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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
02 January 2025 (02.01.2025)

WIPO | PCT

(10) International Publication Number
WO 2025/005916 A1

(51) International Patent Classification:
G06F 21/31 (2013.01) *G06F 21/55* (2013.01)
G06F 21/50 (2013.01) *G06F 21/62* (2013.01)

(21) International Application Number:
PCT/US2023/026515

(22) International Filing Date:
29 June 2023 (29.06.2023)

(25) Filing Language: English

(26) Publication Language: English

(71) Applicant: **VISA INTERNATIONAL SERVICE ASSOCIATION** [US/US]; P.O. Box 8999, San Francisco, California 94128 (US).

(72) Inventor: **RATICA, Adam, Grant**; 7804 Chillicothe Road, Mentor, Ohio 44060 (US).

(74) Agent: **PREPELKA, Nathan, J.** et al.; The Webb Law Firm, One Gateway Center, 420 Ft. Duquesne Blvd., Suite 1200, Pittsburgh, Pennsylvania 15222 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CV, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IQ, IR, IS, IT, JM, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, MG, MK, MN, MU, 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, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, WS, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, CV, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SC, SD, SL, ST, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ,

(54) Title: SYSTEM, METHOD, AND COMPUTER PROGRAM PRODUCT FOR BOT DETERRENCE USING CRYPTOGRAPHY

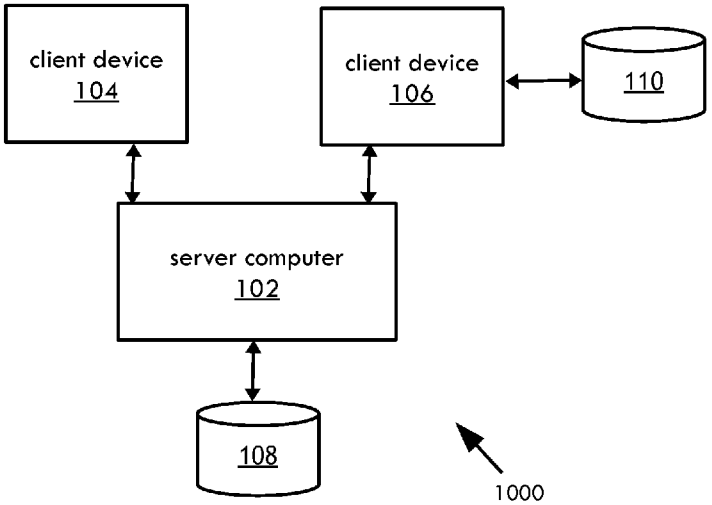

FIG. 1

(57) Abstract: Systems, methods, and computer program products for bot deterrence using cryptography are provided. A system includes at least one processor programmed or configured to, in response to a first request, determine a Proof-of-Work cryptographic challenge corresponding to at least one key, communicate the Proof-of-Work cryptographic challenge to the first client device, receive, from the first client device, a first solution to the Proof-of-Work cryptographic challenge, validate the first request for data based on the first solution to the Proof-of-Work cryptographic challenge, receive a second request from a second client device, communicate the Proof-of-Work cryptographic challenge to the second client device, receive, from the second client device, a second solution to the Proof-of-Work cryptographic challenge, the second solution based on at least a portion of the at least one key, and validate the second request for data based on the second solution to the Proof-of-Work cryptographic challenge.

WO 2025/005916 A1

[Continued on next page]

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, ME, 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))*

SYSTEM, METHOD, AND COMPUTER PROGRAM PRODUCT FOR BOT DETERRENCE USING CRYPTOGRAPHY

BACKGROUND

1. Field

[0001] This disclosure relates generally to cryptography and, in some non-limiting embodiments or aspects, to systems, methods, and computer program products for bot deterrence using cryptography.

2. Technical Considerations

[0002] Servers that provide information, access to systems, or services to client devices are vulnerable to attacks from automated bots. For example, a bot may use brute force password cracking methods to breach a user's account. In other examples, a bot may iteratively attempt to find active payment account identifiers through a payment processing platform. Existing solutions use rate limiting methods that limit the amount of requests that a client device can make in a time period. However, such rate limiting methods can be compromised with multiple devices, spoofing techniques, and by automatically spacing out the requests.

SUMMARY

[0003] According to non-limiting embodiments or aspects, provided is a system comprising at least one processor programmed or configured to: receive a first request from a first client device; in response to the first request, determine a Proof-of-Work cryptographic challenge corresponding to at least one key; communicate the Proof-of-Work cryptographic challenge to the first client device; receive, from the first client device, a first solution to the Proof-of-Work cryptographic challenge; validate the first request for data based on the first solution to the Proof-of-Work cryptographic challenge; receive a second request from a second client device; communicate the Proof-of-Work cryptographic challenge to the second client device; receive, from the second client device, a second solution to the Proof-of-Work cryptographic challenge, the second solution based on at least a portion of the at least one key; and validate the second request for data based on the second solution to the Proof-of-Work cryptographic challenge.

[0004] In non-limiting embodiments or aspects, the at least one processor is further configured to communicate the at least a portion of the at least one key to the second client device, the first client device does not have access to the at least one key. In non-limiting embodiments or aspects, wherein determining the Proof-of-Work

cryptographic challenge based on the first request comprises: determining a challenge difficulty based on data associated with the first client device; and modifying a computational complexity of the Proof-of-Work cryptographic challenge based on the challenge difficulty. In non-limiting embodiments or aspects, the data associated with the first client device comprises a risk score corresponding to at least one of the following: an account holder associated with the first client device, an account identifier associated with the first client device, a network address of the first client device, a device identifier of the first client device, or any combination thereof. In non-limiting embodiments or aspects, the at least a portion of the at least one key comprises the at least one key or a partial key. In non-limiting embodiments or aspects, the first client device comprises a production system, and the second client device comprises a testing system. In non-limiting embodiments or aspects, the Proof-of-Work cryptographic challenge comprises a client-side script.

[0005] According to non-limiting embodiments or aspects, provided is a method comprising: receiving, with at least one processor, a first request from a first client device; in response to the first request, determining, with at least one processor, a Proof-of-Work cryptographic challenge corresponding to at least one key; communicating the Proof-of-Work cryptographic challenge to the first client device; receiving, from the first client device, a first solution to the Proof-of-Work cryptographic challenge; validating, with at least one processor, the first request for data based on the first solution to the Proof-of-Work cryptographic challenge; receiving, with at least one processor, a second request from a second client device; communicating the Proof-of-Work cryptographic challenge to the second client device; receiving, from the second client device, a second solution to the Proof-of-Work cryptographic challenge, the second solution based on at least a portion of the at least one key; and validating, with at least one processor, the second request for data based on the second solution to the Proof-of-Work cryptographic challenge.

[0006] In non-limiting embodiments or aspects, the method further includes communicating the at least a portion of the at least one key to the second client device, the first client device does not have access to the at least one key. In non-limiting embodiments or aspects, wherein determining the Proof-of-Work cryptographic challenge based on the first request comprises: determining a challenge difficulty based on data associated with the first client device; and modifying a computational complexity of the Proof-of-Work cryptographic challenge based on the challenge

difficulty. In non-limiting embodiments or aspects, the data associated with the first client device comprises a risk score corresponding to at least one of the following: an account holder associated with the first client device, an account identifier associated with the first client device, a network address of the first client device, a device identifier of the first client device, or any combination thereof. In non-limiting embodiments or aspects, the at least a portion of the at least one key comprises the at least one key or a partial key. In non-limiting embodiments or aspects, the first client device comprises a production system, and the second client device comprises a testing system. In non-limiting embodiments or aspects, the Proof-of-Work cryptographic challenge comprises a client-side script.

