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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
24 January 2019 (24.01.2019)

WIPO | PCT

(10) International Publication Number
WO 2019/018557 A1

(51) International Patent Classification:
H04L 9/32 (2006.01)

(21) International Application Number:
PCT/US2018/042741

(22) International Filing Date:
18 July 2018 (18.07.2018)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

62/534,181	18 July 2017 (18.07.2017)	US
15/844,510	15 December 2017 (15.12.2017)	US
62/617,993	16 January 2018 (16.01.2018)	US
15/885,688	31 January 2018 (31.01.2018)	US
15/942,299	30 March 2018 (30.03.2018)	US
15/942,288	30 March 2018 (30.03.2018)	US

(71) Applicant: **SQUARE, INC.** [US/US]; 1455 Market Street, Suite 600, San Francisco, CA 94103 (US).

(72) Inventors: **SHARIFI, Kamran**; 1455 Market Street, Suite 600, San Francisco, CA 94103 (US). **REZAYEE, Afshin**; 1455 Market Street, Suite 600, San Francisco, CA 94103 (US). **WADE, Jeremy**; 1455 Market Street, Suite 600, San Francisco, CA 94103 (US). **YANG, Yue**; 1455 Market Street, Suite 600, San Francisco, CA 94103 (US). **GUISE, Max, Joseph**; 1455 Market Street, Suite 600, San Francisco, CA 94103 (US). **SMITH, Malcolm, Ronald**; 1455 Market Street, Suite 600, San Francisco, CA 94103 (US). **HARDY, William**; 1455 Market Street, Suite 600, San Francisco, CA 94103 (US).

(74) Agent: **HOLLAND, Jon, E.** et al.; Maynard Cooper & Gale, P.C., 655 Gallatin Street, SW, Huntsville, AL 35801 (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, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA,

(54) Title: DEVICES WITH PHYSICALLY UNCLONABLE FUNCTIONS

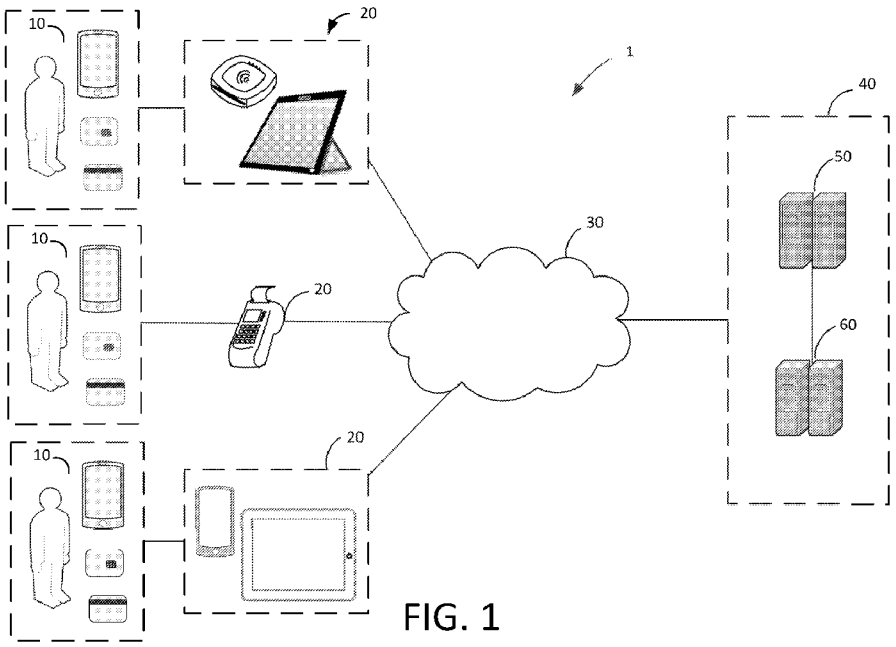


FIG. 1

(57) Abstract: A device may include one or more sources such as circuit elements and electrical components that function as sources for physically unclonable function (PUF) data. PUF data may be acquired from the PUF sources. The resulting PUF values may be used to generate information that may be used for device security operations such as encryption and tamper detection.

