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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
19 December 2024 (19.12.2024)

WIPO | PCT

(10) International Publication Number
WO 2024/258429 A1

(51) International Patent Classification:
G06Q 20/38 (2012.01) *G06Q 20/02* (2012.01)
G06Q 20/34 (2012.01) *G06F 7/58* (2006.01)
G06Q 20/40 (2012.01) *H04L 9/08* (2006.01)

(21) International Application Number:
PCT/US2023/068519

(22) International Filing Date:
15 June 2023 (15.06.2023)

(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: **CHEN, Yuexi**; 882 Balboa Ln, Foster City, California 94404 (US).

(74) Agent: **TOBIN, Garrett J.** et al.; 210 Sixth Avenue, 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: RANDOMIZED APPLICATION TRANSACTION COUNTER

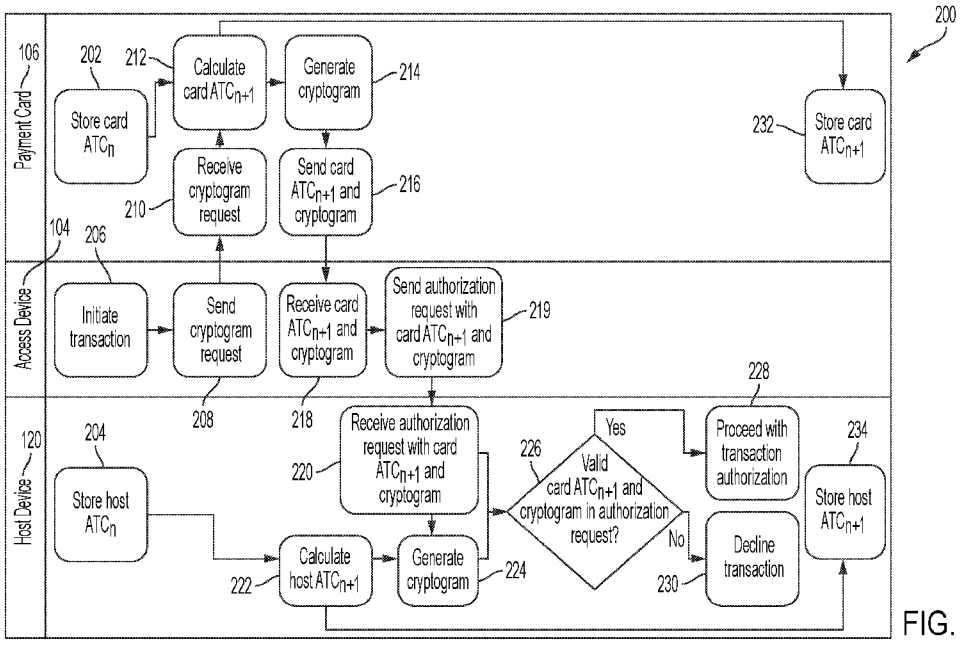

FIG. 2

(57) Abstract: The present disclosure provides devices, systems, and methods for securely conducting payment card transactions based on a randomized application transaction counter (ATC). In one aspect of the present disclosure, a method for implementing a randomized ATC in a payment card transaction can include storing, by a payment card, a first ATC value. The method can further include receiving, by the payment card, a request for a cryptogram from an access device, calculating, by the payment card, a second ATC value by applying the first ATC value to a pseudorandom number generator algorithm, and generating, by the payment card, the cryptogram based on the second ATC value. The method can further include sending, by the payment card, the second ATC value and the cryptogram to the access device. The payment card may store the second ATC value.

WO 2024/258429 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))*

TITLE

RANDOMIZED APPLICATION TRANSACTION COUNTER

TECHNICAL FIELD

[0001] At least some aspects of the present disclosure relate to improving security for payment card (*e.g.*, credit card, debit card) transactions, and more particularly, to improving security related to application transaction counters (ATCs) employed for processing payment card transactions.

BACKGROUND

[0002] Application transaction counters (ATCs) are commonly used in payment card transactions, such as, for example, Europay Mastercard Visa (EMV) transactions. The ATC is a counter that can be maintained by the payment card and used for security-related purposes such as EMV session key diversification, application cryptogram generation, and dynamic data authentication.

[0003] Traditionally, the ATC is incrementally and linearly increased (*e.g.*, 0, 1, 2, 3, etc.) each time the payment card is used to carry out a transaction. Each transaction performed using the payment card can therefore have a unique ATC value. Thus, by using the ATC for session key diversification and application cryptogram generation, traditional ATCs can prevent fraudsters from carrying out replay attacks and prevent fraudsters from identifying the payment card's secret symmetric key and asymmetric key using template attacks.

[0004] However, due to their incrementally and linearly increasing nature, the use of traditional ATCs can potentially enable fraudsters to identify a stolen payment card's secret symmetric key and asymmetric key using dictionary attacks. For example, a fraudster can precompute a collision database. To do this, the fraudster may generate a list of every possible secret symmetric key for the stolen payment card (*e.g.*, every possible 8-byte key, every possible 16-byte key), select an ATC value (*e.g.*, 306), and diversify every one of the potential secret symmetric keys with the selected ATC value to generate a list of session keys. To complete the collision database, the fraudster may select data for application cryptogram generation (*e.g.*, a transaction amount, a currency code, terminal data) and generate a list of application cryptograms based on the selected data and the list of session keys. Thus, the collision database can be a table that includes a list of secret symmetric keys and a list of corresponding application cryptograms for a given ATC value. The fraudster may then determine the current value of the stolen payment card's ATC (*e.g.*, 56) and conduct dummy transactions to cycle the stolen payment card's ATC until reaching the selected ATC value (*e.g.*, 306) of the collision database. Upon reaching the selected ATC value, the fraudster can cause the payment card to generate an application cryptogram by

sending to the payment card the same selected data (*e.g.*, transaction amount, currency code, terminal data) used for the collision database. By identifying a collision (a match) between the cryptogram generated by the card and one of the list of cryptograms in the collision database, the fraudster can look up the stolen payment card's secret symmetric using the collision database. With this information, the fraudster can use the payment card to conduct fraudulent transactions.

[0005] Accordingly, there is a need for alternate devices, systems, and methods for securely conducting payment card transactions. The present disclosure provides various solutions that implement randomized ATCs in payment card transactions

SUMMARY

[0006] According to one aspect, the present disclosure provides a method for implementing a randomized application transaction counter (ATC) in a payment card transaction. The method can include storing, by a payment card, a first ATC value. The method can further include receiving, by the payment card, a request for a cryptogram from an access device. The request can be based on a transaction initiated using the payment card and the access device. The method can further include calculating, by the payment card, a second ATC value by applying the first ATC value to a pseudorandom number generator algorithm and generating, by the payment card, the cryptogram based on the second ATC value. The method can further include sending, by the payment card, the second ATC value and the cryptogram to the access device and storing, by the payment card, the second ATC value.

[0007] According to another aspect, the present disclosure provides a payment card. The payment card can include a circuit. The circuit can receive a first request for a first cryptogram. The first request can be based on a first transaction initiated using the payment card. The circuit can further determine a first application transaction counter (ATC) value for use with the first transaction and generate the first cryptogram based on the first ATC value. The circuit can further receive a second request for a second cryptogram. The second request can be based on a second transaction initiated using the payment card, wherein the second transaction is the next transaction initiated by the payment card following the first transaction. The circuit can further determine a second ATC value for use with the second transaction, wherein the second ATC value is not determined by incrementally increasing the first ATC value. The circuit can further generate the second cryptogram based on the second ATC value.

[0008] According to yet another aspect, the present disclosure provides a method for

implementing a randomized application transaction counter (ATC) in a payment card transaction. The method can include storing, by a host server, a first ATC value associated with a payment card. The method can further include receiving, by the host server, a transaction authorization request. The transaction authorization request can include a transaction ATC value. Transaction authorization request can be based on a transaction initiated using the payment card. The method can further include calculating, by the host server, a second ATC value by applying the first ATC value to a pseudorandom number generator algorithm and comparing, by the host server, the transaction ATC value and the second ATC value.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] In the description, for purposes of explanation and not limitation, specific details are set forth, such as particular aspects, procedures, techniques, etc. to provide a thorough understanding of the present technology. However, it will be apparent to one skilled in the art that the present technology may be practiced in other aspects that depart from these specific details.

[0010] The accompanying drawings, together with the detailed description below, are incorporated in and form part of the specification, and serve to further illustrate aspects of concepts that include the claimed disclosure and explain various principles and advantages of those aspects.

[0011] The apparatuses and methods disclosed herein have been represented where appropriate by conventional symbols in the drawings, showing only those specific details that are pertinent to understanding the various aspects of the present disclosure so as not to obscure the disclosure with details that will be readily apparent to those of ordinary skill in the art having the benefit of the description herein.

[0012] FIG. 1 illustrates a payment network environment, according to at least one aspect of the present disclosure.

[0013] FIG. 2 shows a swimlane diagram illustrating a method for implementing a randomized application transaction counter (ATC) in a payment card transaction, wherein the ATC is generated based on a pseudorandom number generator algorithm, according to at least one aspect of the present disclosure.

[0014] FIG. 3 shows a swimlane diagram illustrating a method for implementing a randomized application transaction counter (ATC) in a payment card transaction, wherein the ATC is selected from a randomly ordered set of ATCs, according to at least one aspect of the present disclosure.

[0015] FIG. 4 is a flow diagram of a method for implementing a randomized application transaction counter (ATC) in a payment card transaction, according to at least one aspect of the present disclosure.

[0016] FIG. 5 is a flow diagram of another method for implementing a randomized application transaction counter (ATC) in a payment card transaction, according to at least one aspect of the present disclosure.

[0017] FIG. 6 is a flow diagram of yet another method for implementing a randomized application transaction counter (ATC) in a payment card transaction, according to at least one aspect of the present disclosure.

[0018] FIG. 7 is a block diagram of a computer apparatus with data processing subsystems or components, according to at least one aspect of the present disclosure.

[0019] FIG. 8 is a diagrammatic representation of an example system that includes a host machine, according to at least one aspect of the present disclosure.

[0020] Corresponding reference characters indicate corresponding parts throughout the several views. The exemplifications set out herein illustrate various aspects of the present disclosure, in one form, and such exemplifications are not to be construed as limiting the scope of the disclosure in any manner.

DESCRIPTION

[0021] Before explaining various forms of the devices, systems, and methods for implementing randomized ATCs, it should be noted that the illustrative forms disclosed herein are not limited in application or use to the details of construction and arrangement of components illustrated in the accompanying drawings and description. The illustrative forms may be implemented or incorporated in other forms, variations and modifications, and may be practiced or carried out in various ways. Further, unless otherwise indicated, the terms and expressions utilized herein have been chosen for the purpose of describing the illustrative forms for the convenience of the reader and are not for the purpose of limitation thereof. Also in the following description, it is to be understood that terms such as “forward,” “rearward,” “left,” “right,” “above,” “below,” “upwardly,” “downwardly,” and the like are words of convenience and are not to be construed as limiting terms.

[0022] As described above, application transaction counters (ATCs) are commonly used in payment card transactions. Traditionally, ATCs are incrementally and linearly increased (*e.g.*, 0, 1, 2, 3, etc.) each time the payment card is used to carry out a transaction. However, due to their incrementally and linearly increasing nature, the use of traditional

ATCs can potentially enable fraudsters to identify a stolen payment card's secret symmetric key and asymmetric key, for example, by using dictionary attacks. Accordingly, there is a need for alternate devices, systems, and methods for securely conducting payment card transactions.

[0023] The present disclosure provides various devices, systems, and methods that implement randomized ATCs in payment card transactions. In one aspect, the present disclosure provides a method for implementing a randomized ATC in a payment card transaction. According to the method, the payment card can store a first ATC value. The payment card can receive a request for a cryptogram from an access device based on a transaction initiated using the payment card. The payment card can calculate a second ATC value by applying the first ATC value to a pseudorandom number generator algorithm, such as, for example a linear congruential generator algorithm. The payment card can generate the cryptogram based on the second ATC value and send the second ATC value and the cryptogram to the access device. Further, the payment card can store the second ATC value. This method can be repeated for subsequent transactions, calculating the next ATC value based on the most recently stored ATC value, so that a randomized ATC value is used for each transaction.

[0024] The devices, systems, and methods provided herein can provide numerous benefits. For example, by implementing randomized ATCs, fraudsters may not be able to use dictionary attacks to identify the secret symmetric key and/or the asymmetric key of a stolen payment card. As described in detail above, executing a dictionary attack can require determining the current value of the stolen payment card's ATC (*e.g.*, 56) and conducting dummy transactions to cycle the stolen payment card's ATC until reaching a selected ATC value (*e.g.*, 306) used to generate a collision database. However, where a randomized ATC is implemented, and an incrementally and linearly increasing ATC value is therefore not implemented, the fraudster may be unable to predictably cycle the stolen payment card's ATC to the selected value. Thus, the fraudster may not be able to cause the payment card to generate a cryptogram for the selected ATC value, thereby preventing the fraudster from implementing the collision database generated based on the selected ATC to identify the stolen card's secret symmetric key. Accordingly, the devices, systems, and methods disclosed herein can provide a specific, nonconventional technological solution to a specific technological problem.

[0025] As another example, the devices, systems, and methods provided herein can be employed using existing payment infrastructure, hardware, software, and/or communication protocols. For example, as disclosed herein, a payment card can be configured to calculate a next ATC value by applying a stored ATC value to a pseudorandom number. Using

existing EMV protocols, the calculated ATC may be used to diversify a session key, may be used to generate an application cryptogram, and may be communicated to an issuer for validation. Comparatively, other solutions that attempt to address the above-mentioned susceptibly of traditional ATCs to dictionary attacks may include introducing randomness as part of the cryptogram generation. However, this approach may require modifications to existing messaging protocols between the payment card, the access device, the acquirer system, the payment transaction services provider system, and/or the issuer system. Such modifications to existing messaging protocols can require significant and potentially expensive changes to existing payment network infrastructure. Accordingly, the devices, systems, and methods provided herein can provide an improvement to existing technology for payment card transaction security.

[0026] FIG. 1 is a diagram of a payment network environment 100 in which a transaction may be conducted based on a randomized ATC, according to at least one aspect of the present disclosure. As shown in FIG. 1, the payment network environment 100 can include a payment gateway system 102, an access device 104, a payment card 106, an issuer system 108, a transaction service provider system 110, an acquirer system 112, and a network 114. The payment gateway system 102, the access device 104, the issuer system 108, the transaction service provider system 110, and/or the acquirer system 112 may interconnect (*e.g.*, establish a connection to communicate) via wired connections, wireless connections, or a combination of wired and wireless connections.

[0027] A “payment network” may refer to an electronic payment system used to accept, transmit, or process transactions made by payment devices for money, goods, or services. The payment network may transfer information and funds among issuers, acquirers, merchants, and payment device users. One illustrative non-limiting example of a payment network is VisaNet, which is operated by Visa, Inc.

[0028] A “system” may refer to one or more computing devices or combinations of computing devices (*e.g.*, processors, servers, client devices, software applications, components of such, and/or the like).

[0029] Referring again to FIG. 1, the access device 104 may include one or more devices capable of receiving information from and/or transmitting information to the payment gateway system 102, the payment card 106, the issuer system 108, the transaction service provider system 110, and/or the acquirer system 112 via the network 114. The access device 104 may be any suitable device that provides access to a remote system. The access device 104 may also be used for communicating with a merchant computer, a transaction processing computer, an authentication computer, or any other suitable system. The access

device 104 device may generally be located in any suitable location, such as at the location of a merchant. The access device 104 device may be in any suitable form. Some examples of the access device 104 can include POS or point-of-sale devices (*e.g.*, POS terminals), cellular phones, PDAs, personal computers (PCs), tablet PCs, hand-held specialized readers, set-top boxes, electronic cash registers (ECRs), automated teller machines (ATMs), virtual cash registers (VCRs), kiosks, security systems, access systems, and the like. The access device 104 may use any suitable contact or contactless mode of operation to send or receive data from, or associated with, the payment card 106. For example, the access device 104 may include a reader, a processor, and a computer-readable medium. A reader can include a radio frequency (RF) antenna, an optical scanners, a bar code reader, and/or a magnetic stripe readers to interact with the payment card 106.