[0007] According to non-limiting embodiments or aspects, provided is a computer program product comprising at least one non-transitory computer-readable medium including program instructions that, when executed by at least one processor, causes the at least one processor to: receive a first request from a first client device; in response to the first request, determine a Proof-of-Work cryptographic challenge corresponding to at least one key; communicate the Proof-of-Work cryptographic challenge to the first client device; receive, from the first client device, a first solution to the Proof-of-Work cryptographic challenge; validate the first request for data based on the first solution to the Proof-of-Work cryptographic challenge; receive a second request from a second client device; communicate the Proof-of-Work cryptographic challenge to the second client device; receive, from the second client device, a second solution to the Proof-of-Work cryptographic challenge, the second solution based on at least a portion of the at least one key; and validate the second request for data based on the second solution to the Proof-of-Work cryptographic challenge.

[0008] In non-limiting embodiments or aspects, the at least one processor is further caused to communicate the at least a portion of the at least one key to the second client device, the first client device does not have access to the at least one key. In non-limiting embodiments or aspects, determining the Proof-of-Work cryptographic challenge based on the first request comprises: determining a challenge difficulty based on data associated with the first client device; and modifying a computational complexity of the Proof-of-Work cryptographic challenge based on the challenge difficulty. In non-limiting embodiments or aspects, the data associated with the first client device comprises a risk score corresponding to at least one of the following: an account holder associated with the first client device, an account identifier associated

with the first client device, a network address of the first client device, a device identifier of the first client device, or any combination thereof. In non-limiting embodiments or aspects, the at least a portion of the at least one key comprises the at least one key or a partial key. In non-limiting embodiments or aspects, the Proof-of-Work cryptographic challenge comprises a client-side script.

[0009] Other non-limiting embodiments or aspects will be set forth in the following numbered clauses:

[0010] Clause 1: A system comprising at least one processor programmed or configured to: receive a first request from a first client device; in response to the first request, determine a Proof-of-Work cryptographic challenge corresponding to at least one key; communicate the Proof-of-Work cryptographic challenge to the first client device; receive, from the first client device, a first solution to the Proof-of-Work cryptographic challenge; validate the first request for data based on the first solution to the Proof-of-Work cryptographic challenge; receive a second request from a second client device; communicate the Proof-of-Work cryptographic challenge to the second client device; receive, from the second client device, a second solution to the Proof-of-Work cryptographic challenge, the second solution based on at least a portion of the at least one key; and validate the second request for data based on the second solution to the Proof-of-Work cryptographic challenge.

[0011] Clause 2: The system of clause 1, wherein the at least one processor is further configured to communicate the at least a portion of the at least one key to the second client device, wherein the first client device does not have access to the at least one key.

[0012] Clause 3: The system of clauses 1 or 2, wherein determining the Proof-of-Work cryptographic challenge based on the first request comprises: determining a challenge difficulty based on data associated with the first client device; and modifying a computational complexity of the Proof-of-Work cryptographic challenge based on the challenge difficulty.

[0013] Clause 4: The system of any of clauses 1-3, wherein the data associated with the first client device comprises a risk score corresponding to at least one of the following: an account holder associated with the first client device, an account identifier associated with the first client device, a network address of the first client device, a device identifier of the first client device, or any combination thereof.

[0014] Clause 5: The system of any of clauses 1-4, wherein the at least a portion of the at least one key comprises the at least one key or a partial key.

[0015] Clause 6: The system of any of clauses 1-5, wherein the first client device comprises a production system, and wherein the second client device comprises a testing system.

[0016] Clause 7: The system of any of clauses 1-6, wherein the Proof-of-Work cryptographic challenge comprises a client-side script.

[0017] Clause 8: A method comprising: receiving, with at least one processor, a first request from a first client device; in response to the first request, determining, with at least one processor, a Proof-of-Work cryptographic challenge corresponding to at least one key; communicating the Proof-of-Work cryptographic challenge to the first client device; receiving, from the first client device, a first solution to the Proof-of-Work cryptographic challenge; validating, with at least one processor, the first request for data based on the first solution to the Proof-of-Work cryptographic challenge; receiving, with at least one processor, a second request from a second client device; communicating the Proof-of-Work cryptographic challenge to the second client device; receiving, from the second client device, a second solution to the Proof-of-Work cryptographic challenge, the second solution based on at least a portion of the at least one key; and validating, with at least one processor, the second request for data based on the second solution to the Proof-of-Work cryptographic challenge.

[0018] Clause 9: The method of clause 8, further comprising communicating the at least a portion of the at least one key to the second client device, wherein the first client device does not have access to the at least one key.

[0019] Clause 10: The method of clauses 8 or 9, wherein determining the Proof-of-Work cryptographic challenge based on the first request comprises: determining a challenge difficulty based on data associated with the first client device; and modifying a computational complexity of the Proof-of-Work cryptographic challenge based on the challenge difficulty.

[0020] Clause 11: The method of any of clauses 8-10, wherein the data associated with the first client device comprises a risk score corresponding to at least one of the following: an account holder associated with the first client device, an account identifier associated with the first client device, a network address of the first client device, a device identifier of the first client device, or any combination thereof.

[0021] Clause 12: The method of any of clauses 8-11, wherein the at least a portion of the at least one key comprises the at least one key or a partial key.

[0022] Clause 13: The method of any of clauses 8-12, wherein the first client device comprises a production system, and wherein the second client device comprises a testing system.

[0023] Clause 14: The method of any of clauses 8-13, wherein the Proof-of-Work cryptographic challenge comprises a client-side script.

[0024] Clause 15: A computer program product comprising at least one non-transitory computer-readable medium including program instructions that, when executed by at least one processor, causes the at least one processor to: receive a first request from a first client device; in response to the first request, determine a Proof-of-Work cryptographic challenge corresponding to at least one key; communicate the Proof-of-Work cryptographic challenge to the first client device; receive, from the first client device, a first solution to the Proof-of-Work cryptographic challenge; validate the first request for data based on the first solution to the Proof-of-Work cryptographic challenge; receive a second request from a second client device; communicate the Proof-of-Work cryptographic challenge to the second client device; receive, from the second client device, a second solution to the Proof-of-Work cryptographic challenge, the second solution based on at least a portion of the at least one key; and validate the second request for data based on the second solution to the Proof-of-Work cryptographic challenge.

[0025] Clause 16: The computer program product of clause 15, wherein the at least one processor is further configured to communicate the at least a portion of the at least one key to the second client device, wherein the first client device does not have access to the at least one key.

[0026] Clause 17: The computer program product of clauses 15 or 16, wherein determining the Proof-of-Work cryptographic challenge based on the first request comprises: determining a challenge difficulty based on data associated with the first client device; and modifying a computational complexity of the Proof-of-Work cryptographic challenge based on the challenge difficulty.

[0027] Clause 18: The computer program product of any of clauses 15-17, wherein the data associated with the first client device comprises a risk score corresponding to at least one of the following: an account holder associated with the first client device, an account identifier associated with the first client device, a network address of the

first client device, a device identifier of the first client device, or any combination thereof.

[0028] Clause 19: The computer program product of any of clauses 15-18, wherein the at least a portion of the at least one key comprises the at least one key or a partial key.

[0029] Clause 20: The computer program product of any of clauses 15-19, wherein the Proof-of-Work cryptographic challenge comprises a client-side script.

[0030] These and other features and characteristics of the present disclosure, as well as the methods of operation and functions of the related elements of structures and the combination of parts and economies of manufacture, will become more apparent upon consideration of the following description and the appended claims with reference to the accompanying drawings, all of which form a part of this specification, wherein like reference numerals designate corresponding parts in the various figures. It is to be expressly understood, however, that the drawings are for the purpose of illustration and description only and are not intended as a definition of the limits of the disclosed subject matter.

