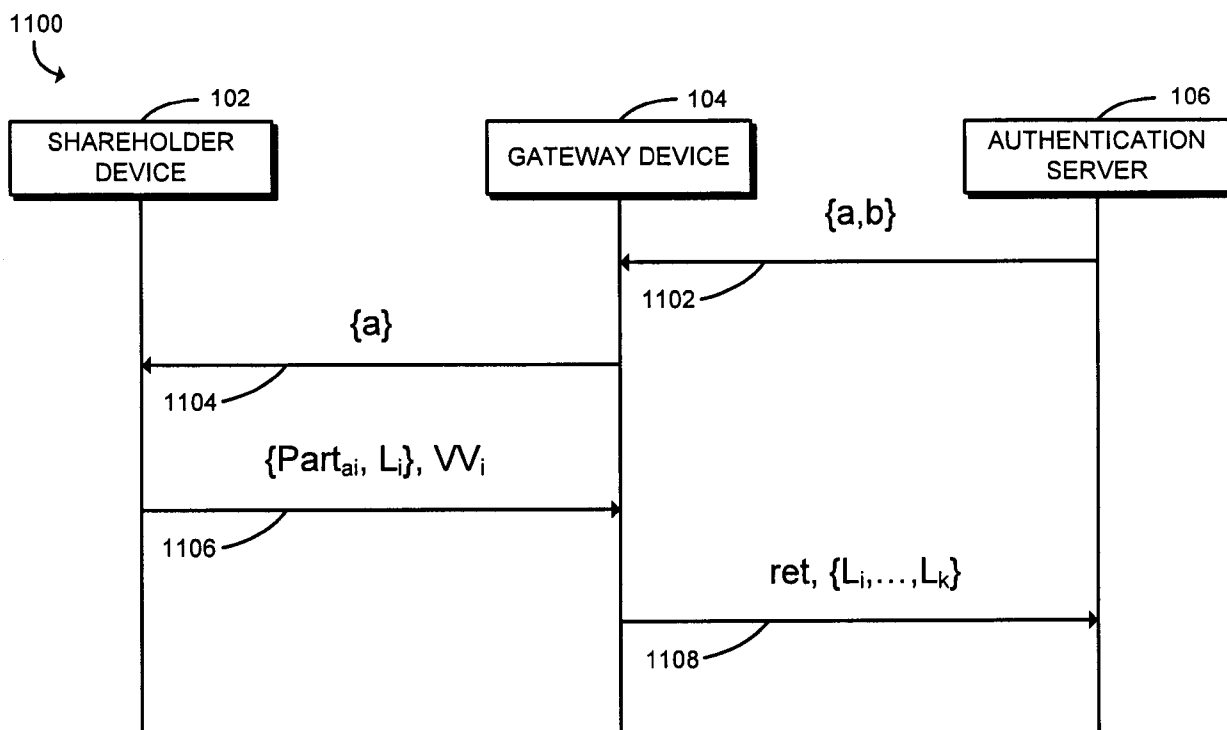


FIG. 11

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2016/000548

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L9/08 H04L9/32
ADD.

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

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04L

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

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

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6 055 508 A (NAOR MONI [IL] ET AL) 25 April 2000 (2000-04-25) column 8, line 63 - column 9, line 25; figure 1 column 12, line 54 - column 13, line 33 -----	1-30
X	GB 2 513 260 A (TOMLINSON MARTIN [GB]; CHENG ANDERSEN [GB]; TIHAI CEN JUNG [GB]) 22 October 2014 (2014-10-22) paragraphs [0045] - [0047], [0096] -----	1-30
X	US 2014/359290 A1 (MCCUSKER KEALAN [GB] ET AL) 4 December 2014 (2014-12-04) paragraphs [0267] - [0285] -----	1-30



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search

1 December 2016

Date of mailing of the international search report

09/12/2016

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Manet, Pascal

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/IB2016/000548

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6055508	A	25-04-2000	NONE

GB 2513260	A	22-10-2014	GB 2513260 A 22-10-2014
			GB 2520446 A 20-05-2015
			US 2015378842 A1 31-12-2015

US 2014359290	A1	04-12-2014	NONE