[0030] As noted above, in some aspects, the access device 104 can comprise a point-of-sale (POS) device. The POS device may include one or more than one device, such a computer, a computer system, a portable electronic device, and/or a peripheral device capable of being used by a merchant to conduct a payment transaction with a user, for example, using the payment card 106. In some aspects, the POS device may be a component of a merchant system associated with a merchant. In some aspects, the POS device can be configured to receive information from the payment card 106 via a communication connection (*e.g.*, a near field communication (NFC) connection, a radio-frequency identification (RFID) communication connection, a Bluetooth® communication connection, and/or the like) and/or transmit information to the payment card 106 via the communication connection.

[0031] A “merchant” may refer to one or more individuals or entities (*e.g.*, operators of retail businesses that provide goods and/or services, and/or access to goods and/or services, to a user (*e.g.*, a customer, a consumer, a customer of the merchant, and/or the like) based on a transaction (*e.g.*, a payment transaction)). As used herein “merchant system” may 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.

[0032] A “user” may include an individual. In some embodiments or aspects, a user may be associated with one or more personal accounts, payment cards, and/or portable electronic devices. The user may also be referred to as a cardholder, account holder, or consumer.

[0033] Referring again to FIG. 1, the payment card 106 can include any device that may be used to conduct a transaction, such as a financial transaction. For example, a payment card 106 may be used to provide payment information to a merchant. The payment card 106

can include a substrate such as a paper, metal, or plastic card, and information that is printed, embossed, encoded, and/or otherwise included at or near a surface of the payment card. The payment card 106 can be hand-held and compact so that it can fit into a consumer's wallet and/or pocket (*e.g.*, pocket-sized). The payment card 106 can be a smart card, a debit device (*e.g.*, a debit card), a credit device (*e.g.*, a credit card), a stored value device (*e.g.*, a stored value card or "prepaid" card), a magnetic stripe or chip card. The payment card 106 may operate in a contact and/or contactless mode. For example, the payment card 106 may be an electronic payment device, such as a smart card, a chip card, an integrated circuit card, and/or a near field communications (NFC) card, among others. The payment card 106 device may include an embedded integrated circuit. The embedded integrated circuit may include a data storage medium (*e.g.*, volatile and/or non-volatile memory) to store information associated with the payment card 106, such as an account identifier and/or a name of an account holder. The payment card 106 card may interface with the access device 104 to initiate a transaction.

[0034] Referring still to FIG. 1, the payment gateway system 102 may include one or more devices capable of receiving information from and/or transmitting information to the access device 104, the issuer system 108, the transaction service provider system 110, and/or the acquirer system 112 via the network 114. For example, the payment gateway system 102 may include a computing device, such as a server (*e.g.*, a transaction processing server), a group of servers, and/or other like devices. The payment gateway system 102 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 (PSP), 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.

[0035] Referring still to FIG. 1, the acquirer system 112 may include one or more devices capable of receiving information from and/or transmitting information to the payment gateway system 102, the access device 104, the issuer system 108, and/or the transaction service provider system 110 via the network 114. For example, the acquirer system 112 may include a computing device, such as a server, a group of servers, and/or other like devices. In some aspects, acquirer system 112 may be associated with an acquirer. In some aspects, the acquirer system 112 may be associated with a merchant account of a merchant associated with the access device 104.

[0036] An "acquirer" may refer to an entity licensed by a transaction service provider and/or approved by a transaction service provider to originate transactions (*e.g.*, payment

transactions) using a portable financial device associated with the transaction service provider. “Acquirer” or “acquirer system” may also refer to one or more computer systems operated by or on behalf of an acquirer, such as a server computer executing one or more software applications (*e.g.*, “acquirer server”). An “acquirer” may be a merchant bank, or in some cases, the merchant system may be the acquirer. The transactions may include original credit transactions (OCTs) and account funding transactions (AFTs). The acquirer may be authorized by the transaction service provider to sign merchants of service providers to originate transactions using a portable financial device of the transaction service provider. The acquirer may contract with payment facilitators to enable the facilitators to sponsor merchants. The acquirer may monitor compliance of the payment facilitators in accordance with regulations of the transaction service provider.

[0037] Referring again to FIG. 1, the transaction service provider system 110 may include one or more devices capable of receiving information from and/or transmitting information to the payment gateway system 102, the access device 104, the issuer system 108, and/or the acquirer system 112 via the network 114. For example, the transaction service provider system 110 may include a computing device, such as a server (*e.g.*, a transaction processing server), a group of servers, and/or other like devices. In some aspects, the transaction service provider system 110 may be associated with a transaction service provider. In some aspects, transaction service provider system 110 may be in communication with a data storage device, which may be local or remote to the transaction service provider system 110. In some aspects, the transaction service provider system 110 may be capable of receiving information from, storing information in, transmitting information to, or searching information stored in a data storage device.

[0038] A “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. For example, a transaction service provider may include a payment network, such as Visa®, MasterCard®, American Express®, or any other entity that processes transactions. As used herein “transaction service provider system” may refer to one or more systems operated by or operated on behalf of a transaction service provider, such as a transaction service provider system executing one or more software applications associated with the transaction service provider. In some non-limiting aspects, a transaction service provider system may include one or more server computers with one or more processors and, in some non-limiting aspects, may be operated by or on behalf of a transaction service provider.

[0039] Referring again to FIG. 1, the issuer system 108 may include one or more devices capable of receiving information from and/or transmitting information to payment gateway system 102, the access device 104, transaction service provider system 110, and/or the acquirer system 112 via the network 114. For example, issuer system 108 may include a computing device, such as a server, a group of servers, and/or other like devices. In various aspects, the issuer system 108 may be associated with an issuer institution. For example, the issuer system 108 may be associated with an issuer institution that issued a credit account, debit account, credit card account, debit card account, and/or the like to a user associated with the payment card 106.

[0040] The terms “issuer institution,” “portable financial device issuer,” “issuer,” or “issuer bank” may refer to one or more entities that provide one or more accounts (*e.g.*, a credit account, a debit account, a credit card account, a debit card account, and/or the like) to a user (*e.g.*, customer, consumer, and/or the like) for conducting transactions (*e.g.*, payment transactions), such as initiating credit and/or debit payments. For example, an issuer may provide an account identifier, such as a personal account number (PAN), to a user that uniquely identifies one or more accounts associated with the user. The account identifier may be used by the user to conduct a payment transaction. 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. As used herein “issuer system” or “issuer institution system” may refer to one or more systems operated by or operated on behalf of an issuer. For example, an issuer system may refer to a server executing one or more software applications associated with the issuer. In some non-limiting aspects of the present disclosure, an issuer system may include one or more servers (*e.g.*, one or more authorization servers) for authorizing a payment transaction. An “issuer” can include a payment account issuer. The payment account (which may be associated with one or more payment devices) may refer to any suitable payment account (*e.g.*, credit card account, a checking account, a savings account, a merchant account assigned to a consumer, or a prepaid account), an employment account, an identification account, an enrollment account (*e.g.*, a student account), etc.

[0041] Referring again to FIG. 1, the network 114 may include one or more wired and/or wireless networks. For example, the network 114 may include a cellular network (*e.g.*, a long-term evolution (LTE) network, a fourth generation (4G) network, a fifth generation (5G) network, a code division multiple access (CDMA) network, etc.), a public land mobile network (PLMN), a local area network (LAN), a wide area network (WAN), a metropolitan area network (MAN), a telephone network (*e.g.*, the public switched telephone network (PSTN)), a private network, an ad hoc network, an intranet, the Internet, a fiber optic-based

network, a cloud computing network, and/or the like, and/or a combination of these or other types of networks.

[0042] The number and arrangement of devices, systems, and networks shown in the payment network environment 100 of FIG. 1 are provided as an example. There may be additional devices, systems, and/or networks, fewer devices, systems, and/or networks, different devices, systems, and/or networks, or differently arranged devices, systems, and/or networks than those shown in FIG. 1. Furthermore, two or more devices shown in FIG. 1 may be implemented within a single device, or a single device shown in FIG. 1 may be implemented as multiple, distributed devices. Additionally or alternatively, a set of devices (*e.g.*, one or more devices) of the payment network environment 100 may perform one or more functions described as being performed by another set of devices of the payment network environment 100.

[0043] FIG. 2 is a swimlane diagram illustrating a method 200 for implementing a randomized application transaction counter (ATC) in a payment card transaction, according to at least one aspect of the present disclosure. The method 200 can be carried out across the payment network environment 100 (FIG. 1). For example, the method 200 may be implemented using the payment card 106, the access device 104, and a host device 120. In some aspects, the host device 120 may be comprised in the issuer system 108. In other aspects, the host device 120 may be comprised in the transaction service provider system 110.

[0044] Referring primarily to FIG. 2, and also to FIG. 1, the payment card 106 can store 202 a card ATC_n and the host device can store 204 a host ATC_n. In some aspects, the card ATC_n and the host ATC_n may be a two-byte hexadecimal value in a range of 0x0000 to 0x7FFF (*e.g.*, with a corresponding decimal integer value in a range of 0 to 32767). In other aspects, the card ATC_n and the host ATC_n may be a two-byte hexadecimal value in a range of 0x0000 to 0xFFFF (*e.g.*, with a corresponding decimal value integer in a range of 0 to 65535).

[0045] The card ATC_n and the host ATC_n have the same value. For example, upon issuance of the payment card 106 (*e.g.*, by an issuer associated with the host device 120) an initial ATC (card $ATC_{n=0}$) may be designated to the payment card 106 and stored 202 on a memory of the payment card 106. The same initial ATC (host $ATC_{n=0}$) may be stored 204 on a memory of the host device 120 and associated with a PAN of the payment card 106. The initial ATC (card $ATC_{n=0}$ = host $ATC_{n=0}$) may be a randomly generated value.

[0046] Referring still primarily to FIG. 2, and also to FIG. 1, according to the method 200, the access device 104 may initiate 206 a transaction based on an interaction with the

payment card 106. For example, the access device 104 may initiate 206 the transaction based on the payment card 106 interacting with a card reader of the access device 104 (*e.g.*, as the result of a user tapping the card proximate to the card reader or dipping the card into the card reader). Based on initiating 206 the transaction, the access device 104 can send 208 a request for a cryptogram (*e.g.*, an application cryptogram) to the payment card 106. The payment card 106 can receive 210 the request for the cryptogram from the access device 104.

[0047] Based on receiving 210 the request, the payment card 106 can calculate 212 a next card ATC_{n+1} based on the stored 202 card ATC_n. The next card ATC_{n+1} can be calculated 212 by applying the stored 202 card ATC_n to a pseudorandom number generator algorithm. Thus, rather than choosing the next card ATC_{n+1} by incrementally increasing the stored ATC_n (*e.g.*, 0, 1, 2, 3, 4, etc.), the value of the next card ATC_{n+1} can be a random value that is calculated 212 by the pseudorandom number generator algorithm (4556, 51131, 92, 3001, 781, etc.).

[0048] In some aspects, the pseudorandom number generator algorithm used to calculate 212 the next card ATC_{n+1} based on the stored 202 card ATC_n can be a linear congruential generator (LCG) algorithm. The LCG algorithm may be defined by the following function:

$$X_{n+1} = (aX_n + c) \bmod m$$

In the above function, each of the parameters *a*, *c*, and *m* are constants. Those of ordinary skill in the art will understand that *a*, *c*, and *m* can be selected to ensure that each calculated value of X_{n+1} is random with respect to X_n. The above function can be used to randomly calculate 212 next card ATC_{n+1} based on the stored 202 card ATC_n, as shown below:

$$\mathrm{ATC}_{n+1} = (a\mathrm{ATC}_n + c) \bmod m$$

In some aspects, an entity associated with the host device 120 (*e.g.*, an issuer associated with the host device 120) can select the parameters *a*, *c*, and *m* to be used by the LCG algorithm.

[0049] Referring still primarily to FIG. 2, and also to FIG. 1, the payment card 106 can generate 214 a cryptogram (*e.g.*, an application cryptogram) based on the card ATC_{n+1}. In some aspects, the cryptogram can be generated 214 according to existing Europay Mastercard Visa (EMV) standards, except that the randomly determined card ATC_{n+1} is used. For example, a master key may be stored by the payment card 106. A session key may be derived for the transaction by diversifying the master key with the card ATC_{n+1}. The session key may then be applied to a cryptographic algorithm (*e.g.*, a Triple Data Encryption Standard (3DES) algorithm) to generate the cryptogram.

[0050] Referring still primarily to FIG. 2, and also to FIG. 1, the payment card 106 can send 216 the calculated 212 card ATC_{n+1} and the generated 214 cryptogram to the access device 104. The access device 104 can receive 218 the card ATC_{n+1} and the cryptogram and send 219 a transaction authorization request comprising the card ATC_{n+1} and the cryptogram to the host device 120. The host device 120 can receive 220 the transaction authorization request comprising the card ATC_{n+1} and the cryptogram. In some aspects, the transaction authorization request may be communicated through one or more intermediaries (*e.g.*, the payment gateway system 102, the acquirer system 112, and/or the transaction service provider system 110) between being sent 219 by the access device 104 and received 220 by the host device 120.

[0051] Referring still primarily to FIG. 2, and also to FIG. 1, as noted above, the host device 120 can store 204 a host ATC_n that is the same value as the card ATC_n stored 202 by the payment card 106. Using the same technique employed by the payment card 106 to calculate 212 the next card ATC_{n+1} based on the stored 202 card ATC_n, the host device 120 can calculate 222 the next host ATC_{n+1} based on the stored 204 host ATC_n. For example, the host device 120 can calculate 222 the next host ATC_{n+1} using the same pseudorandom number generator algorithm, with the same parameters, as is used by the payment card 106 to calculate 212 the next card ATC_{n+1}. Accordingly, both the next card ATC_{n+1} calculated 212 by the payment card 106 and the next host ATC_{n+1} calculated 222 by the host device 120 can be the same value.

[0052] Referring still primarily to FIG. 2, and also to FIG. 1, the host device 120 can generate 224 a cryptogram based on the host ATC_{n+1}. The host device 120 can generate 224 the cryptogram based on the host ATC_{n+1} using the same technique employed by the payment card 106 to generate 214 the cryptogram based on the card ATC_{n+1}. For example, the host device 120 may determine a master key corresponding to the payment card 106. The host device 120 can derive a session key by diversifying the master key with the host ATC_{n+1}. The host device 120 may then apply the session key to a cryptographic algorithm to generate the cryptogram.

[0053] Referring still primarily to FIG. 2, and also to FIG. 1, the host device 120 can determine 226 whether the card ATC_{n+1} and the cryptogram included in the received 220 authorization request are valid. The host device 120 can perform this validation by comparing the card ATC_{n+1} to the host ATC_{n+1} and by comparing the cryptogram included in the authorization request to the cryptogram generated 224 by the host device 120. If the card ATC_{n+1} and the host ATC_{n+1} match and the cryptograms match, then the host device 120 may proceed 228 with the transaction authorization according to existing methods (*e.g.*, determining whether the account associated with the payment card 106 has sufficient funds

for the transaction, etc.). However, if the card ATC_{n+1} and the host ATC_{n+1} do not match, then the card ATC_{n+1} may be invalid. Similarly, if the cryptogram included in the authorization request does not match the cryptogram generated 224 by the host device 120, then the cryptogram included in the authorization request may be invalid. An invalid card ATC_{n+1} and/or an invalid cryptogram can indicate that a fraudster is attempting to conduct a fraudulent transaction using stolen information from the payment card 106. Where the host device 120 determines 226 that the card ATC_{n+1} and/or the cryptogram included in the authorization request are invalid, the host device 120 may decline 230 the transaction.

[0054] Referring still primarily to FIG. 2, and also to FIG. 1, the payment card 106 may store 232 the calculated 212 card ATC_{n+1}. For a next transaction using the payment card 106, the payment card 106 may retrieve the stored 232 card ATC_{n+1} for the calculation of yet a next card ATC_{n+2}. For example, the stored 232 card ATC_{n+1} may replace the stored 202 card ATC_n and the method 200 may be repeated as described herein for the next transaction using the payment card 106.

[0055] Similarly, the host device 120 may store 234 the calculated 222 host ATC_{n+1}. For a next transaction authorization request received 220 based on a next transaction using the payment card 106, the host device 120 may retrieve the stored 234 host ATC_{n+1} for the calculation of yet a next host ATC_{n+2}. For example, the stored 234 host ATC_{n+1} may replace the stored 204 ATC_n and the method 200 may be repeated as described herein for the next transaction using the payment card 106. Thus, this method 200 may be repeated every time the payment card 106 is used to conduct a transaction, with a next card ATC_{n+1} and a next host ATC_{n+1} having the same value being randomly generated for each transaction.