BRIEF DESCRIPTION OF THE DRAWINGS

[0031] Additional advantages and details are explained in greater detail below with reference to the non-limiting, exemplary embodiments that are illustrated in the accompanying schematic figures, in which:

[0032] FIG. 1 is a schematic diagram of a system for bot deterrence using cryptography according to some non-limiting embodiments or aspects;

[0033] FIGS. 2A and 2B are sequence diagrams of a system for bot deterrence using cryptography according to some non-limiting embodiments or aspects;

[0034] FIG. 3 is a flow diagram of a method for bot deterrence using cryptography according to some non-limiting embodiments or aspects; and

[0035] FIG. 4 is a schematic diagram of example components of one or more devices according to some non-limiting embodiments or aspects.

DETAILED DESCRIPTION

[0036] For purposes of the description hereinafter, the terms “end,” “upper,” “lower,” “right,” “left,” “vertical,” “horizontal,” “top,” “bottom,” “lateral,” “longitudinal,” and derivatives thereof shall relate to the embodiments as they are oriented in the drawing figures. However, it is to be understood that the embodiments may assume various alternative variations and step sequences, except where expressly specified to the

contrary. It is also to be understood that the specific devices and processes illustrated in the attached drawings, and described in the following specification, are simply exemplary embodiments or aspects of the disclosed subject matter. Hence, specific dimensions and other physical characteristics related to the embodiments or aspects disclosed herein are not to be considered as limiting.

[0037] No aspect, component, element, structure, act, step, function, instruction, and/or the like used herein should be construed as critical or essential unless explicitly described as such. Also, as used herein, the articles "a" and "an" are intended to include one or more items and may be used interchangeably with "one or more" and "at least one." Furthermore, as used herein, the term "set" is intended to include one or more items (e.g., related items, unrelated items, a combination of related and unrelated items, and/or the like) and may be used interchangeably with "one or more" or "at least one." Where only one item is intended, the term "one" or similar language is used. Also, as used herein, the terms "has," "have," "having," or the like are intended to be open-ended terms. Further, the phrase "based on" is intended to mean "based at least partially on" unless explicitly stated otherwise.

[0038] As used herein, the term "account identifier" may include one or more primary account numbers (PANs), tokens, or other identifiers associated with a customer account. The term "token" may refer to an identifier that is used as a substitute or replacement identifier for an original account identifier, such as a PAN. Account identifiers may be alphanumeric or any combination of characters and/or symbols. Tokens may be associated with a PAN or other original account identifier in one or more data structures (e.g., one or more databases, and/or the like) such that they may be used to conduct a transaction without directly using the original account identifier. In some examples, an original account identifier, such as a PAN, may be associated with a plurality of tokens for different individuals or purposes.

[0039] An "application program interface" (API) refers to computer code or other data sorted on a computer-readable medium that may be executed by a processor to facilitate the interaction between software components, such as a client-side front-end and/or server-side back-end for receiving data from the client. An "interface" refers to a generated display, such as one or more graphical user interfaces (GUIs) with which a user may interact, either directly or indirectly (e.g., through a keyboard, mouse, etc.).

[0040] As used herein, the term "bot" refers to one or more automated or partially automated software applications that perform one or more actions automatically (e.g.,

without human input or with a reduced amount of human input) in a network environment.

[0041] As used herein, the term "communication" may refer to the reception, receipt, transmission, transfer, provision, and/or the like of data (e.g., information, signals, messages, instructions, commands, and/or the like). For one unit (e.g., a device, a system, a component of a device or system, combinations thereof, and/or the like) to be in communication with another unit means that the one unit is able to directly or indirectly receive information from and/or transmit information to the other unit. This may refer to a direct or indirect connection (e.g., a direct communication connection, an indirect communication connection, and/or the like) that is wired and/or wireless in nature. Additionally, two units may be in communication with each other even though the information transmitted may be modified, processed, relayed, and/or routed between the first and second unit. For example, a first unit may be in communication with a second unit even though the first unit passively receives information and does not actively transmit information to the second unit. As another example, a first unit may be in communication with a second unit if at least one intermediary unit processes information received from the first unit and communicates the processed information to the second unit.

[0042] As used herein, the term "computing device" may refer to one or more electronic devices configured to process data. A computing device may, in some examples, include the necessary components to receive, process, and output data, such as a processor, a display, a memory, an input device, a network interface, and/or the like. A computing device may be a mobile device. As an example, a mobile device may include a cellular phone (e.g., a smartphone or standard cellular phone), a portable computer, a wearable device (e.g., watches, glasses, lenses, clothing, and/or the like), a personal digital assistant (PDA), and/or other like devices. A computing device may also be a desktop computer or other form of non-mobile computer.

[0043] As used herein, the term "issuer institution" may refer to one or more entities, such as a bank, that provide accounts to customers for conducting transactions (e.g., payment transactions), such as initiating credit and/or debit payments. For example, an issuer institution may provide an account identifier, such as a PAN, to a customer that uniquely identifies one or more accounts associated with that customer. The account identifier may be embodied on a portable financial device, such as a physical financial instrument, e.g., a payment card, and/or may be electronic and used for

electronic payments. The term "issuer system" refers to one or more computer devices operated by or on behalf of an issuer institution, such as a server computer executing one or more software applications. For example, an issuer system may include one or more authorization servers for authorizing a transaction.

[0044] As used herein, the term "merchant" may refer to an individual or entity that provides goods and/or services, or access to goods and/or services, to customers based on a transaction, such as a payment transaction. The term "merchant" or "merchant system" may also refer to one or more computer systems operated by or on behalf of a merchant, such as a server computer executing one or more software applications.

[0045] As used herein, a "point-of-sale (POS) device" may refer to one or more devices, which may be used by a merchant to conduct a transaction (e.g., a payment transaction) and/or process a transaction. For example, a POS device may include one or more client devices. Additionally or alternatively, a POS device may include peripheral devices, card readers, scanning devices (e.g., code scanners), Bluetooth® communication receivers, near-field communication (NFC) receivers, radio frequency identification (RFID) receivers, and/or other contactless transceivers or receivers, contact-based receivers, payment terminals, and/or the like. As used herein, a "point-of-sale (POS) system" may refer to one or more client devices and/or peripheral devices used by a merchant to conduct a transaction. For example, a POS system may include one or more POS devices and/or other like devices that may be used to conduct a payment transaction. In some non-limiting embodiments or aspects, a POS system (e.g., a merchant POS system) may include one or more server computers programmed or configured to process online payment transactions through webpages, mobile applications, and/or the like.

[0046] As used herein, the terms "client" and "client device" may refer to one or more client-side devices or systems (e.g., remote from a transaction service provider) used to initiate or facilitate a transaction (e.g., a payment transaction). As an example, a "client device" may refer to one or more POS devices used by a merchant, one or more acquirer host computers used by an acquirer, one or more mobile devices used by a user, and/or the like. In some non-limiting embodiments or aspects, a client device may be an electronic device configured to communicate with one or more networks and initiate or facilitate transactions. For example, a client device may include one or more computers, portable computers, laptop computers, tablet computers, mobile

devices, cellular phones, wearable devices (e.g., watches, glasses, lenses, clothing, and/or the like), PDAs, and/or the like. Moreover, a "client" may also refer to an entity (e.g., a merchant, an acquirer, and/or the like) that owns, utilizes, and/or operates a client device for initiating transactions (e.g., for initiating transactions with a transaction service provider).