[Continued on next page]

WO 2019/018557 A1

SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

Published:

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

TITLE: **DEVICES WITH PHYSICALLY UNCLONABLE FUNCTIONS**

RELATED APPLICATIONS

[0001] This application claims priority to U.S. Patent Application No. 15/942,288, entitled "Devices with Modifiable Physically Unclonable Functions" and filed on March 30, 2018, which is incorporated herein by reference. This application claims priority to U.S. Patent Application No. 15/942,299, entitled "Devices with On-Board Physically Unclonable Functions" and filed on March 30, 2018, which is incorporated herein by reference. This application claims priority to U.S. Patent Application No. 15/885,688, entitled "Device Security with Physically Unclonable Functions" and filed on January 31, 2018, which is incorporated herein by reference. This application claims priority to U.S. Provisional Application No. 62/617,993, entitled "Devices with Modifiable Physically Unclonable Functions" and filed on January 16, 2018, which is incorporated herein by reference. This application also claims priority to U.S. Patent Application No. 15/844,510, entitled "Device Security with Physically Unclonable Functions" and filed on December 15, 2017, which is incorporated herein by reference. This application further claims priority to U.S. Provisional Patent Application No. 62/534,181, entitled "Device Security with Physically Unclonable Functions" and filed on July 18, 2017, which is incorporated herein by reference.

BACKGROUND

[0002] Electronic devices may perform operations involving critical information such as personally identifying information, account information, medical information, business information, or various other types of sensitive information that has economic or other value. Such devices may be ripe targets for hackers or other attackers who seek to access such critical information through eavesdropping or hacking devices. For example, an attacker may attempt monitor signals that are transmitted to or received by devices, as well as signals that are internal to the devices. This may be done by non-invasive or invasive means. In many cases, attackers attempt to physically access components of the device, such as one or more communication lines carrying data or a processor that communicates and processes payment information. Attackers may also attempt to

simulate an external device or internal components of the device under attack. Accordingly, device makers employ a variety of methods to encrypt and protect critical information, safely store cryptographic information, and to identify and prevent tamper attempts.

BRIEF DESCRIPTION OF THE DRAWINGS

[0003] The above and other features of the present disclosure, its nature and various advantages will be more apparent upon consideration of the following detailed description, taken in conjunction with the accompanying drawings in which:

[0004] FIG. 1 shows an illustrative block diagram of a payment system in accordance with some embodiments of the present disclosure;

[0005] FIG. 2 depicts an illustrative block diagram of a payment device and payment terminal in accordance with some embodiments of the present disclosure;

[0006] FIG. 3 depicts an illustrative block diagram of a payment reader in accordance with some embodiments of the present disclosure;

[0007] FIG. 4A depicts an exemplary anti-tamper mesh capacitance-based physically unclonable function in accordance with some embodiments of the present disclosure;

[0008] FIG. 4B depicts an exemplary anti-tamper coating-based physically unclonable function in accordance with some embodiments of the present disclosure;

[0009] FIG. 5A depicts an exemplary memory-based physically unclonable function (PUF) in accordance with some embodiments of the present disclosure;

[0010] FIG. 5B depicts an exemplary ring oscillator-based physically unclonable function in accordance with some embodiments of the present disclosure;

[0011] FIG. 5C depicts an exemplary arbiter-based physically unclonable function in accordance with some embodiments of the present disclosure;

[0012] FIG. 6A depicts an exemplary line capacitance-based physically unclonable function measurement in accordance with some embodiments of the present disclosure;

[0013] FIG. 6B depicts an exemplary chip card interface for measurement in accordance with physically unclonable function derivation in accordance with some embodiments of the present disclosure;

[0014] FIG. 6C depicts an exemplary line time domain reflectometry-based physically unclonable function measurement in accordance with some embodiments of the present disclosure;