[0056] According to some aspects of the method 200, the transaction initiated 206 by the access device 104 may be an online transaction. Where the transaction is an online transaction, the method 200 may generally proceed as described above, for example.

[0057] According to other aspects of the method 200, the transaction initiated 206 by the access device 104 may be an offline transaction with deferred authorization. For example, the transaction initiated 206 by the access device 104 may be a first offline transaction. The payment card 106 may calculate 212 a first card ATC_{n+1} for the first offline transaction. Following the first offline transaction, the payment card 106 may be used to conduct a second offline transaction (or an online transaction) and may calculate 212 a second card ATC_{n+2} for the second offline transaction. The host device 120 may receive 220 the transaction authorization request for the second offline transaction (including the second card ATC_{n+2}) prior to receiving 220 the transaction authorization request for the first offline transaction (including the first card ATC_{n+1}).

[0058] In order to be able to validate card ATCs for multiple offline transactions (and/or a mix of online and offline transactions) that may be received 220 in a different order than the transactions were initiated 206, according to some aspects of the method 200, calculating 222 the next host ATC_{n+1} can include calculating a set of next host ATC values (*e.g.*, host ATC_{n+1}, host ATC_{n+2}, . . . ATC_{n+k}). Each host ATC in the set may be calculated by sequentially applying an output host ATC value calculated by the pseudorandom number generator algorithm as an input host ATC value for calculating a next ATC value of the set of ATC values until a predetermined number (k) of ATC values is calculated. The predetermined number of ATC values calculated for the set can be selected based on a desired window size for deferred authorization. In this aspect, determining 226 whether the first card ATC_{n+1} in the transaction authorization request for the first transaction is valid can include comparing the first card ATC_{n+1} to the set of host ATC values. Similarly, determining 226 whether the second card ATC_{n+2} in the transaction authorization request for the second transaction is valid can include comparing the second card ATC_{n+2} to the set of host ATC values. In each case, the host device 120 can determine that the card ATC is valid, even if the second card ATC_{n+2} is received before the first card ATC_{n+1}, because both the first card ATC_{n+1} and the second card ATC_{n+2} are included in the set of host ATC values.

[0059] FIG. 3 shows a swimlane diagram illustrating a method 300 for implementing a randomized application transaction counter (ATC) in a payment card transaction, according to at least one aspect of the present disclosure. The method 300 can be similar to the method 200 (FIG. 2) in many respects. Any of the aspects of the method 200 described herein can be applied to the method 300 and vice versa. The method 300 can be carried out across the payment network environment 100 (FIG. 1) and may be implemented using the payment card 106, the access device 104, and a host device 120.

[0060] Referring primarily to FIG. 3, and also to FIG. 1, the payment card 106 can store 302 a randomized series of card ATC values and the host device can store 304 a randomized series of host ATC values. In some aspects, each of card ATC in the series of card ATC values and each host ATC in the series of host ATC values may be a two-byte hexadecimal value in a range of 0x0000 to 0x7FFF (*e.g.*, with a corresponding decimal integer value in a range of 0 to 32767). In other aspects, each card ATC in the series of card ATC values and each host ATC in the series of host ATC values may be a two-byte hexadecimal value in a range of 0x0000 to 0xFFFF (*e.g.*, with a corresponding decimal value integer in a range of 0 to 65535).

[0061] The randomized series of card ATC values stored 302 by the payment card 106 and the randomized series of host ATC values stored 304 by the host device 120 can be the same series of ATC values stored the same order. For example, upon issuance of the

payment card 106 (*e.g.*, by an issuer associated with the host device 120), a unique randomized series of ATC values may be generated for the payment card 106. In one aspect, the randomized series of card ATC values may be generated by selecting an ordered sequence of ATC values (*e.g.*, 0, 1, 2, 3, 4 . . . 65534, 65535) and applying the ordered sequence to a shuffle algorithm, such as Fisher-Yates shuffle algorithm, to randomize the sequence (*e.g.*, 4556, 51131, 92 . . . 3001, 781). The randomized series of ATC values can be designated to the payment card 106 and stored 302 on a memory of the payment card 106 as the randomized series of card ATC values. The same randomized series of ATC values may be stored 304 on a memory of the host device 120 as the randomized series of host ATC values and associated with a PAN of the payment card 106. A different randomized series of ATC values can be generated for each payment card 106 that is issued.

[0062] Referring still primarily to FIG. 3, and also to FIG. 1, according to the method 300, the access device 104 may initiate 306 a transaction based on an interaction with the payment card 106. Based on initiating 306 the transaction, the access device 104 can send 308 a request for a cryptogram (*e.g.*, an application cryptogram) to the payment card 106. The payment card 106 can receive 310 the request for the cryptogram from the access device 104.

[0063] Based on receiving 310 the request, the payment card 106 can select 312 a next card ATC from the series of randomized card ATC values stored 302 by the card. This selection can be performed based on a counter that is increased 332 each time a transaction is carried out using the payment card 106. Thus, rather than choosing the next card ATC based on an ordered sequence of ATC values (*e.g.*, 0, 1, 2, 3, 4, etc.), the value of the next card ATC can be a random value selected from a randomized sequence of ATC values (*e.g.*, 4556, 51131, 92 . . . 3001, 781).

[0064] Referring still primarily to FIG. 3, and also to FIG. 1, the payment card 106 can generate 314 a cryptogram (*e.g.*, an application cryptogram) based on the selected 312 card. In some aspects, the cryptogram can be generated 314 according to existing Europay Mastercard Visa (EMV) standards, except that the card ATC used to generate 314 the cryptogram is selected 312 from a randomize sequence of ATC values rather than an ordered sequence of ATC values. For example, a master key may be stored by the payment card 106. A session key may be derived for the transaction by diversifying the master key with the selected 312 card ATC. The session key may then be applied to a cryptographic algorithm (*e.g.*, a Triple Data Encryption Standard (3DES) algorithm) to generate the cryptogram.

[0065] Referring still primarily to FIG. 3, and also to FIG. 1, the payment card 106 can send 316 the selected 312 card ATC and the generated 314 cryptogram to the access device 104. The access device 104 can receive 318 the card ATC and the cryptogram and send 319 a transaction authorization request comprising the card ATC and the cryptogram to the host device 120. The host device 120 can receive 320 the transaction authorization request comprising the card ATC and the cryptogram. In some aspects, the transaction authorization request may be communicated through one or more intermediaries (*e.g.*, the payment gateway system 102, the acquirer system 112, and/or the transaction service provider system 110) between being sent 319 by the access device 104 and received 320 by the host device 120.

[0066] Referring still primarily to FIG. 3, and also to FIG. 1, as noted above, the host device 120 can store 304 a randomized series of host ATC values that is the same the randomized series of card ATC values stored 302 by the payment card 106. The host device 120 can maintain a counter that is increased 334 every time it processes a transaction from the payment card 106. As valid transactions are processed, the payment card 106 increases its counter and the host device 120 increases 334 its counter such that the counters correspond to one another. The host device 120 can select 322 a host ATC from the stored 304 series of randomized host ATC values based on the host device 120 counter. Where a valid transaction is being processes, the host ATC selected 322 by the host device 120 matches the card ATC selected 312 by the payment card.

[0067] Referring still primarily to FIG. 3, and also to FIG. 1, the host device 120 can generate 324 a cryptogram based on the selected 322 host ATC. The host device 120 can generate 324 the cryptogram based on the selected 322 host ATC using the same technique employed by the payment card 106 to generate 314 the cryptogram based on the selected 312 card ATC.

[0068] Referring still primarily to FIG. 3, and also to FIG. 1, the host device 120 can determine 326 whether the card ATC and the cryptogram included in the received 320 authorization request are valid. The host device 120 can perform this validation by comparing the card ATC to the host ATC and by comparing the cryptogram included in the authorization request to the cryptogram generated 324 by the host device 120. If the card ATC and the host ATC match and the cryptograms match, then the host device 120 may proceed 328 with the transaction authorization according to existing methods (*e.g.*, determining whether the account associated with the payment card 106 has sufficient funds for the transaction, etc.). However, if the card ATC and the host ATC do not match, then the card ATC may be invalid. Similarly, if the cryptogram included in the authorization request does not match the cryptogram generated 324 by the host device 120, then the cryptogram

included in the authorization request may be invalid. An invalid card ATC and/or an invalid cryptogram can indicate that a fraudster is attempting to conduct a fraudulent transaction using stolen information from the payment card 106. Where the host device 120 determines 326 that the card ATC and/or the cryptogram included in the authorization request are invalid, the host device 120 may decline 330 the transaction.

[0069] Referring still primarily to FIG. 3, and also to FIG. 1, as noted above, the payment card 106 can increase 332 a card ATC series counter every time the payment card 106 is used to conduct a transaction and the host device 120 can increase 334 a host ATC series counter every time the host device 120 processes a transaction corresponding to the payment card 106. Thus, to carry out a next transaction using the payment card 106, the method 300 may be repeated as described above, where the payment card 106 will select 312 the next card ATC from the randomized series of card ATC values and the host device 120 will select 322 a corresponding next host ATC from the randomized shears of host ATC values.

[0070] According to some aspects of the method 300, the transaction initiated 306 by the access device 104 may be an online transaction. Where the transaction is an online transaction, the method 300 may generally proceed as described above, for example.

[0071] According to other aspects of the method 300, the transaction initiated 306 by the access device 104 may be an offline transaction with deferred authorization. For example, the transaction initiated 206 by the access device 104 may be a first offline transaction. In order to be able to validate card ATCs for multiple offline transactions (and/or a mix of online and offline transactions) that may be received 320 in a different order than the transactions were initiated 306, according to some aspects of the method 300, selecting 322 a host ATC from the randomized series of host ATC values can include selecting a predetermined number (k) of the next host ATC values in the series. The predetermined number (k) of ATC values can be selected based on a desired window size for deferred authorization. In this aspect, determining 326 whether the card ATC in the transaction authorization request for an offline transaction valid can include comparing the card ATC to the predetermined number (k) of the next host ATC values in the series. This can enable the host device 120 to validate transaction authorization requests for offline transactions that may be received 320 in a different order than the transactions were initiated 306.

[0072] FIG. 4 is a flow diagram of a method 400 for implementing a randomized application transaction counter (ATC) in a payment card transaction, according to at least one aspect of the present disclosure. The method 400 can be similar to the method 200 (FIG. 2) in many respects. Any of the aspects of the method 200 described herein can be

applied to the method 400 and vice versa. In some aspects, the method 300 can be carried by the payment card 106 communicating with the access device 104.

[0073] Referring primarily to FIG. 4, and also to FIG. 1, according to the method 400, the payment card 106 can store 402 a first ATC value. The payment card 106 can receive 404 a request for a cryptogram from the access device 104. The request for the cryptogram may be based on a transaction initiated using the payment card 106 and the access device 104. The payment card 106 can calculate 406 a second ATC value by applying the first ATC value to a pseudorandom number generator algorithm and generate 408 the cryptogram based on the second ATC value. Further, the payment card 106 can send 410 the second ATC value and the cryptogram to the access device. The payment card 106 can store 412 the second ATC value.

[0074] According to one aspect of the method 400, the payment card 106 can calculate 406 the second ATC value by applying the first ATC value to a linear congruential generator algorithm.

[0075] According to one aspect of the method 400, the first ATC value is stored 402 by the payment card based on an issuance of the payment card by an issuer (*e.g.*, an issuer associated with the issuer system 108 (FIG. 1)).

[0076] According to one aspect of the method 400, the request received 404 by the payment card 106 is a first request, the transaction corresponding to the request is a first transaction, and the cryptogram generated 408 by the payment card 106 is a first cryptogram. Further, the access device 104 can be a first access device. In this aspect, according to the method 400, the payment card 106 can receive a second request for a second cryptogram from a second access device. The second request can be based on a second transaction initiated using the payment card 106 and the second access device. The payment card 106 can calculate a third ATC value by applying the second ATC value to the pseudorandom number generator algorithm and generate the second cryptogram based on the third ATC value. The payment card 106 can send the third ATC value and the second cryptogram to the second access device. Further, the payment card 106 can store the third ATC value.

[0077] According to one aspect of the method 400, the payment card 106 can generate 408 the cryptogram based on the second ATC value by diversifying a session key based on the second ATC value and generating the cryptogram based on the session key.

[0078] According to one aspect of the method 400, the transaction is an online transaction. Further, generating 408 the cryptogram based on the second ATC value can include generating an authorization request cryptogram (ARQC).

[0079] FIG. 5 is a flow diagram of method 500 for implementing a randomized application transaction counter (ATC) in a payment card transaction, according to at least one aspect of the present disclosure. The method 500 can be similar to the method 200 (FIG. 2) in many respects and/or may be similar to the method 300 (FIG. 3) in many respects. Any of the aspects of the method 200 and/or the method 300 described herein can be applied to the method 500 and vice versa. In some aspects, the method 500 can be carried out by a circuit of the payment card 106 communicating with the access device 104.

[0080] Referring primarily to FIG. 5, and also to FIG. 1, according to the method 500, the payment card 106 can receive 502 a first request for a first cryptogram. The first request can be based on a first transaction initiated using the payment card 106. The payment card 106 can determine 504 a first ATC value for use with the first transaction and generate 506 the first cryptogram based on the first ATC value. Further, the payment card 106 can receive 508 a second request for a second cryptogram. The second request can be based on a second transaction initiated using the payment card 106. The second transaction can be the next transaction initiated by the payment card 106 following the first transaction. The payment card 106 determine 510 a second ATC value for use with the second transaction and generate 512 the second cryptogram based on the second ATC value. The second ATC value is not determined by incrementally and/or linearly increasing the first ATC value.

[0081] According to one aspect of the method 500, the payment card 106 can apply the first ATC value to a pseudorandom number generator algorithm to determine 510 the second ATC value. The pseudorandom number generator algorithm can be a linear congruential generator algorithm, for example.

[0082] According to one aspect of the method 500, the payment card 106 can store an initial ATC value. The initial ATC value may be provided by an issuer (*e.g.*, an issuer associated with the issuer system 108) of the payment card 106 based on issuing the payment card 106. The payment card 106 can apply the initial ATC value to a pseudorandom number generator algorithm to determine 504 the first ATC value.

[0083] According to one aspect of the method 500, the payment card can store a randomized series of ATC values. The randomized series of ATC values can include the first ATC value and the second ATC value. The randomized series of ATC values may be provided by an issuer (*e.g.*, an issuer associated with the issuer system 108) of the payment card 106 based on issuing the payment card 106. The randomized series of ATC values may be randomized based on a Fisher-Yates shuffle algorithm, for example.

[0084] According to one aspect of the method 500, the payment card 106 comprises a circuit is configured according to a Europay Mastercard Visa (EMV) standard.

[0085] FIG. 6 is a flow diagram of a method 600 for implementing a randomized application transaction counter (ATC) in a payment card transaction, according to at least one aspect of the present disclosure. The method 600 can be similar to the method 200 (FIG. 2) in many respects. Any of the aspects of the method 200 described herein can be applied to the method 600 and vice versa. In some aspects, the method 600 can be carried by an issuer system 108. In other aspects, the method 600 can be carried out by a transaction service provider system 110 rather than the issuer system 108 described below. The issuer system 108 and/or the transaction service provider system 110 can sometimes be referred to as a host device 120.

[0086] Referring primarily to FIG. 6, and also to FIG. 1, according to the method 600, the issuer system 108 can store 602 a first ATC value associated with the payment card 106. The issuer system 108 can receive 604 a transaction authorization request. The transaction authorization request can include a transaction ATC value. The transaction authorization request can be based on a transaction initiated using the payment card 106. The issuer system 108 can calculate 606 a second ATC value by applying the first ATC value to a pseudorandom number generator algorithm. Further, the issuer system 108 can compare 608 the transaction ATC value and the second ATC value.

[0087] According to one aspect of the method 600, the issuer system 108 can authorize the transaction based on the transaction ATC value matching the second ATC value. In another aspect of the method 600, the issuer system 108 can decline the transaction based on the transaction ATC value not matching the second ATC value.

[0088] According to one aspect of the method 600, the issuer system can store the second ATC value.