[0047] As used herein, the term "payment device" may refer to a payment card (e.g., a credit or debit card), a gift card, a smartcard, smart media, a payroll card, a healthcare card, a wristband, a machine-readable medium containing account information, a keychain device or fob, an RFID transponder, a retailer discount or loyalty card, a cellular phone, an electronic wallet mobile application, a personal digital assistant (PDA), a pager, a security card, a computing device, an access card, a wireless terminal, a transponder, and/or the like. In some non-limiting embodiments or aspects, the payment device may include volatile or non-volatile memory to store information (e.g., an account identifier, a name of the account holder, and/or the like).

[0048] As used herein, the term "payment gateway" may refer to an entity and/or a payment processing system operated by or on behalf of such an entity (e.g., a merchant service provider, a payment service provider, a payment facilitator, a payment facilitator that contracts with an acquirer, a payment aggregator, and/or the like), which provides payment services (e.g., transaction service provider payment services, payment processing services, and/or the like) to one or more merchants. The payment services may be associated with the use of payment devices managed by a transaction service provider. As used herein, the term "payment gateway system" may refer to one or more computer systems, computer devices, servers, groups of servers, and/or the like, operated by or on behalf of a payment gateway.

[0049] As used herein, the term "server" may refer to or include one or more computing devices that are operated by or facilitate communication and processing for multiple parties in a network environment, such as the internet, although it will be appreciated that communication may be facilitated over one or more public or private network environments and that various other arrangements are possible. Further, multiple computing devices (e.g., servers, POS devices, mobile devices, etc.) directly or indirectly communicating in the network environment may constitute a "system." Reference to "a server" or "a processor," as used herein, may refer to a previously-recited server and/or processor that is recited as performing a previous step or function, a different server and/or processor, and/or a combination of servers and/or

processors. For example, as used in the specification and the claims, a first server and/or a first processor that is recited as performing a first step or function may refer to the same or different server and/or a processor recited as performing a second step or function.

[0050] As used herein, the term "transaction service provider" may refer to an entity that receives transaction authorization requests from merchants or other entities and provides guarantees of payment, in some cases through an agreement between the transaction service provider and an issuer institution. For example, a transaction service provider may include a payment network such as Visa® or any other entity that processes transactions. The term "transaction processing system" may refer to one or more computer systems operated by or on behalf of a transaction service provider, such as a transaction processing server executing one or more software applications. A transaction processing server may include one or more processors and, in some non-limiting embodiments or aspects, may be operated by or on behalf of a transaction service provider.

[0051] Non-limiting embodiments or aspects of the disclosed subject matter are directed to systems, methods, and computer program products for bot deterrence using cryptography. Non-limiting embodiments allow for the dynamic alteration of a cryptographic challenge based on a requesting client system, thereby expending a varying level of computing resources for different requesting client systems. This allows for testing (e.g., load testing) to be performed in an efficient way, while security is dynamically enforced in production. Other improvements and advantages are provided by the non-limiting embodiments discussed herein.

[0052] Referring to FIG. 1, a system 1000 for bot deterrence using cryptography is shown according to some non-limiting embodiments or aspects. A server computer 102 may include one or more computing devices such as a web server, private server, authentication server (e.g., such as a 3D Secure system), and/or any other computing device configured to communicate with one or more client devices (e.g., 104, 106). The server computer 102 may be in communication with a local or remote data storage device 108, which includes one or more key values (e.g., symmetric keys, asymmetric key pairs, and/or the like). The server computer 102 may be in communication with any number of client devices through one or more network environments, such as but not limited to the internet, a private network, and/or the like. For example, the server

computer 102 may operate as a web server that provides content to web browsers and/or applications executing on one or more client devices 104, 106.

[0053] In non-limiting embodiments, and with continued reference to FIG. 1, a client device 104 may communicate a request to the server computer 102. For example, the client device 104 may communicate a request to access a system that the server computer 102 controls access to, may communicate a request to conduct a payment transaction, may communicate a request to be authenticated, and/or the like. The client device 104 may also request that the server computer 102 perform an action and/or provide an output. It will be appreciated that various requests may be communicated to the server computer 102. Requests may be communicated through an API and/or via any relevant communication protocol (e.g., HTTP).

[0054] Still referring to FIG. 1, the server computer 102 may generate and communicate a cryptographic challenge to the client device 104 in response to the request. For example, a Proof-of-Work (PoW) cryptographic challenge may be provided that can be solved with computational processes with or without a secret key. The PoW cryptographic challenge may be configured to require a particular amount of computation to solve, which can be reduced and/or minimalized with a full or partial key that the client device 104 may or may not have. As an example, the cryptographic challenge may include a series of cryptographic operations (e.g., encryption, hashing, etc.) on data. The client device 104 (e.g., an application executing on the client device 104) may solve the challenge by completing one or more tasks (e.g., computing the cryptographic operations). For example, the challenge may include a client-side script (e.g., JavaScript or the like) that includes logic that is executed by the client device 104. The resulting output of the client device 104 may be communicated to the server computer 102 and validated by the server computer 102. For example, a digital signature generated by the client device 104 may be validated based on recreating the digital signature with the same inputs and comparing the digital signatures.

[0055] With continued reference to FIG. 1, a second client device 106 is also shown to be in communication with the server computer 102. In operation, any number of client devices may communicate with the server computer 102. In the example shown in FIG. 1, the client device 106 may be in communication with a local or remote data storage device 110, which includes one or more key values that were previously provisioned by the server computer 102 and/or another entity. For example, the client device 106 may have a key stored in memory that fully or partially matches a key used

to generate the challenge. Thus, the client device 106 may solve the challenge by applying the key (e.g., by decrypting data with the key, digitally signing data with the key, and/or the like).

[0056] In the example shown in FIG. 1, the first client device 104 does not have access to the key and therefore must perform a PoW process to solve the challenge. The challenge may be configured to utilize a sufficient amount of computational resources (e.g., processing cycles and/or the like) to discourage a bot from making multiple simultaneous and/or sequential requests, but without imposing a significant burden on the client device 104 making a single request. For example, a bot may seek to iterate requests through a payment platform to find active account identifiers (e.g., PANs or the like), requiring a large volume of requests. Further, the second client device 106 may be provided the key for testing and/or as a trusted system. For example, the server computer 102 may provision keys to certain client devices (e.g., client device 106) that are trusted and/or designated as being able to bypass the challenge. In some examples, a key may be provided to a client to permit load testing without having to change any validation logic or other configuration of the server computer 102. In some non-limiting embodiments, the key provisioned to client device 106 may be only a partial key to simplify, but not remove, the processing required to solve the challenge.

[0057] In non-limiting embodiments, the challenge may be dynamically generated to change the difficulty, thereby changing the computational demand (e.g., CPU cost). The difficulty of a challenge may depend on the client device that is making the request. The server computer 102 may first determine a challenge difficulty based on data associated with the client device 104, which may include an IP address, historical access data, a risk score, and/or the like. The server computer 102 may then modify a computational complexity of the PoW cryptographic challenge based on the challenge difficulty. For example, a client device 104 may be associated with a risk score and the challenge may increase in difficulty as the risk score increases. It will be appreciated that risk scores or other metrics may be generated in various ways based on historical data. For example, in a payment processing context, historical transaction data may be used to generate a risk score for a client device (e.g., a user device requesting a transaction, a merchant device requesting a transaction, or the like) that is used to determine the difficulty of the challenge. In non-limiting embodiments, a risk score may be based on an account holder associated with the first client device, an

account identifier associated with the first client device, a network address of the first client device, and/or a device identifier of the first client device.

[0058] In non-limiting embodiments, testing systems may share a key, whereas production systems that are designated as trusted systems may be provided a secure, unique key that is not shared with other systems or client devices.