[0089] According to one aspect of the method 600, the transaction authorization request received 604 by the issuer system 108 can further include a cryptogram generated based on the transaction ATC value. In this aspect, the issuer system 108 can generate a session key based on the transaction ATC value and validate the cryptogram based on the session key.

[0090] According to one aspect of the method 600, the transaction is an offline transaction and the transaction authorization request received 604 by the issuer system 108 is a deferred authorization request. In this aspect, the issuer system 108 can calculate a set of ATC values. The set of ATC values includes a predetermined number of ATC values. Calculating the set of ATC values can include sequentially applying an output ATC value calculated by the pseudorandom number generator algorithm as an input ATC value for calculating a next ATC value of the set of ATC values until the predetermined number of ATC values is calculated. Further, the issuer system 108 can compare the transaction ATC

value to the set of ATC values. The issuer system 108 can authorize the deferred authorization request based on the transaction ATC value matching one ATC value from the set of ATC values.

[0091] FIG. 7 is a block diagram of a computer apparatus 3000 comprising data processing subsystems or components, according to at least one aspect of the present disclosure. The subsystems shown in FIG. 7 are interconnected via a system bus 3010. Additional subsystems such as a printer 3018, keyboard 3026, fixed disk 3028 (or other memory comprising computer readable media), monitor 3022, which is coupled to a display adapter 3020, and others are shown. Peripherals and input/output (I/O) devices, which couple to an I/O controller 3012 (which can be a processor or other suitable controller), can be connected to the computer system by any number of means known in the art, such as a serial port 3024. For example, the serial port 3024 or external interface 3030 can be used to connect the computer apparatus to a wide area network such as the Internet, a mouse input device, or a scanner. The interconnection via system bus allows the central processor 3016 to communicate with each subsystem and to control the execution of instructions from system memory 3014 or the fixed disk 3028, as well as the exchange of information between subsystems. The system memory 3014 and/or the fixed disk 3028 may embody a computer readable medium.

[0092] FIG. 8 is a diagrammatic representation of an example computing system 4000 that includes a host machine 4002 within which a set of instructions to perform various aspects any one or more of the methodologies discussed herein may be executed, such as, for example, the method 200 of FIG. 2, the method 300 of FIG. 3, and the method 600 of FIG. 6, according to at least one aspect of the present disclosure. In various aspects, the host machine 4002 operates as a standalone device or may be connected (*e.g.*, networked) to other machines. In a networked deployment, the host machine 4002 may operate in the capacity of a server or a client machine in a server-client network environment, or as a peer machine in a peer-to-peer (or distributed) network environment. The host machine 4002 may be a computer or computing device, a personal computer (PC), a tablet PC, a set-top box (STB), a personal digital assistant (PDA), a cellular telephone, a portable music player (*e.g.*, a portable hard drive audio device such as an Moving Picture Experts Group Audio Layer 3 (MP3) player), a web appliance, a network router, switch or bridge, or any machine capable of executing a set of instructions (sequential or otherwise) that specify actions to be taken by that machine. Further, while only a single machine is illustrated, the term “machine” shall also be taken to include any collection of machines that individually or jointly execute a set (or multiple sets) of instructions to perform any one or more of the methodologies discussed herein.

[0093] The example system 4000 includes the host machine 4002, running a host operating system (OS) 4004 on a processor or multiple processor(s)/processor core(s) 4006 (*e.g.*, a central processing unit (CPU), a graphics processing unit (GPU), or both), and various memory nodes 4008. The host OS 4004 may include a hypervisor 4010 which is able to control the functions and/or communicate with a virtual machine ("VM") 4012 running on machine readable media. The VM 4012 also may include a virtual CPU or vCPU 4014. The memory nodes 4008 may be linked or pinned to virtual memory nodes or vNodes 4016. When the memory node 4008 is linked or pinned to a corresponding vNode 4016, then data may be mapped directly from the memory nodes 4008 to the corresponding vNode 4016.

[0094] All the various components shown in host machine 4002 may be connected with and to each other, or communicate to each other via a bus (not shown) or via other coupling or communication channels or mechanisms. The host machine 4002 may further include a video display, audio device or other peripherals 4018 (*e.g.*, a liquid crystal display (LCD), alpha-numeric input device(s) including, *e.g.*, a keyboard, a cursor control device, *e.g.*, a mouse, a voice recognition or biometric verification unit, an external drive, a signal generation device, *e.g.*, a speaker,) a persistent storage device 4020 (also referred to as disk drive unit), and a network interface device 4022. The host machine 4002 may further include a data encryption module (not shown) to encrypt data. The components provided in the host machine 4002 are those typically found in computer systems that may be suitable for use with aspects of the present disclosure and are intended to represent a broad category of such computer components that are known in the art. Thus, the system 4000 can be a server, minicomputer, mainframe computer, or any other computer system. The computer may also include different bus configurations, networked platforms, multi-processor platforms, and the like. Various operating systems may be used including UNIX, LINUX, WINDOWS, QNX ANDROID, IOS, CHROME, TIZEN, and other suitable operating systems.

[0095] The disk drive unit 4024 also may be a Solid-state Drive (SSD), a hard disk drive (HDD) or other includes a computer or machine-readable medium on which is stored one or more sets of instructions and data structures (*e.g.*, data/instructions 4026) embodying or utilizing any one or more of the methodologies or functions described herein. The data/instructions 4026 also may reside, completely or at least partially, within the main memory node 4008 and/or within the processor(s) 4006 during execution thereof by the host machine 4002. The data/instructions 4026 may further be transmitted or received over a network 4028 via the network interface device 4022 utilizing any one of several well-known transfer protocols (*e.g.*, Hyper Text Transfer Protocol (HTTP)).

[0096] The processor(s) 4006 and memory nodes 4008 also may comprise machine-

readable media. The term "computer-readable medium" or “machine-readable medium” should be taken to include a single medium or multiple medium (*e.g.*, a centralized or distributed database and/or associated caches and servers) that store the one or more sets of instructions. The term "computer-readable medium" shall also be taken to include any medium that is capable of storing, encoding, or carrying a set of instructions for execution by the host machine 4002 and that causes the host machine 4002 to perform any one or more of the methodologies of the present application, or that is capable of storing, encoding, or carrying data structures utilized by or associated with such a set of instructions. The term ”computer-readable medium” shall accordingly be taken to include, but not be limited to, solid-state memories, optical and magnetic media, and carrier wave signals. Such media may also include, without limitation, hard disks, floppy disks, flash memory cards, digital video disks, random access memory (RAM), read only memory (ROM), and the like. The example aspects described herein may be implemented in an operating environment comprising software installed on a computer, in hardware, or in a combination of software and hardware.

[0097] One skilled in the art will recognize that Internet service may be configured to provide Internet access to one or more computing devices that are coupled to the Internet service, and that the computing devices may include one or more processors, buses, memory devices, display devices, input/output devices, and the like. Furthermore, those skilled in the art may appreciate that the Internet service may be coupled to one or more databases, repositories, servers, and the like, which may be utilized to implement any of the various aspects of the disclosure as described herein.

[0098] The computer program instructions also may be loaded onto a computer, a server, other programmable data processing apparatus, or other devices to cause a series of operational steps to be performed on the computer, other programmable apparatus or other devices to produce a computer implemented process such that the instructions which execute on the computer or other programmable apparatus provide processes for implementing the functions/acts specified in the flowchart and/or block diagram block or blocks.

[0099] Suitable networks may include or interface with any one or more of, for instance, a local intranet, a PAN (Personal Area Network), a LAN (Local Area Network), a WAN (Wide Area Network), a MAN (Metropolitan Area Network), a virtual private network (VPN), a storage area network (SAN), a frame relay connection, an Advanced Intelligent Network (AIN) connection, a synchronous optical network (SONET) connection, a digital T1, T3, E1 or E3 line, Digital Data Service (DDS) connection, DSL (Digital Subscriber Line) connection, an Ethernet connection, an ISDN (Integrated Services Digital Network) line, a dial-up port

such as a V.90, V.34 or V.34bis analog modem connection, a cable modem, an ATM (Asynchronous Transfer Mode) connection, or an FDDI (Fiber Distributed Data Interface) or CDDI (Copper Distributed Data Interface) connection. Furthermore, communications may also include links to any of a variety of wireless networks, including WAP (Wireless Application Protocol), GPRS (General Packet Radio Service), GSM (Global System for Mobile Communication), CDMA (Code Division Multiple Access) or TDMA (Time Division Multiple Access), cellular phone networks, GPS (Global Positioning System), CDPD (cellular digital packet data), RIM (Research in Motion, Limited) duplex paging network, Bluetooth radio, or an IEEE 802.11-based radio frequency network. The network 4028 can further include or interface with any one or more of an RS-232 serial connection, an IEEE-1394 (Firewire) connection, a Fiber Channel connection, an IrDA (infrared) port, a SCSI (Small Computer Systems Interface) connection, a USB (Universal Serial Bus) connection or other wired or wireless, digital or analog interface or connection, mesh or Digi® networking.

[0100] In general, a cloud-based computing environment is a resource that typically combines the computational power of a large grouping of processors (such as within web servers) and/or that combines the storage capacity of a large grouping of computer memories or storage devices. Systems that provide cloud-based resources may be utilized exclusively by their owners or such systems may be accessible to outside users who deploy applications within the computing infrastructure to obtain the benefit of large computational or storage resources.

[0101] The cloud is formed, for example, by a network of web servers that comprise a plurality of computing devices, such as the host machine 4002, with each server 4030 (or at least a plurality thereof) providing processor and/or storage resources. These servers manage workloads provided by multiple users (*e.g.*, cloud resource customers or other users). Typically, each user places workload demands upon the cloud that vary in real-time, sometimes dramatically. The nature and extent of these variations typically depends on the type of business associated with the user.

[0102] It is noteworthy that any hardware platform suitable for performing the processing described herein is suitable for use with the technology. The terms “computer-readable storage medium” and “computer-readable storage media” as used herein refer to any medium or media that participate in providing instructions to a CPU for execution. Such media can take many forms, including, but not limited to, non-volatile media, volatile media, and transmission media. Non-volatile media include, for example, optical or magnetic disks, such as a fixed disk. Volatile media include dynamic memory, such as system RAM. Transmission media include coaxial cables, copper wire and fiber optics, among others, including the wires that comprise one aspect of a bus. Transmission media can also take the

form of acoustic or light waves, such as those generated during radio frequency (RF) and infrared (IR) data communications. Common forms of computer-readable media include, for example, a flexible disk, a hard disk, magnetic tape, any other magnetic medium, a CD-ROM disk, digital video disk (DVD), any other optical medium, any other physical medium with patterns of marks or holes, a RAM, a PROM, an EPROM, an EEPROM, a FLASH EPROM, any other memory chip or data exchange adapter, a carrier wave, or any other medium from which a computer can read.

[0103] Various forms of computer-readable media may be involved in carrying one or more sequences of one or more instructions to a CPU for execution. A bus carries the data to system RAM, from which a CPU retrieves and executes the instructions. The instructions received by system RAM can optionally be stored on a fixed disk either before or after execution by a CPU.

[0104] Computer program code for carrying out operations for aspects of the present technology may be written in any combination of one or more programming languages, including an object oriented programming language such as Java, Smalltalk, C++, or the like and conventional procedural programming languages, such as the "C" programming language, Go, Python, or other programming languages, including assembly languages. The program code may execute entirely on the user's computer, partly on the user's computer, as a stand-alone software package, partly on the user's computer and partly on a remote computer or entirely on the remote computer or server. In the latter scenario, the remote computer may be connected to the user's computer through any type of network, including a local area network (LAN) or a wide area network (WAN), or the connection may be made to an external computer (for example, through the Internet using an Internet Service Provider).

[0105] A “key” may refer to a piece of information that is used in a cryptographic algorithm to transform input data into another representation.

[0106] A “cryptographic algorithm” can be an encryption algorithm that transforms original data into an alternate representation, or a decryption algorithm that transforms encrypted information back to the original data. Examples of cryptographic algorithms may include triple data encryption standard (TDES), data encryption standard (DES), advanced encryption standard (AES), etc. Encryption techniques may include symmetric and asymmetric encryption techniques.

[0107] Examples of the devices, systems, and methods according to various aspects of the present disclosure are provided below in the following numbered clauses. An aspect of any of the devices(s), method(s) and/or system(s) may include any one or more than one, and any combination of, the numbered clauses described below.

[0108] Clause 1: A method for implementing a randomized application transaction counter (ATC) in a payment card transaction, the method comprising: storing, by a payment card, a first ATC value; receiving, by the payment card, a request for a cryptogram from an access device, wherein the request is based on a transaction initiated using the payment card and the access device; calculating, by the payment card, a second ATC value by applying the first ATC value to a pseudorandom number generator algorithm; generating, by the payment card, the cryptogram based on the second ATC value; sending, by the payment card, the second ATC value and the cryptogram to the access device; and storing, by the payment card, the second ATC value.

[0109] Clause 2: The method of Clause 1, wherein calculating the second ATC value by applying the first ATC value to the pseudorandom number generator algorithm comprises applying the first ATC value to a linear congruential generator algorithm.

[0110] Clause 3: The method of any of Clauses 1-2, where the first ATC value is stored by the payment card based on an issuance of the payment card by an issuer.

[0111] Clause 4: The method of any of Clauses 1-3, wherein the request is a first request, wherein the transaction is a first transaction, wherein the cryptogram is a first cryptogram, and wherein the access device is a first access device, the method further comprising: receiving, by the payment card, a second request for a second cryptogram from a second access device, wherein the second request is based on a second transaction initiated using the payment card and the second access device; calculating, by the payment card, a third ATC value by applying the second ATC value to the pseudorandom number generator algorithm; generating, by the payment card, the second cryptogram based on the third ATC value; sending, by the payment card, the third ATC value and the second cryptogram to the second access device; and storing, by the payment card, the third ATC value.

[0112] Clause 5: The method of any of Clauses 1-3, wherein generating, by the payment card, the cryptogram based on the second ATC value comprises: diversifying, by the payment card, a session key based base on the second ATC value; and generating, by the payment card, the cryptogram based on the session key.

[0113] Clause 6: The method of Clauses 1-3, wherein the transaction is an online transaction, and wherein generating the cryptogram based on the second ATC value comprises generating an authorization request cryptogram (ARQC).

[0114] Clause 7: A payment card, comprising: a circuit to: receive a first request for a first cryptogram, wherein the first request is based on a first transaction initiated using the payment card; determine a first application transaction counter (ATC) value for use with the

first transaction; generate the first cryptogram based on the first ATC value; receive a second request for a second cryptogram, wherein the second request is based on a second transaction initiated using the payment card, and wherein the second transaction is the next transaction initiated by the payment card following the first transaction; determine a second ATC value for use with the second transaction, wherein the second ATC value is not determined by incrementally increasing the first ATC value; and generate the second cryptogram based on the second ATC value.

[0115] Clause 8. The payment card of Clause 7, wherein the circuit is to: apply the first ATC value to a pseudorandom number generator algorithm to determine the second ATC value.

[0116] Clause 9: The payment card of Clause 8, wherein the pseudorandom number generator algorithm is a linear congruential generator algorithm.

[0117] Clause 10: The payment card of any of Clauses 8-9, wherein the circuit is further to: store an initial ATC value, wherein the initial ATC value is provided by an issuer of the payment card based on issuing the payment card; and apply the initial ATC value to the pseudorandom number generator algorithm to determine the first ATC value.

[0118] Clause 11: The payment card of Clause 7, wherein the circuit is to: store a randomized series of ATC values, wherein the randomized series of ATC values includes the first ATC value and the second ATC value, and wherein the randomized series of ATC values is provided by an issuer of the payment card based on issuing the payment card.

[0119] Clause 12: The payment card of Clause 11, wherein the randomized series of ATC values is randomized based on a Fisher-Yates shuffle algorithm.

[0120] Clause 13: The payment card of any of Clause 7-12, wherein the circuit is configured according to a Europay Mastercard Visa (EMV) standard.

[0121] Clause 14: A method for implementing a randomized application transaction counter (ATC) in a payment card transaction, the method comprising: storing, by a host server, a first ATC value associated with a payment card; receiving, by the host server, a transaction authorization request, wherein the transaction authorization request comprises a transaction ATC value, and wherein the transaction authorization request is based on a transaction initiated using the payment card; calculating, by the host server, a second ATC value by applying the first ATC value to a pseudorandom number generator algorithm; and comparing, by the host server, the transaction ATC value and the second ATC value.

[0122] Clause 15: The method of Clause 14, further comprising: authorizing, by the host server, the transaction based on the transaction ATC value matching the second ATC value.

[0123] Clause 16: The method of Clause 14, further comprising: declining, by the host server, the transaction based on the transaction ATC value not matching the second ATC value.

[0124] Clause 17: The method of any of Clauses 14-16, further comprising: storing, by the host server, the second ATC value.

[0125] Clause 18: The method of any of Clauses 14-17, wherein the transaction authorization request further comprises a cryptogram generated based on the transaction ATC value, the method further comprising: generating, by the host server, a session key based on the transaction ATC value; and validating, by the host server, the cryptogram based on the session key.

[0126] Clause 19: The method of Clause 14, wherein the transaction is an offline transaction, wherein the transaction authorization request is a deferred online authorization request, the method further comprising: calculating, by the host server, a set of ATC values, wherein the set of ATC values includes a predetermined number of ATC values, and wherein calculating the set of ATC values comprises sequentially applying an output ATC value calculated by the pseudorandom number generator algorithm as an input ATC value for calculating a next ATC value of the set of ATC values until the predetermined number of ATC values is calculated; and comparing, by the host server, the transaction ATC value to the set of ATC values.

[0127] Clause 20: The method of Clause 19, further comprising: authorizing, by the host server, the deferred online authorization request based on the transaction ATC value matching one ATC value from the set of ATC values.

[0128] Further, it is understood that any one or more of the following-described forms, expressions of forms, examples, can be combined with any one or more of the other following-described forms, expressions of forms, and examples.

[0129] While several forms have been illustrated and described, it is not the intention of Applicant to restrict or limit the scope of the appended claims to such detail. Numerous modifications, variations, changes, substitutions, combinations, and equivalents to those forms may be implemented and will occur to those skilled in the art without departing from the scope of the present disclosure. Moreover, the structure of each element associated with the described forms can be alternatively described as a means for providing the function performed by the element. Also, where materials are disclosed for certain components, other materials may be used. It is therefore to be understood that the foregoing description and the appended claims are intended to cover all such modifications, combinations, and variations as falling within the scope of the disclosed forms. The appended claims are intended to

cover all such modifications, variations, changes, substitutions, modifications, and equivalents.

[0130] As used herein, a “server” may include one or more computing devices which can be individual, stand-alone machines located at the same or different locations, may be owned or operated by the same or different entities, and may further be one or more clusters of distributed computers or “virtual” machines housed within a datacenter. It should be understood and appreciated by a person of skill in the art that functions performed by one “server” can be spread across multiple disparate computing devices for various reasons. As used herein, a “server” is intended to refer to all such scenarios and should not be construed or limited to one specific configuration. Further, a server as described herein may, but need not, reside at (or be operated by) a merchant, a payment network, a financial institution, a healthcare provider, a social media provider, a government agency, or agents of any of the aforementioned entities. The term “server” may also refer to or include one or more processors or computers, storage devices, or similar computer arrangements 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 computers, *e.g.*, servers, or other computerized devices, *e.g.*, point-of-sale devices, directly or indirectly communicating in the network environment may constitute a “system,” such as a merchant's point-of-sale 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.

[0131] As used herein, a “server computer” may describe a powerful computer or cluster of computers. For example, the server computer can be a large mainframe, a minicomputer cluster, or a group of servers functioning as a unit. The server computer may be associated with an entity such as a payment processing network, a wallet provider, a merchant, an authentication cloud, an acquirer or an issuer. In one example, the server computer may be a database server coupled to a Web server. The server computer may be coupled to a database and may include any hardware, software, other logic, or combination of the preceding for servicing the requests from one or more client computers. The server computer may comprise one or more computational apparatuses and may use any of a variety of computing structures, arrangements, and compilations for servicing the requests

from one or more client computers. In some embodiments or aspects, the server computer may provide and/or support payment network cloud service.

[0132] Reference to “a device,” “a server,” “a processor,” and/or the like, as used herein, may refer to a previously recited device, server, or processor that is recited as performing a previous step or function, a different server or processor, and/or a combination of servers and/or processors. For example, as used in the specification and the claims, a first server or a first processor that is recited as performing a first step or a first function may refer to the same or different server or the same or different processor recited as performing a second step or a second function.

[0133] One or more components may be referred to herein as “configured to,” “configurable to,” “operable/operative to,” “adapted/adaptable,” “able to,” “conformable/conformed to,” etc. Those skilled in the art will recognize that “configured to” can generally encompass active-state components and/or inactive-state components and/or standby-state components, unless context requires otherwise.

[0134] Those skilled in the art will recognize that, in general, terms used herein, and especially in the appended claims (*e.g.*, bodies of the appended claims) are generally intended as “open” terms (*e.g.*, the term “including” should be interpreted as “including but not limited to,” the term “having” should be interpreted as “having at least,” the term “includes” should be interpreted as “includes but is not limited to,” etc.). It will be further understood by those within the art that if a specific number of an introduced claim recitation is intended, such an intent will be explicitly recited in the claim, and in the absence of such recitation no such intent is present. For example, as an aid to understanding, the following appended claims may contain usage of the introductory phrases “at least one” and “one or more” to introduce claim recitations. However, the use of such phrases should not be construed to imply that the introduction of a claim recitation by the indefinite articles “a” or “an” limits any particular claim containing such introduced claim recitation to claims containing only one such recitation, even when the same claim includes the introductory phrases “one or more” or “at least one” and indefinite articles such as “a” or “an” (*e.g.*, “a” and/or “an” should typically be interpreted to mean “at least one” or “one or more”); the same holds true for the use of definite articles used to introduce claim recitations.

[0135] The term “substantially”, “about”, or “approximately” as used in the present disclosure, unless otherwise specified, means an acceptable error for a particular value as determined by one of ordinary skill in the art, which depends in part on how the value is measured or determined. In certain aspects, the term “substantially”, “about”, or “approximately” means within 1, 2, 3, or 4 standard deviations. In certain aspects, the term

"substantially", "about", or "approximately" means within 50%, 20%, 15%, 10%, 9%, 8%, 7%, 6%, 5%, 4%, 3%, 2%, 1%, 0.5%, or 0.05% of a given value or range.

[0136] In addition, even if a specific number of an introduced claim recitation is explicitly recited, those skilled in the art will recognize that such recitation should typically be interpreted to mean at least the recited number (*e.g.*, the bare recitation of "two recitations," without other modifiers, typically means at least two recitations, or two or more recitations). Furthermore, in those instances where a convention analogous to "at least one of A, B, and C, etc." is used, in general such a construction is intended in the sense one having skill in the art would understand the convention (*e.g.*, "a system having at least one of A, B, and C" would include but not be limited to systems that have A alone, B alone, C alone, A and B together, A and C together, B and C together, and/or A, B, and C together, etc.). In those instances where a convention analogous to "at least one of A, B, or C, etc." is used, in general such a construction is intended in the sense one having skill in the art would understand the convention (*e.g.*, "a system having at least one of A, B, or C" would include but not be limited to systems that have A alone, B alone, C alone, A and B together, A and C together, B and C together, and/or A, B, and C together, etc.). It will be further understood by those within the art that typically a disjunctive word and/or phrase presenting two or more alternative terms, whether in the description, claims, or drawings, should be understood to contemplate the possibilities of including one of the terms, either of the terms, or both terms unless context dictates otherwise. For example, the phrase "A or B" will be typically understood to include the possibilities of "A" or "B" or "A and B."

[0137] With respect to the appended claims, those skilled in the art will appreciate that recited operations therein may generally be performed in any order. Also, although various operational flow diagrams are presented in a sequence(s), it should be understood that the various operations may be performed in other orders than those which are illustrated, or may be performed concurrently. Examples of such alternate orderings may include overlapping, interleaved, interrupted, reordered, incremental, preparatory, supplemental, simultaneous, reverse, or other variant orderings, unless context dictates otherwise. Furthermore, terms like "responsive to," "related to," or other past-tense adjectives are generally not intended to exclude such variants, unless context dictates otherwise.

[0138] It is worthy to note that any reference to "one aspect," "an aspect," "an exemplification," "one exemplification," and the like means that a particular feature, structure, or characteristic described in connection with the aspect is included in at least one aspect. Thus, appearances of the phrases "in one aspect," "in an aspect," "in an exemplification," and "in one exemplification" in various places throughout the specification are not necessarily all referring to the same aspect. Furthermore, the particular features, structures

or characteristics may be combined in any suitable manner in one or more aspects.

[0139] As used herein, the singular form of “a”, “an”, and “the” include the plural references unless the context clearly dictates otherwise.

[0140] Any patent application, patent, non-patent publication, or other disclosure material referred to in this specification and/or listed in any Application Data Sheet is incorporated by reference herein, to the extent that the incorporated materials is not inconsistent herewith. As such, and to the extent necessary, the disclosure as explicitly set forth herein supersedes any conflicting material incorporated herein by reference. Any material, or portion thereof, that is said to be incorporated by reference herein, but which conflicts with existing definitions, statements, or other disclosure material set forth herein will only be incorporated to the extent that no conflict arises between that incorporated material and the existing disclosure material.

[0141] In summary, numerous benefits have been described which result from employing the concepts described herein. The foregoing description of the one or more forms has been presented for purposes of illustration and description. It is not intended to be exhaustive or limiting to the precise form disclosed. Modifications or variations are possible in light of the above teachings. The one or more forms were chosen and described in order to illustrate principles and practical application to thereby enable one of ordinary skill in the art to utilize the various forms and with various modifications as are suited to the particular use contemplated. It is intended that the claims submitted herewith define the overall scope.

CLAIMS

What is claimed is:

1. A method for implementing a randomized application transaction counter (ATC) in a payment card transaction, the method comprising:

storing, by a payment card, a first ATC value;

receiving, by the payment card, a request for a cryptogram from an access device, wherein the request is based on a transaction initiated using the payment card and the access device;

calculating, by the payment card, a second ATC value by applying the first ATC value to a pseudorandom number generator algorithm;

generating, by the payment card, the cryptogram based on the second ATC value;

sending, by the payment card, the second ATC value and the cryptogram to the access device; and

storing, by the payment card, the second ATC value.

2. The method of Claim 1, wherein calculating the second ATC value by applying the first ATC value to the pseudorandom number generator algorithm comprises applying the first ATC value to a linear congruential generator algorithm.

3. The method of Claim 1, where the first ATC value is stored by the payment card based on an issuance of the payment card by an issuer.

4. The method of Claim 1, wherein the request is a first request, wherein the transaction is a first transaction, wherein the cryptogram is a first cryptogram, and wherein the access device is a first access device, the method further comprising:

receiving, by the payment card, a second request for a second cryptogram from a second access device, wherein the second request is based on a second transaction initiated using the payment card and the second access device;

calculating, by the payment card, a third ATC value by applying the second ATC value to the pseudorandom number generator algorithm;

generating, by the payment card, the second cryptogram based on the third ATC value;

sending, by the payment card, the third ATC value and the second cryptogram to the second access device; and

storing, by the payment card, the third ATC value.

5. The method of Claim 1, wherein generating, by the payment card, the cryptogram based on the second ATC value comprises:

diversifying, by the payment card, a session key based base on the second ATC value; and

generating, by the payment card, the cryptogram based on the session key.

6. The method of Claim 1, wherein the transaction is an online transaction, and wherein generating the cryptogram based on the second ATC value comprises generating an authorization request cryptogram (ARQC).

7. A payment card, comprising:

a circuit to:

receive a first request for a first cryptogram, wherein the first request is based on a first transaction initiated using the payment card;

determine a first application transaction counter (ATC) value for use with the first transaction;

generate the first cryptogram based on the first ATC value;

receive a second request for a second cryptogram, wherein the second request is based on a second transaction initiated using the payment card, and wherein the second transaction is the next transaction initiated by the payment card following the first transaction;

determine a second ATC value for use with the second transaction, wherein the second ATC value is not determined by incrementally increasing the first ATC value; and

generate the second cryptogram based on the second ATC value.

8. The payment card of Claim 7, wherein the circuit is to:

apply the first ATC value to a pseudorandom number generator algorithm to determine the second ATC value.

9. The payment card of Claim 8, wherein the pseudorandom number generator algorithm is a linear congruential generator algorithm.

10. The payment card of Claim 8, wherein the circuit is further to:

store an initial ATC value, wherein the initial ATC value is provided by an issuer of the payment card based on issuing the payment card; and

apply the initial ATC value to the pseudorandom number generator algorithm to determine the first ATC value.

11. The payment card of Claim 7, wherein the circuit is to:

store a randomized series of ATC values, wherein the randomized series of ATC values includes the first ATC value and the second ATC value, and wherein the randomized series of ATC values is provided by an issuer of the payment card based on issuing the payment card.

12. The payment card of Claim 11, wherein the randomized series of ATC values is randomized based on a Fisher-Yates shuffle algorithm.

13. The payment card of Claim 7, wherein the circuit is configured according to a Europay Mastercard Visa (EMV) standard.

14. A method for implementing a randomized application transaction counter (ATC) in a payment card transaction, the method comprising:

storing, by a host server, a first ATC value associated with a payment card;

receiving, by the host server, a transaction authorization request, wherein the transaction authorization request comprises a transaction ATC value, and wherein the transaction authorization request is based on a transaction initiated using the payment card;

calculating, by the host server, a second ATC value by applying the first ATC value to a pseudorandom number generator algorithm; and

comparing, by the host server, the transaction ATC value and the second ATC value.

15. The method of Claim 14, further comprising:

authorizing, by the host server, the transaction based on the transaction ATC value matching the second ATC value.

16. The method of Claim 14, further comprising:

declining, by the host server, the transaction based on the transaction ATC value not matching the second ATC value.

17. The method of Claim 14, further comprising:

storing, by the host server, the second ATC value.

18. The method of Claim 14, wherein the transaction authorization request further comprises a cryptogram generated based on the transaction ATC value, the method further comprising:

generating, by the host server, a session key based on the transaction ATC value; and

validating, by the host server, the cryptogram based on the session key.

19. The method of Claim 14, wherein the transaction is an offline transaction, wherein the transaction authorization request is a deferred online authorization request, the method further comprising:

calculating, by the host server, a set of ATC values, wherein the set of ATC values includes a predetermined number of ATC values, and wherein calculating the set of ATC values comprises sequentially applying an output ATC value calculated by the pseudorandom number generator algorithm as an input ATC value for calculating a next ATC value of the set of ATC values until the predetermined number of ATC values is calculated; and

comparing, by the host server, the transaction ATC value to the set of ATC values.

20. The method of Claim 19, further comprising:

authorizing, by the host server, the deferred online authorization request based on the transaction ATC value matching one ATC value from the set of ATC values.