[0059] Referring now to FIG. 2A, a sequence diagram for bot deterrence using cryptography is shown according to non-limiting embodiments or aspects. At step s1 a client device 104 sends a request message to the server computer 102. For example, the client device 104 may send a request for a payment transaction, a request to access data or a system, and/or the like. In response, the server computer 102 may communicate a challenge back to the client device 104 at step s2. The challenge may be generated by the server computer 102 based on data about and/or provided by the client device 104. The challenge may be already generated and stored by the server computer 102. At step s3, the client device 104 solves the challenge. For example, the client device 104 may perform a PoW challenge in which the client device 104 proves that a certain amount of computational work has been performed by, for example, attempting to solve a hash sequence, puzzle, and/or the like.

[0060] With continued reference to FIG. 2A, at step s4, the client device 104 communicates the output of the challenge (e.g., a solution or partial solution to the challenge) to the server computer 102. At step s5, the server computer 102 validates the challenge response. The validation may be performed by recreating the solution or retrieving a preexisting solution from memory and comparing it with the solution received from the client device 104. In response to validating the response to the challenge or determining that the response is invalid, the server computer 102 at step s6 may communicate a message to the client device 104 that includes requested data, a confirmation, a notification, and/or the like.

[0061] Referring now to FIG. 2B, a sequence diagram for bot deterrence using cryptography is shown according to non-limiting embodiments or aspects. A client device 106 is provisioned with a key from the server computer 102 at step s0. The client device 106 may be a testing system, a trusted system, and/or the like. The client device 106 stores the key received at this step in memory. Steps s1-s6 may be proceed as described in connection with FIG. 2A, except that step s3 may involve the client device 106 applying the key to the cryptographic challenge. Thus, having the

key in memory from receiving it at step s0 allows the client device 106 to solve the challenge using fewer computational resources.

[0062] Referring now to FIG. 3, a flow diagram for bot deterrence using cryptography is shown according to non-limiting embodiments or aspect. The steps shown in FIG. 3 are for example purposes only, and it will be appreciated that additional, fewer, different, and/or a different order of steps may be used in non-limiting embodiments. In non-limiting embodiments, a step may be automatically performed in response to completion of a preceding step. At step 300, a request is received from a client device. For example, the client device may communicate a request to access a system that the server computer controls access to, may communicate a request to conduct a payment transaction, and/or the like. At step 302, a challenge difficulty is determined. For example, a challenge difficulty may be determined based on a risk score associated with the client device, a user of the client device, and/or the like. A higher risk score may result in a higher difficulty (e.g., more computational complexity required) as compared to a lower risk score. At step 304, the cryptographic challenge is generated based on the difficulty determined at step 302.

[0063] With continued reference to FIG. 3, at step 306 the cryptographic challenge may be communicated to the client device that made the request at step 300. For example, the cryptographic challenge may be implemented by a client-side script that is executed by a web browser or other application executing on the client device. At step 308 a challenge response is received from the client device. The challenge response may include, for example, a hash value or the like. At step 310, it is determined if the challenge response is valid. For example, the server computer may compare a predetermined solution to the challenge response, may process the challenge response with a proof algorithm, and/or the like. In response to the challenge matching the predetermined solution, it may be determined that the challenge response is valid and the method may proceed to step 312. At step 312 the request received at step 300 may be validated and the server computer may perform one or more actions and/or allow access to one or more systems. If the challenge response is not validated at step 310, the request received at step 300 may be denied at step 314.

[0064] Non-limiting embodiments may be used to process requests made in a 3D Secure system for adding security to a transaction. For example, a risk score used in a 3D Secure system may be used to change the difficulty (e.g., length) of the

cryptographic challenge for a client device. A higher risk score (e.g., a higher probability of risk) may result in a more difficult challenge, such that there is a proportional relationship between risk and difficulty. Other non-limiting embodiments may be used in other scenarios and/or in combination with other systems. For example, some merchant systems may make requests to a transaction processing system and/or payment gateway, and non-limiting embodiments may be used to deter a rogue merchant from using its account to test potentially fraudulent account identifiers or the like.

[0065] In some non-limiting embodiments, bots may be encouraged to subscribe and/or register to engage with another system (e.g., such as a server computer that provides access to a service) such that the difficulty of a challenge is reduced or minimized. For example, some bots may be trusted bots that are provided with a key and/or partial key, such that the system deters unregistered and/or untrusted bots from making transactions. Different levels of difficulty and/or different percentages of the key provided may be based on one or more different tiers of subscription and/or trust, as an example. It will be appreciated that other applications are possible.

[0066] In non-limiting embodiments, the cryptographic challenge may be created by the server computer 102 based on a number of parameters, including a known secret key, a type of cryptographic algorithm (e.g., SHA256), and/or a difficulty level (e.g., a value in a range of 0-10 or the like). As an example, the following is a routine that a server computer may perform:

```
hmacKey := <knownSecret>;
algorithm := "SHA256";
difficulty := 10; # Change to make this more or less challenging
randomValue := SecureRandom.generate();
highEnthropyChallenge := hmac(algorithm, hmacKey, randomValue);
targetHash := hash(algorithm, highEnthropyChallenge);
truncatedEnthropyChallenge := truncate(highEnthropyChallenge, difficulty);
session.store("highEnthropyChallenge", highEnthropyChallenge);
returnToClient(algorithm, difficulty, randomValue, truncatedEnthropyChallenge, targetHash);
```

[0067] In non-limiting embodiments, a client device may solve the cryptographic challenge after identifying the parameters and/or data needed to perform it. As an example, the following is a routine that a client computer may perform:

```
algorithm := responseFromServer.get("algorithm");
difficulty := responseFromServer.get("difficulty");
randomValue := responseFromServer.get("randomValue");
truncatedEnthropyChallenge:=
responseFromServer.get("truncatedEnthropyChallenge");
targetHash := responseFromServer.get("targetHash");
foundEnthropyChallenge = null;
FOR i=0 TO 256^difficulty
        testEnthropyChallenge := concatenateAndPad(truncatedEnthropyChallene, i);
        testHash := hash(algorithm, testEnthropyChallenge);
        IF testHash == targetHash THEN
                foundEnthropyChallenge := testEnthropyChallenge;
                BREAK
        END IF
NEXT
submitToServer(foundEnthropyChallenge);
```

[0068] In the above example routine, the value of “randomValue” is obtained but cannot be used to solve the challenge without the value of “<knownSecret>”.

[0069] The following is an example routine that may be used by the server computer to validate the PoW challenge received from the client computer:

```
foundEnthropyChallenge := requestFromClient.get("foundEnthropyChallenge");
highEnthropyValue := session.get("highEnthropyValue");
IF highEnthropyValue == foundEnthropyChallenge THEN
        # Valid client response
        # TODO next SUCCESS step
ELSE
        # Invalid response
        # TODO next FAILURE step
END If
```

[0070] The following is an example routine that may be used by a client computer having a key to bypass the PoW challenge received from the server computer:

```
hmacKey := <knownSecret>;
algorithm := responseFromServer.get("algorithm");
difficulty := responseFromServer.get("difficulty");
```

```
randomValue := responseFromServer.get("randomValue");
truncatedEnthropyChallenge:=
responseFromServer.get("truncatedEnthropyChallenge");
targetHash := responseFromServer.get("targetHash");
highEnthropyChallenge := hmac(algorithm, hmacKey, randomValue);
submitToServer(highEnthropyChallenge);
```

[0071] It will be appreciated that various routines, algorithms, and techniques may be used to generate, solve, and validate a cryptographic challenge and that the examples provided herein are for illustration purposes.