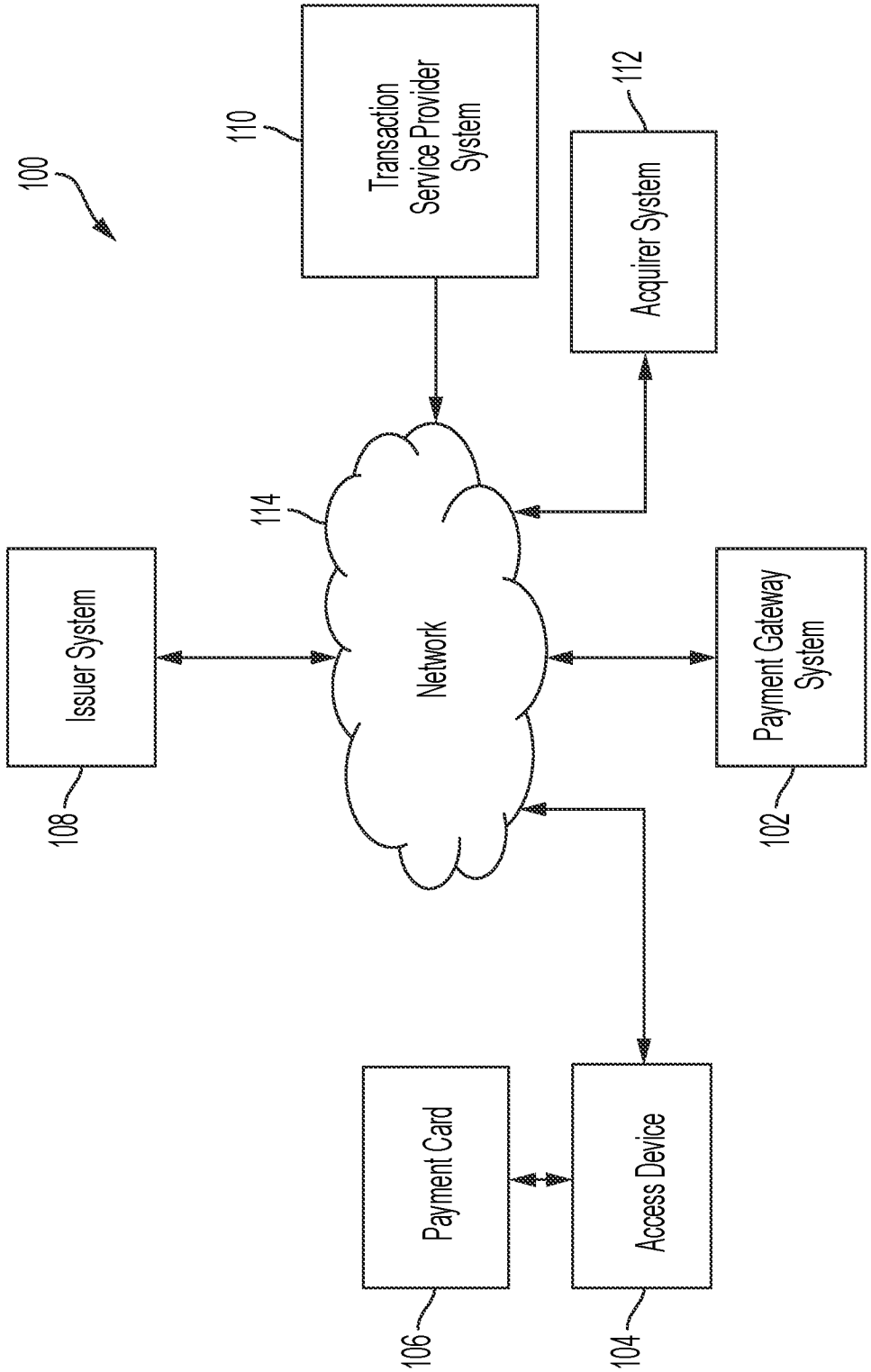
100
Transaction Service Provider System
110
Acquirer System
112
Issuer System
108
Network
114
Payment Gateway System
102
Payment Card
106
Access Device
104

FIG. 1

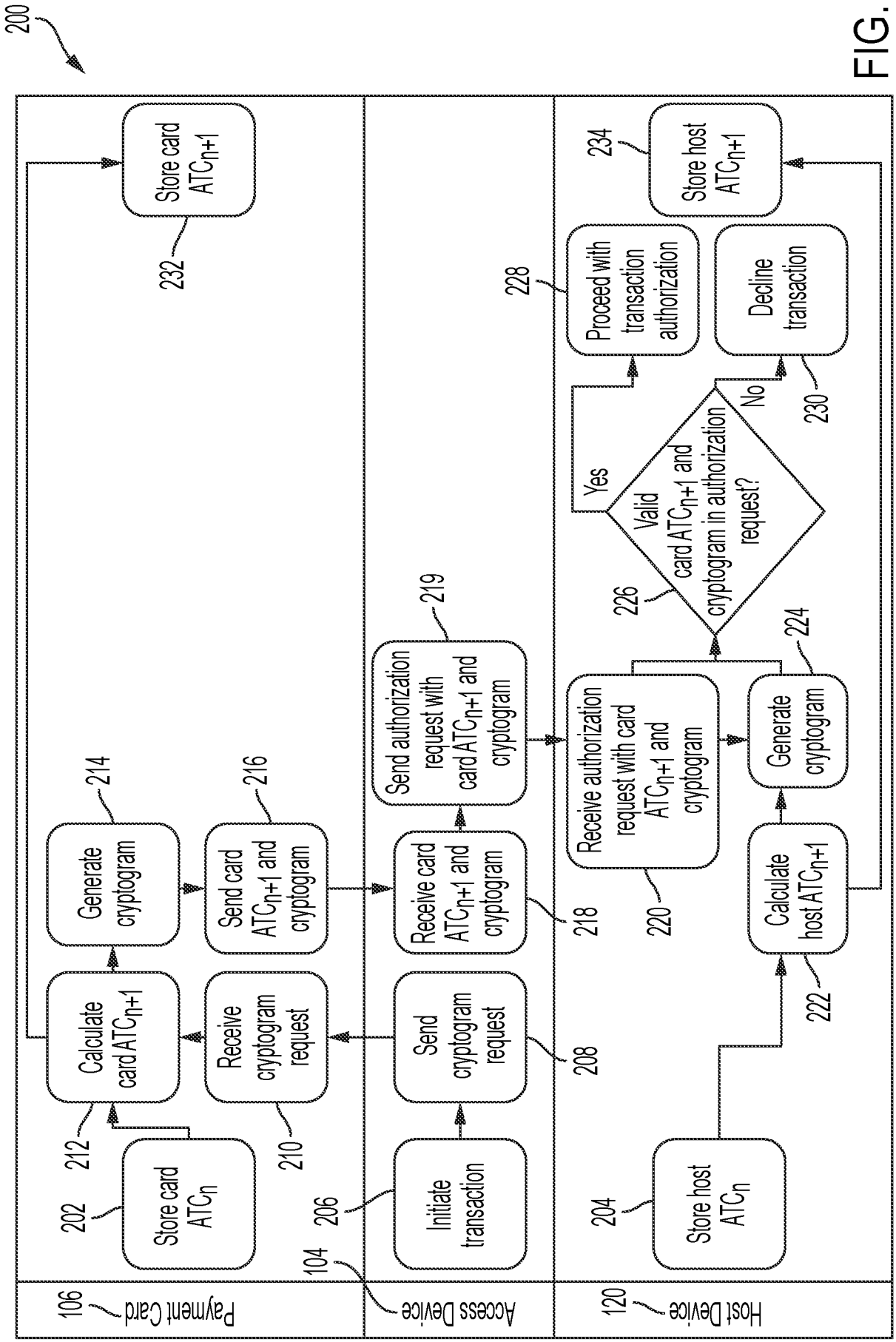
200
Payment Card
106
Access Device
104
Host Device
120
Store card ATCn
202
Calculate card ATCn+1
212
Generate cryptogram
214
Receive cryptogram request
210
Send card ATCn+1 and cryptogram
216
Store card ATCn+1
232
Initiate transaction
206
Send cryptogram request
208
Receive card ATCn+1 and cryptogram
218
Send authorization request with card ATCn+1 and cryptogram
219
Store host ATCn
204
Calculate host ATCn+1
222
Generate cryptogram
224
Receive authorization request with card ATCn+1 and cryptogram
220
Valid card ATCn+1 and cryptogram in authorization request?
226
Yes
No
Proceed with transaction authorization
228
Decline transaction
230
Store host ATCn+1
234

FIG. 2

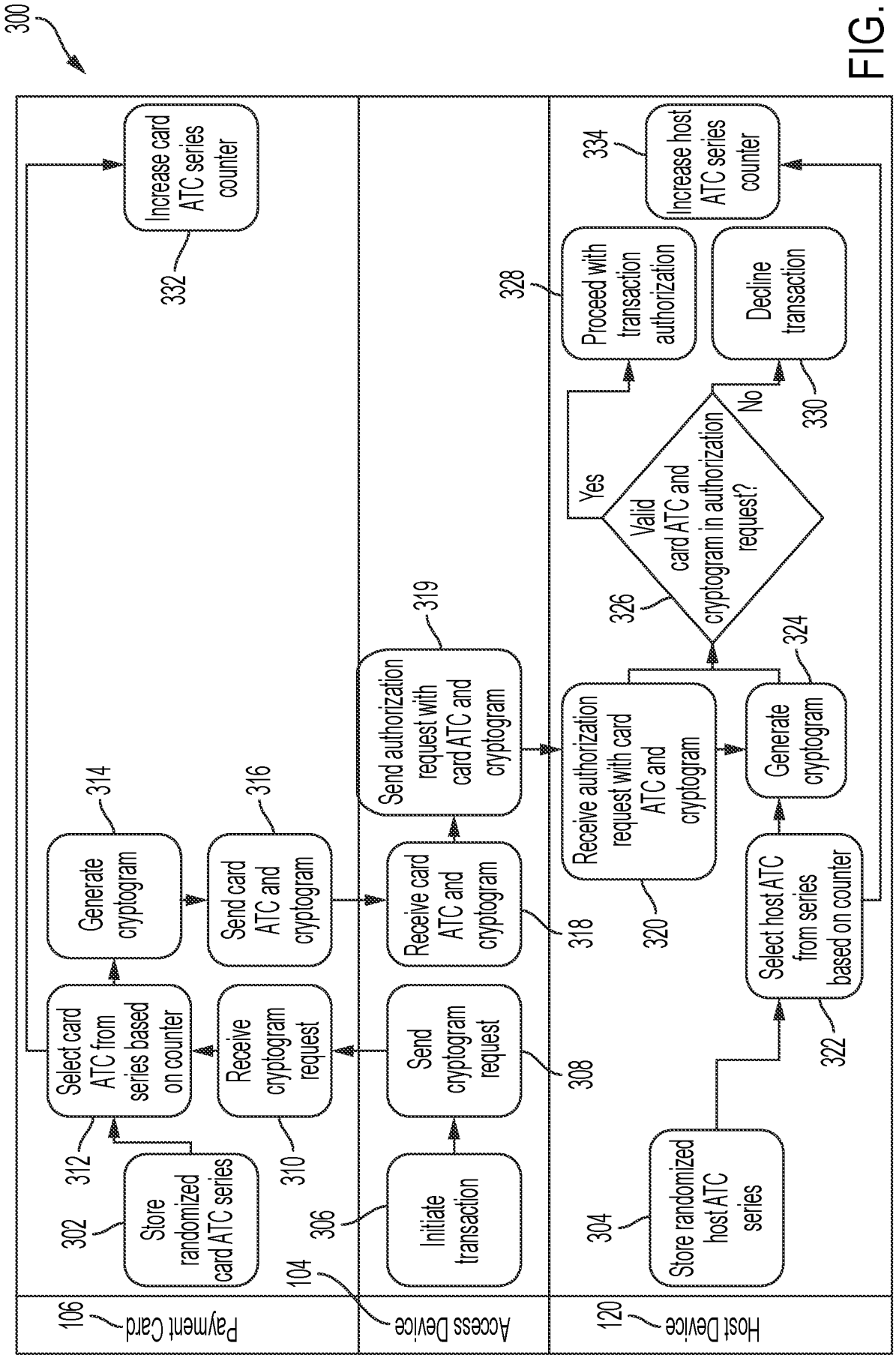
300
Payment Card
106
Access Device
104
Host Device
120
Store randomized card ATC series
302
Select card ATC from series based on counter
312
Generate cryptogram
314
Send card ATC and cryptogram
316
Receive cryptogram request
310
Increase card ATC series counter
332
Initiate transaction
306
Send cryptogram request
308
Receive card ATC and cryptogram
318
Send authorization request with card ATC and cryptogram
319
Store randomized host ATC series
304
Receive authorization request with card ATC and cryptogram
320
Select host ATC from series based on counter
322
Generate cryptogram
324
Valid card ATC and cryptogram in authorization request?
326
Yes
No
Proceed with transaction authorization
328
Decline transaction
330
Increase host ATC series counter
334

FIG. 3

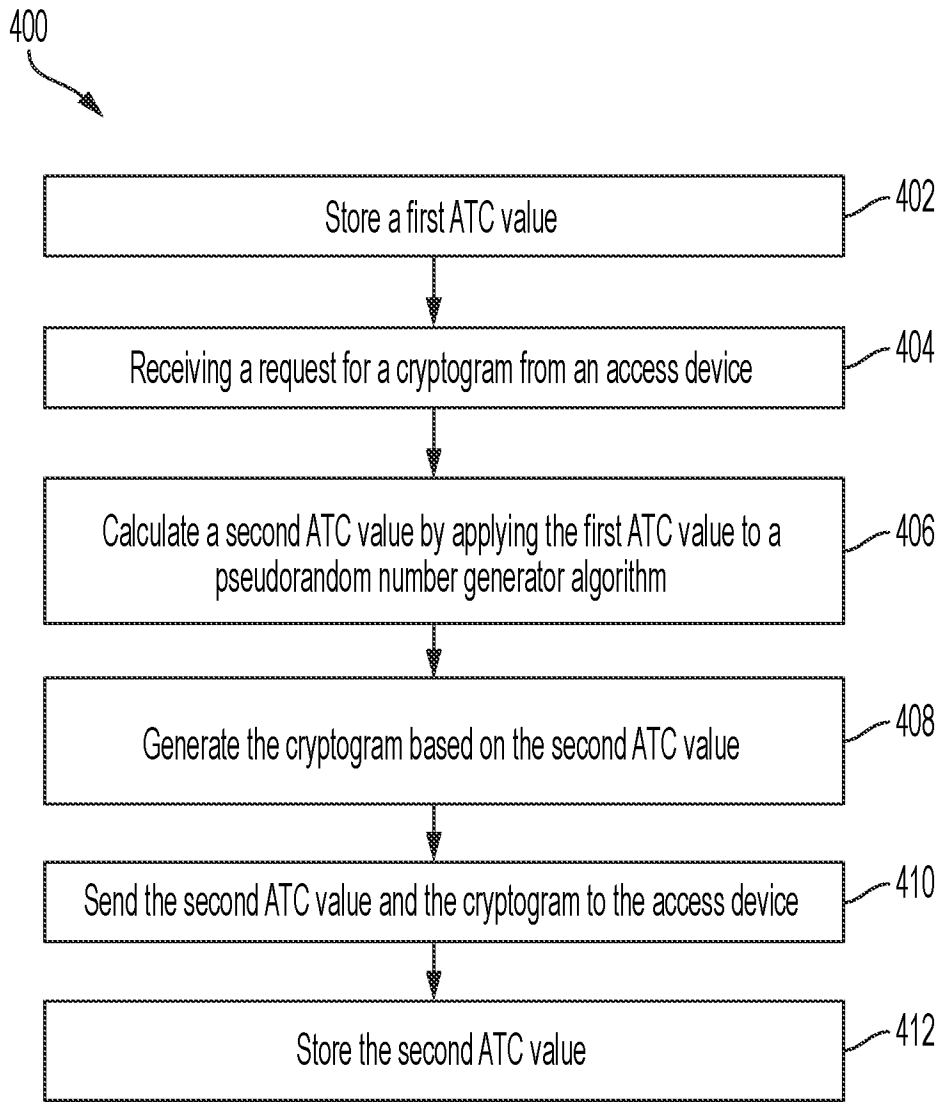
400
Store a first ATC value
402
Receiving a request for a cryptogram from an access device
404
Calculate a second ATC value by applying the first ATC value to a pseudorandom number generator algorithm
406
Generate the cryptogram based on the second ATC value
408
Send the second ATC value and the cryptogram to the access device
410
Store the second ATC value
412