[0072] Referring now to FIG. 4, shown is a diagram of example components of a device 400 according to non-limiting embodiments or aspects. Device 400 may correspond to at least one of the computing devices (e.g., 102, 104, 106) in FIG. 1. In some non-limiting embodiments or aspects, such systems or devices may include at least one device 400 and/or at least one component of device 400. The number and arrangement of components shown in FIG. 4 are provided as an example. In some non-limiting embodiments or aspects, device 400 may include additional components, fewer components, different components, or differently arranged components than those shown in FIG. 4. Additionally, or alternatively, a set of components (e.g., one or more components) of device 400 may perform one or more functions described as being performed by another set of components of device 400.

[0073] As shown in FIG. 4, device 400 may include bus 402, processor 404, memory 406, storage component 408, input component 410, output component 412, and communication interface 414. Bus 402 may include a component that permits communication among the components of device 400. In some non-limiting embodiments or aspects, processor 404 may be implemented in hardware, firmware, or a combination of hardware and software. For example, processor 404 may include a processor (e.g., a central processing unit (CPU), a graphics processing unit (GPU), an accelerated processing unit (APU), etc.), a microprocessor, a digital signal processor (DSP), and/or any processing component (e.g., a field-programmable gate array (FPGA), an application-specific integrated circuit (ASIC), etc.) that can be programmed to perform a function. Memory 406 may include random access memory (RAM), read only memory (ROM), and/or another type of dynamic or static storage device (e.g., flash memory, magnetic memory, optical memory, etc.) that stores information and/or instructions for use by processor 404.

[0074] With continued reference to FIG. 4, storage component 408 may store information and/or software related to the operation and use of device 400. For example, storage component 408 may include a hard disk (e.g., a magnetic disk, an optical disk, a magneto-optic disk, a solid state disk, etc.) and/or another type of computer-readable medium. Input component 410 may include a component that permits device 400 to receive information, such as via user input (e.g., a touch screen display, a keyboard, a keypad, a mouse, a button, a switch, a microphone, etc.). Additionally, or alternatively, input component 410 may include a sensor for sensing information (e.g., a global positioning system (GPS) component, an accelerometer, a gyroscope, an actuator, etc.). Output component 412 may include a component that provides output information from device 400 (e.g., a display, a speaker, one or more light-emitting diodes (LEDs), etc.). Communication interface 414 may include a transceiver-like component (e.g., a transceiver, a separate receiver and transmitter, etc.) that enables device 400 to communicate with other devices, such as via a wired connection, a wireless connection, or a combination of wired and wireless connections. Communication interface 414 may permit device 400 to receive information from another device and/or provide information to another device. For example, communication interface 414 may include an Ethernet interface, an optical interface, a coaxial interface, an infrared interface, a radio frequency (RF) interface, a universal serial bus (USB) interface, a Wi-Fi® interface, a cellular network interface, and/or the like.

[0075] Device 400 may perform one or more processes described herein. Device 400 may perform these processes based on processor 404 executing software instructions stored by a computer-readable medium, such as memory 406 and/or storage component 408. A computer-readable medium may include any non-transitory memory device. A memory device includes memory space located inside of a single physical storage device or memory space spread across multiple physical storage devices. Software instructions may be read into memory 406 and/or storage component 408 from another computer-readable medium or from another device via communication interface 414. When executed, software instructions stored in memory 406 and/or storage component 408 may cause processor 404 to perform one or more processes described herein. Additionally, or alternatively, hardwired circuitry may be used in place of or in combination with software instructions to perform one or more processes described herein. Thus, embodiments described herein are not limited to

any specific combination of hardware circuitry and software. The term “programmed or configured,” as used herein, refers to an arrangement of software, hardware circuitry, or any combination thereof on one or more devices.

[0076] Although embodiments have been described in detail for the purpose of illustration, it is to be understood that such detail is solely for that purpose and that the disclosure is not limited to the disclosed embodiments or aspects, but, on the contrary, is intended to cover modifications and equivalent arrangements that are within the spirit and scope of the appended claims. For example, it is to be understood that the present disclosure contemplates that, to the extent possible, one or more features of any embodiment or aspect can be combined with one or more features of any other embodiment or aspect.

WHAT IS CLAIMED IS:

1. A system comprising at least one processor programmed or configured to:

receive a first request from a first client device;

in response to the first request, determine a Proof-of-Work cryptographic challenge corresponding to at least one key;

communicate the Proof-of-Work cryptographic challenge to the first client device;

receive, from the first client device, a first solution to the Proof-of-Work cryptographic challenge;

validate the first request for data based on the first solution to the Proof-of-Work cryptographic challenge;

receive a second request from a second client device;

communicate the Proof-of-Work cryptographic challenge to the second client device;

receive, from the second client device, a second solution to the Proof-of-Work cryptographic challenge, the second solution based on at least a portion of the at least one key; and

validate the second request for data based on the second solution to the Proof-of-Work cryptographic challenge.

2. The system of claim 1, wherein the at least one processor is further configured to communicate the at least a portion of the at least one key to the second client device, wherein the first client device does not have access to the at least one key.

3. The system of claim 1, wherein determining the Proof-of-Work cryptographic challenge based on the first request comprises:

determining a challenge difficulty based on data associated with the first client device; and

modifying a computational complexity of the Proof-of-Work cryptographic challenge based on the challenge difficulty.

4. The system of claim 1, wherein the data associated with the first client device comprises a risk score corresponding to at least one of the following: an account holder associated with the first client device, an account identifier associated with the first client device, a network address of the first client device, a device identifier of the first client device, or any combination thereof.

5. The system of claim 1, wherein the at least a portion of the at least one key comprises the at least one key or a partial key.

6. The system of claim 1, wherein the first client device comprises a production system, and wherein the second client device comprises a testing system.

7. The system of claim 1, wherein the Proof-of-Work cryptographic challenge comprises a client-side script.

8. A method comprising:

receiving, with at least one processor, a first request from a first client device;

in response to the first request, determining, with at least one processor, a Proof-of-Work cryptographic challenge corresponding to at least one key;

communicating the Proof-of-Work cryptographic challenge to the first client device;

receiving, from the first client device, a first solution to the Proof-of-Work cryptographic challenge;

validating, with at least one processor, the first request for data based on the first solution to the Proof-of-Work cryptographic challenge;

receiving, with at least one processor, a second request from a second client device;

communicating the Proof-of-Work cryptographic challenge to the second client device;

receiving, from the second client device, a second solution to the Proof-of-Work cryptographic challenge, the second solution based on at least a portion of the at least one key; and

validating, with at least one processor, the second request for data based on the second solution to the Proof-of-Work cryptographic challenge.

9. The method of claim 8, further comprising communicating the at least a portion of the at least one key to the second client device, wherein the first client device does not have access to the at least one key.

10. The method of claim 8, wherein determining the Proof-of-Work cryptographic challenge based on the first request comprises:

determining a challenge difficulty based on data associated with the first client device; and

modifying a computational complexity of the Proof-of-Work cryptographic challenge based on the challenge difficulty.

11. The method of claim 8, wherein the data associated with the first client device comprises a risk score corresponding to at least one of the following: an account holder associated with the first client device, an account identifier associated with the first client device, a network address of the first client device, a device identifier of the first client device, or any combination thereof.

12. The method of claim 8, wherein the at least a portion of the at least one key comprises the at least one key or a partial key.

13. The method of claim 8, wherein the first client device comprises a production system, and wherein the second client device comprises a testing system.

14. The method of claim 8, wherein the Proof-of-Work cryptographic challenge comprises a client-side script.

15. A computer program product comprising at least one non-transitory computer-readable medium including program instructions that, when executed by at least one processor, causes the at least one processor to:

receive a first request from a first client device;

in response to the first request, determine a Proof-of-Work cryptographic challenge corresponding to at least one key;

communicate the Proof-of-Work cryptographic challenge to the first client device;

receive, from the first client device, a first solution to the Proof-of-Work cryptographic challenge;

validate the first request for data based on the first solution to the Proof-of-Work cryptographic challenge;

receive a second request from a second client device;

communicate the Proof-of-Work cryptographic challenge to the second client device;

receive, from the second client device, a second solution to the Proof-of-Work cryptographic challenge, the second solution based on at least a portion of the at least one key; and

validate the second request for data based on the second solution to the Proof-of-Work cryptographic challenge.

16. The computer program product of claim 15, wherein the at least one processor is further caused to communicate the at least a portion of the at least one key to the second client device, wherein the first client device does not have access to the at least one key.

17. The computer program product of claim 15, wherein determining the Proof-of-Work cryptographic challenge based on the first request comprises:

determining a challenge difficulty based on data associated with the first client device; and

modifying a computational complexity of the Proof-of-Work cryptographic challenge based on the challenge difficulty.

18. The computer program product of claim 15, wherein the data associated with the first client device comprises a risk score corresponding to at least one of the following: an account holder associated with the first client device, an account identifier associated with the first client device, a network address of the first client device, a device identifier of the first client device, or any combination thereof.

19. The computer program product of claim 15, wherein the at least a portion of the at least one key comprises the at least one key or a partial key.

20. The computer program product of claim 15, wherein the Proof-of-Work cryptographic challenge comprises a client-side script.

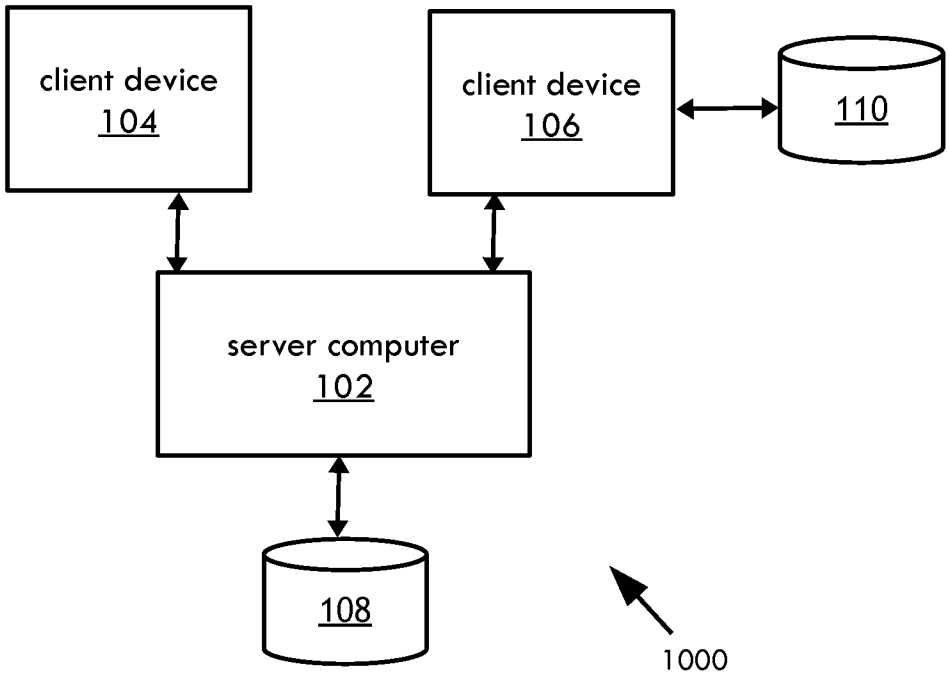
client device
104
client device
106
110
server computer
102
108
1000

FIG. 1

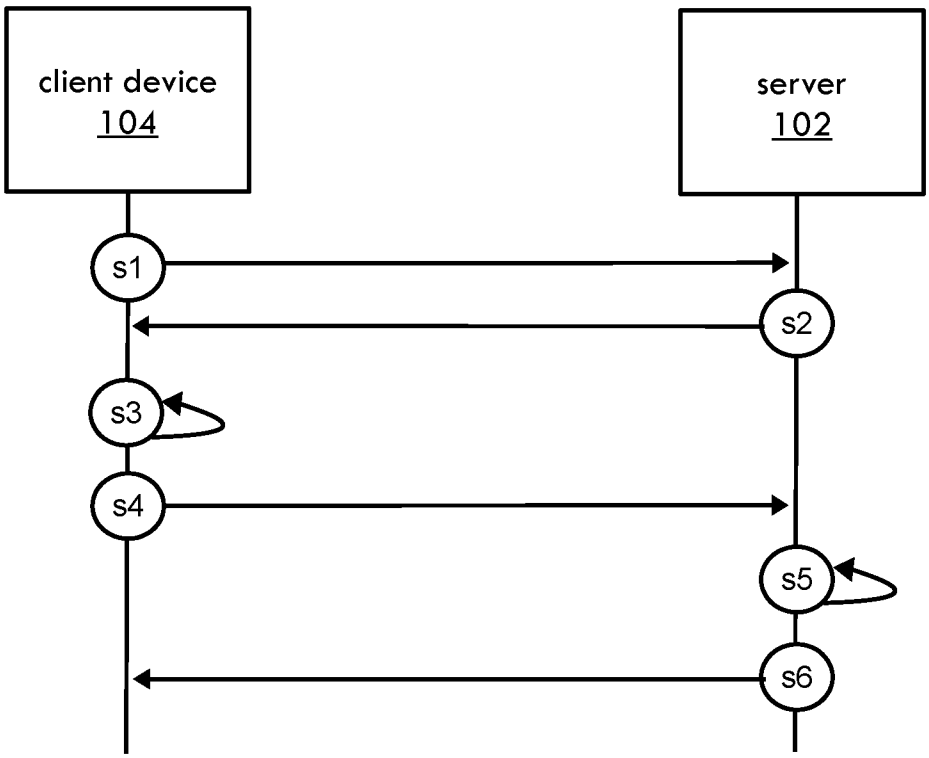
client device
104
server
102
s1
s2
s3
s4
s5
s6

FIG. 2A

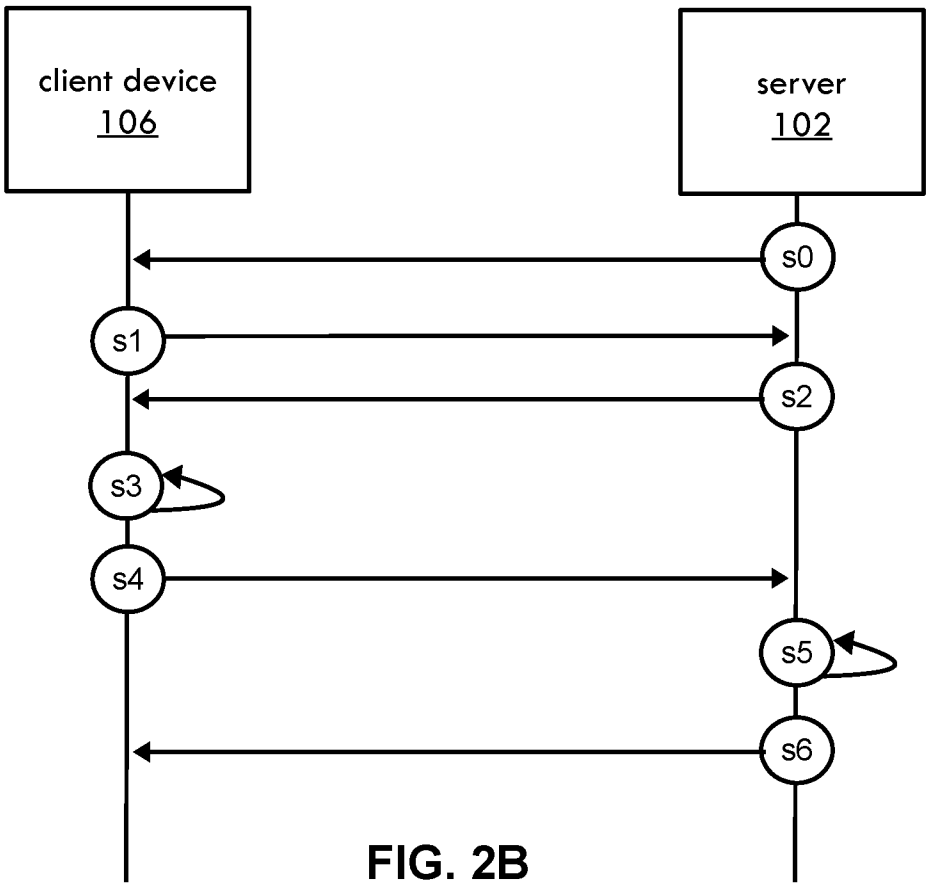
client device
106
server
102
s0
s1
s2
s3
s4
s5
s6