FIG. 4

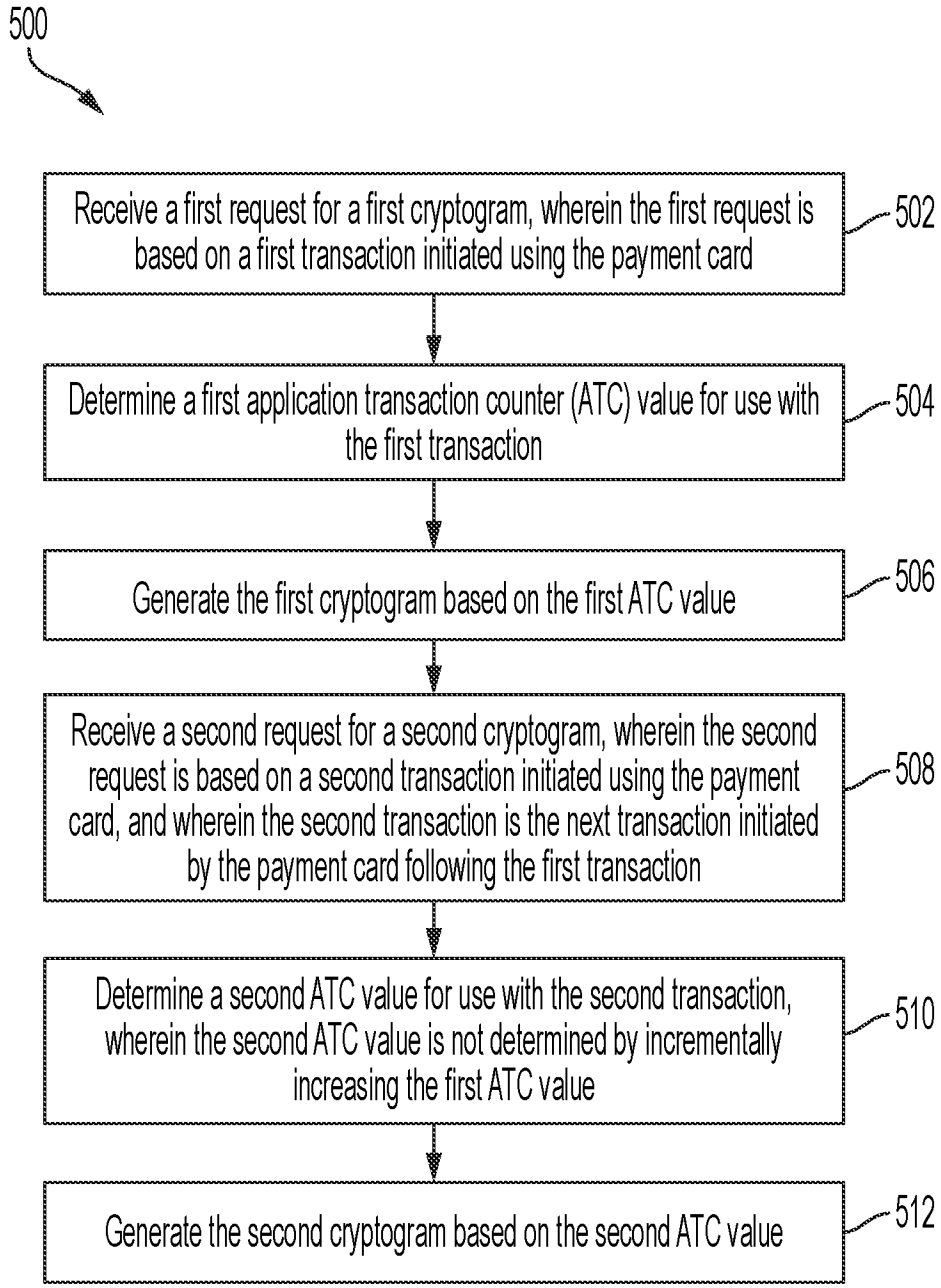
500
Receive a first request for a first cryptogram, wherein the first request is based on a first transaction initiated using the payment card
502
Determine a first application transaction counter (ATC) value for use with the first transaction
504
Generate the first cryptogram based on the first ATC value
506
Receive a second request for a second cryptogram, wherein the second request is based on a second transaction initiated using the payment card, and wherein the second transaction is the next transaction initiated by the payment card following the first transaction
508
Determine a second ATC value for use with the second transaction, wherein the second ATC value is not determined by incrementally increasing the first ATC value
510
Generate the second cryptogram based on the second ATC value
512

FIG. 5

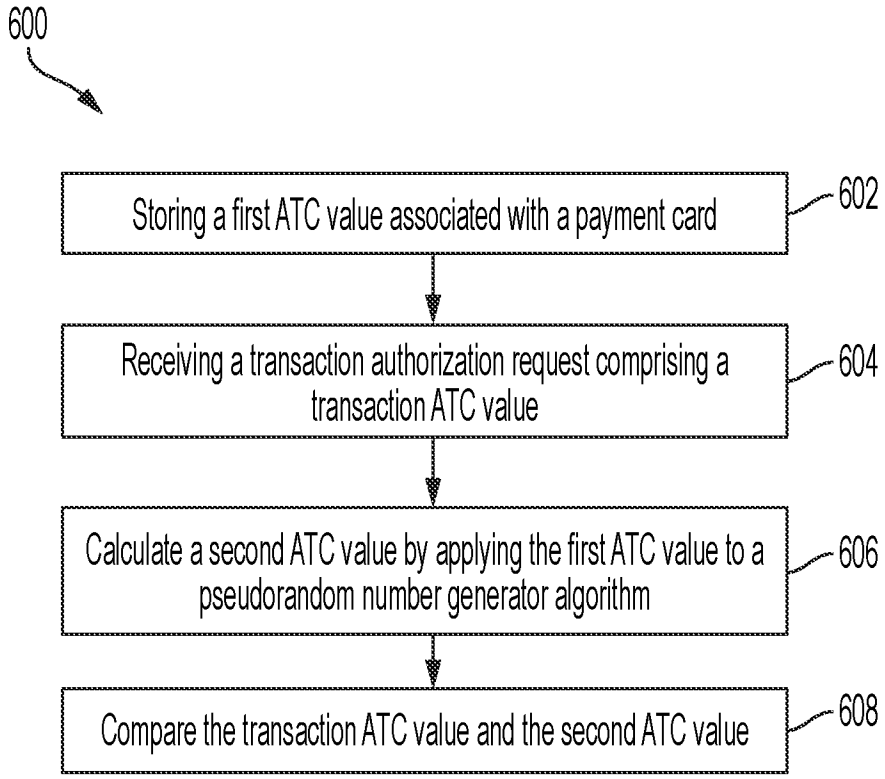
600
Storing a first ATC value associated with a payment card
602
Receiving a transaction authorization request comprising a transaction ATC value
604
Calculate a second ATC value by applying the first ATC value to a pseudorandom number generator algorithm
606
Compare the transaction ATC value and the second ATC value
608

FIG. 6

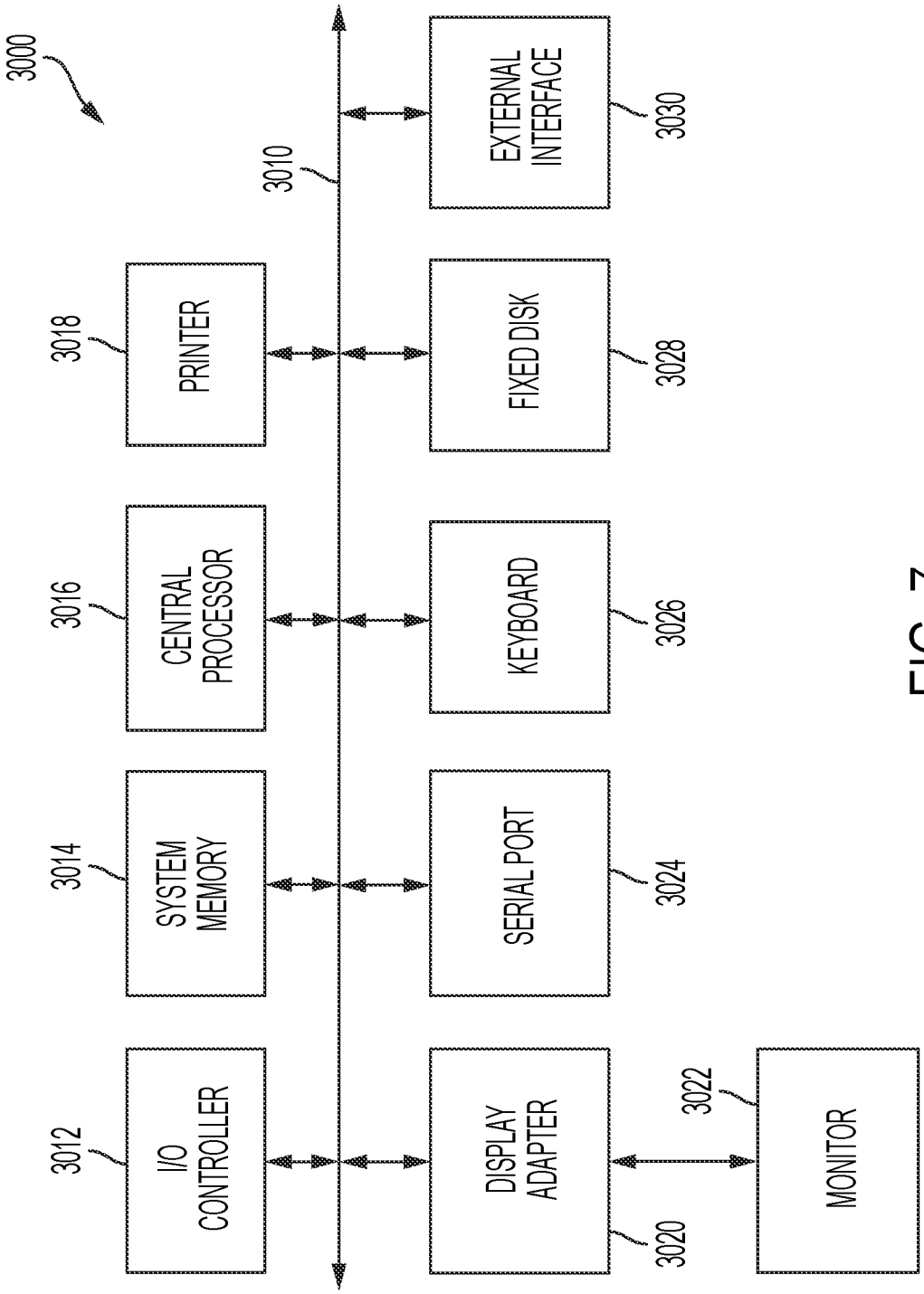
3000
3010
3012
I/O CONTROLLER
3014
SYSTEM MEMORY
3016
CENTRAL PROCESSOR
3018
PRINTER
DISPLAY ADAPTER
3020
3022
MONITOR
SERIAL PORT
3024
KEYBOARD
3026
FIXED DISK
3028
EXTERNAL INTERFACE
3030

FIG. 7

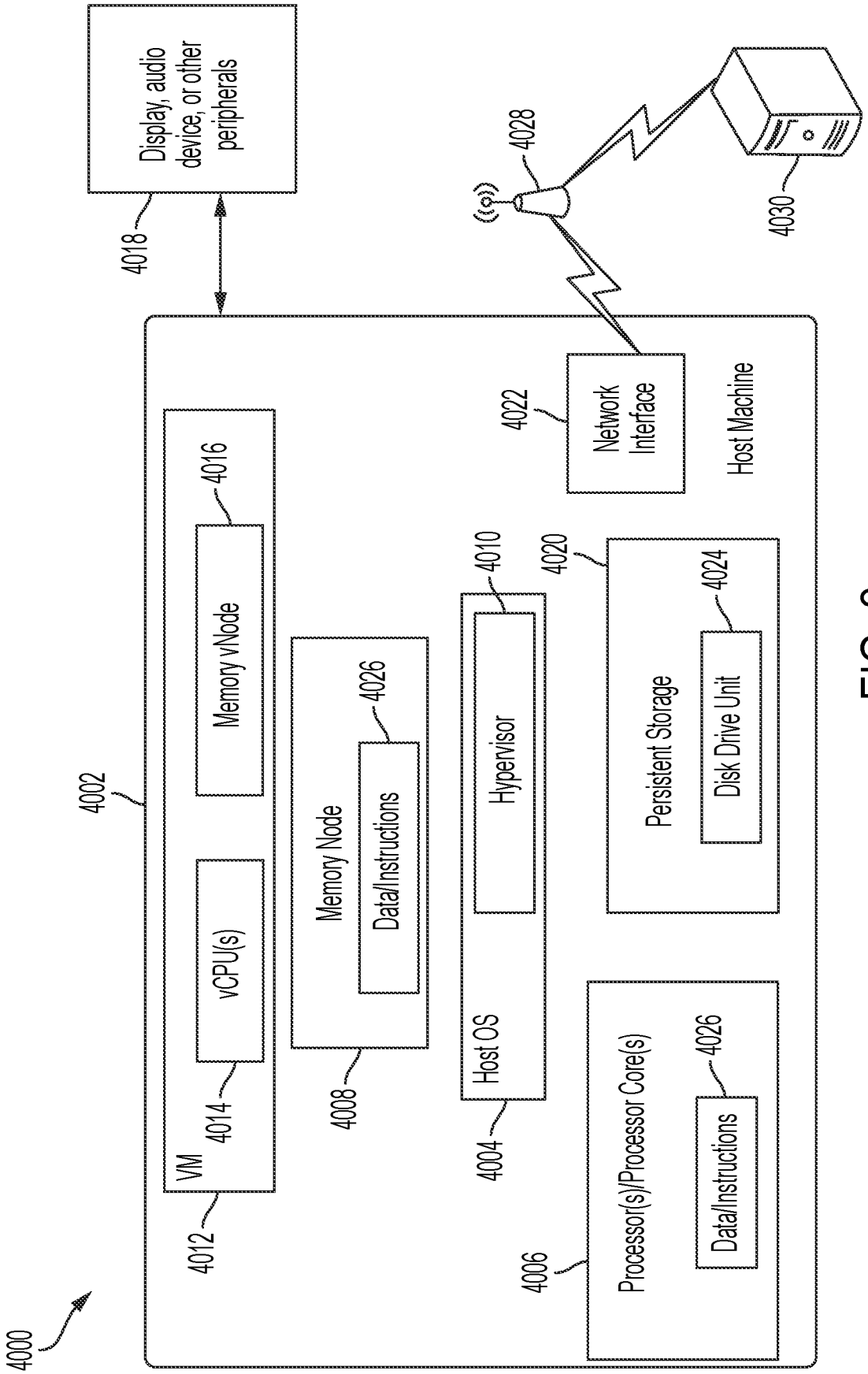
4000
4002
VM
4012
vCPU(s)
4014
Memory vNode
4016
Memory Node
4008
Data/Instructions
4026
Host OS
4004
Hypervisor
4010
Processor(s)/Processor Core(s)
4006
Data/Instructions
4026
Persistent Storage
4020
Disk Drive Unit
4024
Network Interface
4022
Host Machine
Display, audio device, or other peripherals
4018
4028
4030

FIG. 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2023/068519

A. CLASSIFICATION OF SUBJECT MATTER

G06Q 20/38(2012.01)i; **G06Q 20/34**(2012.01)i; **G06Q 20/40**(2012.01)i; **G06Q 20/02**(2012.01)i; **G06F 7/58**(2006.01)i; **H04L 9/08**(2006.01)i

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)

G06Q 20/38(2012.01); G06Q 20/20(2012.01); G06Q 20/28(2012.01); G06Q 20/32(2012.01); G06Q 20/34(2012.01); G06Q 20/40(2012.01); G08B 1/08(2006.01); H04L 9/08(2006.01); H04W 12/06(2009.01); H04W 12/08(2009.01)

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

Korean utility models and applications for utility models
Japanese utility models and applications for utility models

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

eKOMPASS(KIPO internal) & Keywords: payment card, application transaction counter (ATC), cryptogram, pseudorandom, algorithm

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP 2974219 B1 (ASSA ABLOY AB) 16 June 2021 (2021-06-16) See paragraphs 4, 13, 46, 53-57, 70, 80-81, 84 and claim 1.	1-20
Y	US 2006-0012473 A1 (FRED BISHOP et al.) 19 January 2006 (2006-01-19) See paragraphs 37, 39-40, 44, 66-67 and claims 1-2, 6-9, 21-25.	1-20
Y	CN 107392591 A (HENGBAO CORP.) 24 November 2017 (2017-11-24) See claims 1-2.	4,7-13
A	US 2019-0295063 A1 (VISA INTERNATIONAL SERVICE ASSOCIATION) 26 September 2019 (2019-09-26) See the whole document.	1-20
A	WO 2013-130912 A2 (GOOGLE INC.) 06 September 2013 (2013-09-06) See the whole document.	1-20

✓ 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
08 March 2024	**11 March 2024**
Name and mailing address of the ISA/KR **Korean Intellectual Property Office** **189 Cheongsa-ro, Seo-gu, Daejeon** **35208, Republic of Korea** Facsimile No. **+82-42-481-8578**	Authorized officer **LEE Kang Ha** Telephone No. **+82-42-481-5003**

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2023/068519

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2019-0108515 A1 (MASTERCARD INTERNATIONAL INCORPORATED) 11 April 2019 (2019-04-11) See the whole document.	1-20

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2023/068519

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
EP	2974219	B1	16 June 2021	AU	2014-229568	A1	22 October 2015
				AU	2014-229575	A1	22 October 2015
				CA	2904150	A1	18 September 2014
				CA	2905522	A1	18 September 2014
				EP	2974219	A2	20 January 2016
				EP	2974220	A2	20 January 2016
				EP	2974222	A2	20 January 2016
				EP	2974222	B1	02 September 2020
				EP	3910876	A1	17 November 2021
				EP	3998743	A1	18 May 2022
				US	10404682	B2	03 September 2019
				US	10652233	B2	12 May 2020
				US	11026092	B2	01 June 2021
				US	11172365	B2	09 November 2021
				US	11252569	B2	15 February 2022
				US	2016-0021091	A1	21 January 2016
				US	2016-0021100	A1	21 January 2016
				US	2016-0205549	A1	14 July 2016
				US	2018-0097797	A1	05 April 2018
				US	2019-0349352	A1	14 November 2019
				US	2019-0349353	A1	14 November 2019
				US	2019-0379652	A1	12 December 2019
				US	9825941	B2	21 November 2017
				US	9860236	B2	02 January 2018
				WO	2014-140807	A2	18 September 2014
				WO	2014-140807	A3	04 December 2014
				WO	2014-140814	A2	18 September 2014
				WO	2014-140814	A3	04 December 2014
				WO	2014-140818	A2	18 September 2014
				WO	2014-140818	A3	04 December 2014
US	2006-0012473	A1	19 January 2006	AR	025574	A1	04 December 2002
				AR	027848	A1	16 April 2003
				AR	030184	A1	13 August 2003
				AR	041912	A1	01 June 2005
				AT	258328	T	15 February 2004
				AT	311634	T	15 December 2005
				AT	476718	T	15 August 2010
				AT	E258328	T1	15 February 2004
				AU	2000-70907	A1	26 March 2001
				AU	2000-70907	B2	19 August 2004
				AU	2000-73498	A1	10 April 2001
				AU	2000-73498	B2	19 May 2005
				AU	2001-22635	A1	03 July 2001
				AU	2001-232875	B2	12 January 2006
				AU	2001-32875	A1	31 July 2001
				AU	2001-43473	A1	17 September 2001
				AU	2002-248656	B2	30 March 2006
				AU	2002-318293	B2	06 December 2007
				AU	2003-248849	A1	23 January 2004
				AU	2003-259100	A1	23 January 2004

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2023/068519

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
		AU	2003-259100	A8	23 January 2004
		AU	2003-265262	A1	23 January 2004
		AU	2003-265262	A8	23 January 2004
		AU	2003-287337	A1	03 June 2004
		AU	2003-293507	A1	30 June 2004
		AU	2003-293507	A8	30 June 2004
		AU	2003-297858	A1	30 June 2004
		AU	2004-216969	A1	16 September 2004
		AU	2004-216969	B2	06 December 2007
		AU	2004-216969	C1	30 October 2008
		AU	2004-216969	C1	06 December 2007
		AU	2004-231226	A1	23 December 2004
		AU	2004-231226	B2	05 June 2008
		AU	2005-266964	A1	02 February 2006
		AU	2005-266964	B2	03 February 2011
		AU	2005-277794	A1	02 March 2006
		AU	2005-292417	A1	13 April 2006
		AU	2005-292417	B2	31 March 2011
		AU	2005-294782	A1	20 April 2006
		AU	2005-295684	A1	27 April 2006
		AU	2005-295684	B2	24 December 2009
		AU	2005-295767	A1	27 April 2006
		AU	2006-348401	A1	22 May 2008
		AU	2006-348401	A8	16 June 2011
		AU	2006-348401	A8	22 May 2008
		AU	2006-348401	B2	02 June 2011
		AU	2006-348401	B8	02 June 2011
		AU	2006-348401	B8	16 June 2011
		AU	2008-276123	A1	22 January 2009
		AU	2008-276123	B2	18 August 2011
		AU	2011-203221	A1	21 July 2011
		AU	2011-203221	B2	21 February 2013
		BR	0013822	A	23 July 2002
		BR	0014018	A	21 May 2002
		BR	0208536	A	14 September 2004
		BR	0210962	A	08 June 2004
		BR	0304735	A	06 July 2004
		CA	2382882	A1	15 March 2001
		CA	2382882	C	24 April 2007
		CA	2382922	A1	08 March 2001
		CA	2382922	C	13 December 2011
		CA	2397722	A1	26 July 2001
		CA	2397722	C	20 May 2014
		CA	2410006	A1	29 November 2001
		CA	2442518	A1	10 October 2002
		CA	2452351	A1	23 January 2003
		CA	2458143	A1	15 January 2004
		CA	2509552	A1	24 June 2004
		CA	2509680	A1	24 June 2004
		CA	2518481	A1	16 September 2004

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2023/068519

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
		CA	2575096	A1	02 February 2006
		CA	2578360	A1	02 March 2006
		CA	2580485	A1	20 April 2006
		CA	2583402	A1	13 April 2006
		CA	2583782	A1	27 April 2006
		CA	2584094	A1	27 April 2006
		CA	2693136	A1	22 January 2009
		CA	2693136	C	03 July 2012
		CA	2753375	A1	08 March 2001
		CA	2753375	C	22 September 2015
		CA	2836286	A1	13 April 2006
		CA	2893917	A1	08 March 2001
		CA	2893917	C	17 January 2017
		CN	100370838	C	20 February 2008
		CN	101187989	A	28 May 2008
		CN	101187989	C	28 May 2008
		CN	101583968	A	18 November 2009
		CN	104933564	A	23 September 2015
		CN	1235175	C	04 January 2006
		CN	1376292	A	23 October 2002
		CN	1387660	A	25 December 2002
		CN	1539246	A	20 October 2004
		CN	1682222	A	12 October 2005
		CN	1682222	C	12 October 2005
		CR	6597	A	22 July 2004
		CR	6604	A	27 April 2004
		CZ	20020744	A3	18 February 2004
		CZ	20020776	A3	11 September 2002
		CZ	2002744	A3	18 February 2004
		CZ	2002776	A3	11 September 2002
		DE	60007883	T2	14 October 2004
		DE	60024478	T2	17 August 2006
		DK	1212732	T3	07 June 2004
		DK	1222620	T3	18 April 2006
		DK	1222620	T5	03 July 2006
		DZ	3214	A1	08 March 2001
		DZ	3215	A1	15 March 2001
		EP	1148040	A1	24 October 2001
		EP	1148040	B1	05 January 2005
		EP	1212732	A2	12 June 2002
		EP	1212732	B1	21 January 2004
		EP	1222620	A2	17 July 2002
		EP	1222620	B1	30 November 2005
		EP	1261945	A2	04 December 2002
		EP	1350175	A1	08 October 2003
		EP	1386268	A2	04 February 2004
		EP	1413150	A2	28 April 2004
		EP	1563421	A2	17 August 2005
		EP	1570418	A2	07 September 2005
		EP	1570418	B1	04 August 2010

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2023/068519

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
		EP	1570420	A1	07 September 2005
		EP	1599818	A2	30 November 2005
		EP	1610897	A1	04 January 2006
		EP	1728188	A2	06 December 2006
		EP	1794708	A2	13 June 2007
		EP	1805699	A1	11 July 2007
		EP	1815320	A2	08 August 2007
		EP	1815411	A2	08 August 2007
		EP	1815419	A2	08 August 2007
		EP	1828971	A2	05 September 2007
		EP	1958121	A2	20 August 2008
		EP	2183120	A1	12 May 2010
		EP	2183120	B1	26 August 2015
		EP	2291793	A1	09 March 2011
		ES	2215064	T3	01 October 2004
		ES	2256037	T3	16 July 2006
		HK	1047810	A1	07 March 2003
		HK	1047810	B	11 August 2006
		HK	1048184	A1	21 March 2003
		HK	1048550	A1	04 April 2003
		HK	1048550	B	21 October 2004
		HR	20020180	A2	30 June 2004
		HR	20020197	A2	31 October 2004
		HR	P20020180	A2	30 June 2004
		HR	P20020197	A2	31 October 2004
		HU	0202471	A2	28 November 2002
		HU	0202700	A2	28 December 2002
		HU	226649	B1	28 May 2009
		IL	148319	A0	12 September 2002
		IL	148319	B	05 February 2006
		IL	148320	A0	12 September 2002
		IL	148320	B	08 July 2008
		JP	2002-097165	A	02 April 2002
		JP	2003-508838	A	04 March 2003
		JP	2003-509231	A	11 March 2003
		JP	2003-521052	A	08 July 2003
		JP	2004-535640	A	25 November 2004
		JP	2005-520269	A	07 July 2005
		JP	2006-510138	A	23 March 2006
		JP	2006-513071	A	20 April 2006
		JP	2006-519426	A	24 August 2006
		JP	2007-066316	A	15 March 2007
		JP	2007-220104	A	30 August 2007
		JP	2008-165810	A	17 July 2008
		JP	2009-076057	A	09 April 2009
		JP	2009-301578	A	24 December 2009
		JP	2010-533923	A	28 October 2010
		JP	2011-060291	A	24 March 2011
		JP	2013-137780	A	11 July 2013
		JP	4777917	B2	21 September 2011

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2023/068519

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
		JP	4792652	B2	12 October 2011
		JP	4934807	B2	23 May 2012
		JP	5439322	B2	12 March 2014
		JP	5643854	B2	17 December 2014
		KR	10-0584646	B1	30 May 2006
		KR	10-0699954	B1	27 March 2007
		KR	10-0728530	B1	14 June 2007
		KR	10-0806993	B1	25 February 2008
		KR	10-2002-0039339	A	25 May 2002
		KR	10-2002-0042669	A	05 June 2002
		KR	10-2002-0070500	A	09 September 2002
		KR	10-2004-0024867	A	22 March 2004
		KR	10-2004-0028939	A	03 April 2004
		MA	27459	A1	01 August 2005
		MA	29420	B1	02 May 2008
		MX	2010000677	A	20 December 2010
		MX	PA02002081	A	30 July 2004
		MX	PA02002446	A	10 September 2004
		MX	PA02007142	A	27 May 2003
		MX	PA02011602	A	05 April 2004
		MX	PA04000189	A	18 June 2004
		MX	PA04000253	A	04 May 2004
		MX	PA05009378	A	05 December 2005
		NO	20020996	A	24 April 2002
		NO	20020996	D0	28 February 2002
		NO	20020996	L	24 April 2002
		NO	20021105	A	06 May 2002
		NO	20021105	D0	06 March 2002
		NO	20021105	L	06 May 2002
		NZ	517720	A	26 March 2004
		NZ	517840	A	24 March 2005
		NZ	530497	A	25 November 2005
		PL	353773	A1	01 December 2003
		PL	354415	A1	12 January 2004
		PT	1212732	E	30 June 2004
		PT	1212732	T	30 June 2004
		RU	2252451	C2	20 May 2005
		RU	2265247	C2	27 November 2005
		SI	1212732	T1	31 October 2004
		SI	EP1212732	T1	31 October 2004
		TR	200201280	T2	21 August 2002
		TR	200201399	T2	21 November 2002
		TR	200202436	T2	21 January 2003
		TW	200422964	A	01 November 2004
		TW	240209	A	21 September 2005
		TW	504647	A	01 October 2002
		TW	504647	B	01 October 2002
		TW	535078	B	01 June 2003
		TW	544605	B	01 August 2003
		TW	548564	B	21 August 2003

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2023/068519

Patent document cited in search report			Publication date (day/month/year)	Patent family member(s)			Publication date (day/month/year)
				TW	I240209	B	21 September 2005
				US	6417410	B1	09 July 2002
				US	6581839	B1	24 June 2003
				US	6742704	B2	01 June 2004
				US	6749123	B2	15 June 2004
				US	6764014	B2	20 July 2004
				US	6997378	B2	14 February 2006
				US	7035872	B2	25 April 2006
				US	7059531	B2	13 June 2006
				US	7070112	B2	04 July 2006
				US	7093767	B2	22 August 2006
				US	7119659	B2	10 October 2006
				US	7121471	B2	17 October 2006
				US	7154375	B2	26 December 2006
				US	7156301	B1	02 January 2007
				US	7163145	B2	16 January 2007
				US	7172112	B2	06 February 2007
				US	7222101	B2	22 May 2007
				US	7228155	B2	05 June 2007
				US	7239226	B2	03 July 2007
				US	7249112	B2	24 July 2007
				US	7268667	B2	11 September 2007
				US	7268668	B2	11 September 2007
				US	7303120	B2	04 December 2007
				US	7306158	B2	11 December 2007
				US	7312707	B1	25 December 2007
				US	7343351	B1	11 March 2008
				US	7360689	B2	22 April 2008
CN	107392591	A	24 November 2017	CN	107392591	B	07 February 2020
US	2019-0295063	A1	26 September 2019	AU	2014-368949	A1	09 June 2016
				BR	112016014106	A2	08 August 2017
				CA	2931093	A1	25 June 2015
				CN	105830107	A	03 August 2016
				CN	115082065	A	20 September 2022
				EP	3084701	A1	26 October 2016
				EP	3084701	A4	09 August 2017
				EP	3084701	B1	04 May 2022
				EP	4057203	A1	14 September 2022
				JP	2017-507518	A	16 March 2017
				JP	2019-180097	A	17 October 2019
				JP	6551850	B2	31 July 2019
				KR	10-2016-0101117	A	24 August 2016
				KR	10-2021-0024669	A	05 March 2021
				KR	10-2021-0107894	A	01 September 2021
				KR	10-2022-0084421	A	21 June 2022
				KR	10-2221636	B1	03 March 2021
				KR	10-2293822	B1	26 August 2021
				KR	10-2408299	B1	13 June 2022
				KR	10-2526100	B1	26 April 2023
				RU	2016129192	A	24 January 2018

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2023/068519

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
		RU 2019111186 A	07 May 2019
		RU 2686014 C1	23 April 2019
		SG 10201900964 A	28 March 2019
		SG 11201604906 A	28 July 2016
		US 10402814 B2	03 September 2019
		US 10664824 B2	26 May 2020
		US 10909522 B2	02 February 2021
		US 11017386 B2	25 May 2021
		US 11164176 B2	02 November 2021
		US 2015-0178724 A1	25 June 2015
		US 2015-0180836 A1	25 June 2015
		US 2016-0140545 A1	19 May 2016
		US 2016-0217452 A1	28 July 2016
		US 2018-0189783 A1	05 July 2018
		US 2018-0232722 A1	16 August 2018
		US 2021-0357925 A1	18 November 2021
		US 2022-0019995 A1	20 January 2022
		US 9922322 B2	20 March 2018
		US 9972005 B2	15 May 2018
		WO 2015-095771 A1	25 June 2015
WO 2013-130912 A2	06 September 2013	AU 2013-202684 B1	18 July 2013
		AU 2013-202684 B9	18 July 2013
		AU 2013-202684 B9	25 July 2013
		AU 2013-205181 B1	18 July 2013
		AU 2013-205181 B9	25 July 2013
		BR 112014021376 A2	20 June 2017
		BR 112014021376 A8	02 January 2018
		US 2013-0226791 A1	29 August 2013
		US 2013-0226796 A1	29 August 2013
		US 2013-0226797 A1	29 August 2013
		US 2015-0073953 A1	12 March 2015
		US 8898088 B2	25 November 2014
		US 8959034 B2	17 February 2015
		US 9020858 B2	28 April 2015
		WO 2013-130912 A3	21 November 2013
US 2019-0108515 A1	11 April 2019	AU 2018-241186 A1	02 May 2019
		AU 2020-205279 A1	06 August 2020
		AU 2020-205279 B2	20 January 2022
		BR 102018070400 A2	24 April 2019
		CA 3019776 A1	05 April 2019
		CA 3019776 C	08 August 2023
		CN 109636593 A	16 April 2019
		CN 109636593 B	18 July 2023
		EP 3471037 A1	17 April 2019
		JP 2019-071052 A	09 May 2019
		JP 6615297 B2	04 December 2019
		MX 2018012075 A	04 July 2019
		RU 2699409 C1	05 September 2019
		SG 10201808702 A	30 May 2019
		US 11080697 B2	03 August 2021

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2023/068519

Patent document cited in search report	Publication date (day/month/year)	Patent family member(s)	Publication date (day/month/year)
		US 11810107 B2	07 November 2023
		US 2021-0357922 A1	18 November 2021