FIG. 2B

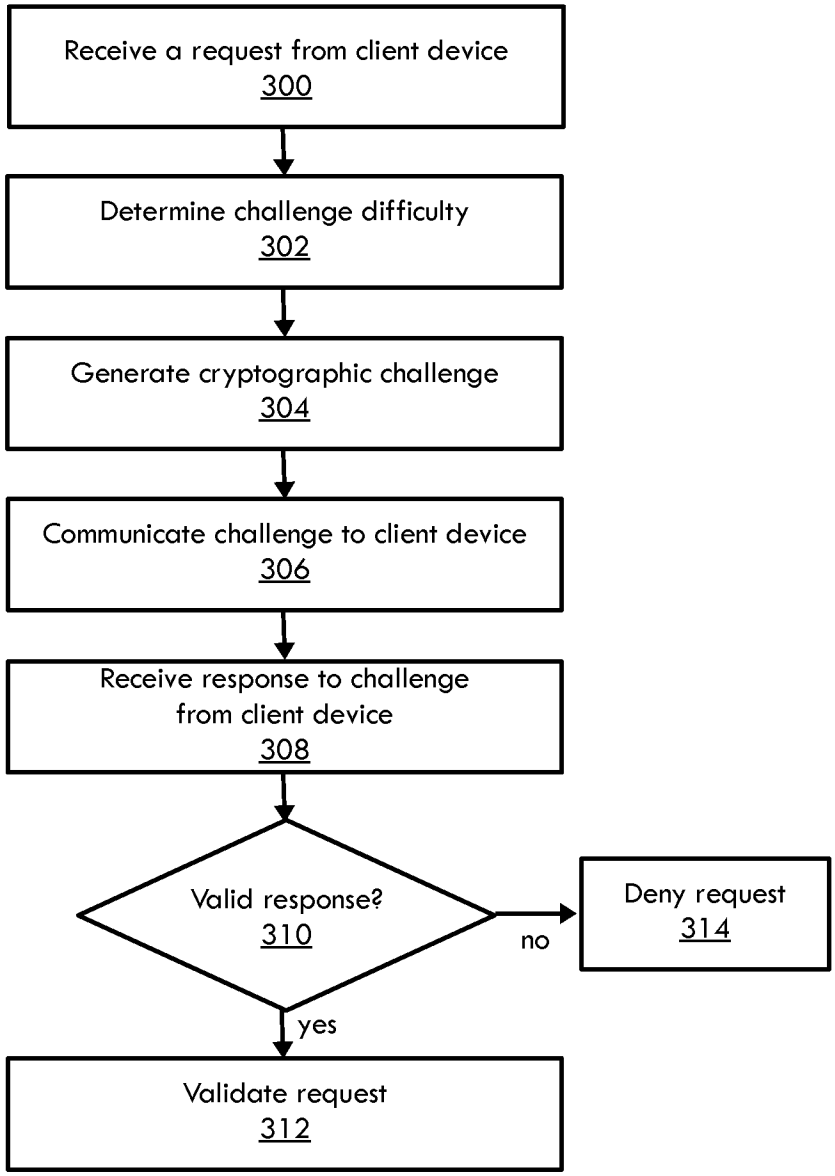
Receive a request from client device
300
Determine challenge difficulty
302
Generate cryptographic challenge
304
Communicate challenge to client device
306
Receive response to challenge from client device
308
Valid response?
310
no
Deny request
314
yes
Validate request
312

FIG. 3

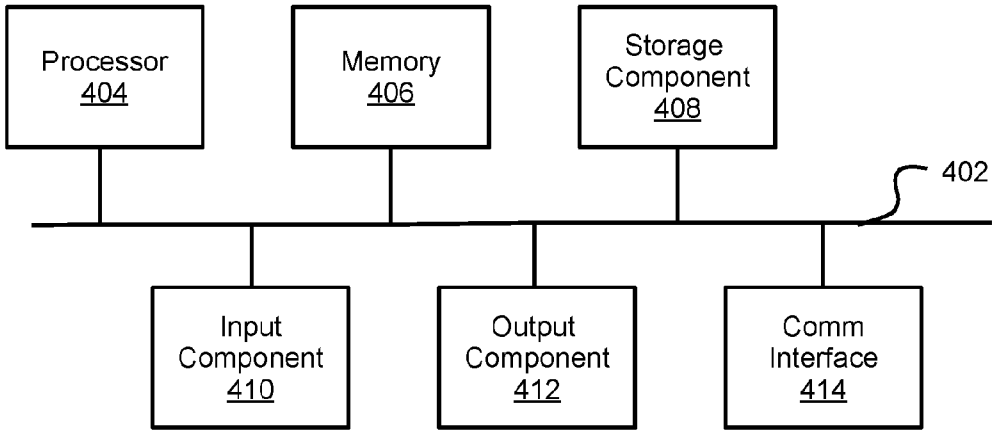
Processor
404
Memory
406
Storage
Component
408
402
Input
Component
410
Output
Component
412
Comm
Interface
414

FIG. 4


400

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 23/26515

A. CLASSIFICATION OF SUBJECT MATTER

IPC - INV. G06F 21/31, G06F 21/50, G06F 21/55, G06F 21/62 (2023.01)
ADD.

CPC - INV. G06F 21/31, G06F 21/50, G06F 21/55, G06F 21/62
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)
See Search History.document

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X -- Y	US 2010/0031315 A1 (Feng et al.), 04 February 2010 (04.02.2010), entire document, especially Abstract and para [0053], [0057], [0077]-[0078], [0083], [0087], [0092]-[0093] and [0103].	1-3, 5, 7-10, 12, 14-17, 19-20 --- - 4, 6, 11, 13, 18
Y	US 9,807,092 B1 (DCS7, LLC), 31 October 2017 (31.10.2017), entire document, especially Abstract and col 22, ln 10-12, col 25, ln 46-52 and col 30, ln 25-28.	4, 11, 18
Y	US 2020/0174912 A1 (Bank of America Corporation), 04 June 2020 (04.06.2020), entire document, especially Abstract and para [0026] and [0036].	6, 13

☐ 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
"D" document cited by the applicant in the international application
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
22 August 2023	SEP 29 2023
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-8300	Authorized officer Kari Rodriquez Telephone No. PCT Helpdesk: 571-272-4300