[0015] FIG. 7A depicts an exemplary PUF reliability determination in accordance with some embodiments of the present disclosure;

[0016] FIG. 7B depicts an exemplary PUF uniqueness determination in accordance with some embodiments of the present disclosure;

[0017] FIG. 8A depicts an exemplary PUF randomness determination in accordance with some embodiments of the present disclosure;

[0018] FIG. 8B depicts an exemplary PUF bit-aliasing determination in accordance with some embodiments of the present disclosure;

[0019] FIG. 9A depicts an exemplary diagram of a process flow for device authentication based on a PUF in accordance with some embodiments of the present disclosure;

[0020] FIG. 9B depicts an exemplary diagram of a process flow for PUF initialization and key generation in accordance with some embodiments of the present disclosure;

[0021] FIG. 10A depicts an exemplary diagram of a process flow for PUF key initialization in accordance with some embodiments of the present disclosure;

[0022] FIG. 10B depicts an exemplary diagram of a process flow for PUF key reconstruction in accordance with some embodiments of the present disclosure;

[0023] FIG. 11 depicts an exemplary flow diagram of PUF-based device protection in accordance with some embodiments of the present disclosure;

[0024] FIG. 12 depicts an exemplary flow diagram of PUF source selection in accordance with some embodiments of the present disclosure;

[0025] FIG. 13 depicts an illustrative block diagram of a PUF source in accordance with some embodiments of the present disclosure;

[0026] FIG. 14 depicts exemplary dielectric fuses for a PUF source;

[0027] FIG. 15 depicts exemplary amorphous silicon fuses for a PUF source;

[0028] FIG. 16 depicts an exemplary diagram of a process flow for modifying a PUF source in accordance with some embodiments of the present disclosure; and

[0029] FIG. 17 depicts an illustrative block diagram of circuitry for generating a random value based on at least one programmable PUF source and at least one non-programmable PUF source.

[0030] FIG. 18 depicts an exemplary printed circuit board having a reader chip and on-board PUF source.

[0031] FIG. 19 depicts an exemplary diagram of a process flow for combining PUF data from multiple PUF sources, such as at least one on-board PUF source and at least one on-chip PUF source, to provide a cryptographic key.

[0032] FIG. 20 depicts an exemplary reader chip having a time-domain reflectometer for interrogating an on-board PUF source for obtaining PUF data.

[0033] FIG. 21 depicts an exemplary on-board PUF source within a signal path between a reader chip and at least one other component of a printed circuit board.

[0034] FIG. 22 depicts an exemplary on-board PUF source within a path dedicated for the on-board PUF source.

[0035] FIG. 23 depicts exemplary conductive traces that may be formed on a printed circuit board.

[0036] FIG. 24 depicts the exemplary conductive traces of FIG. 23 after holes have been drilled into the traces.

DETAILED DESCRIPTION

[0037] An electronic device such as a payment reader may include cryptographic processing capabilities and tamper protection devices. For example, cryptographic operations may be performed within a unique portion of the electronic device (*e.g.*, physically and/or logically segregated) such that critical information is only provided to external devices or portions of the electronic device in encrypted form. Tamper protection devices may include a variety of physical and electrical components (*e.g.*, tamper lines, tamper meshes, temperature monitors, voltage monitors, clock monitors,

tamper domes, tamper coatings, line-detection tamper devices, RF tamper detection components, etc.) to identify and prevent eavesdropping and tamper detection attempts.

[0038] In an exemplary embodiment of a payment reader including EMV card, swipe card, or NFC payment capability, there are multiple opportunities for an attacker to attempt to obtain critical information such as payment information or to otherwise engage in fraudulent transactions. For example, an attacker may attempt to intercept NFC communications, read data being communicated over the physical connections with the EMV card, or intercept that data from the magnetic stripe of a traditional swiping transaction. Moreover, signals carrying this and other critical information are transmitted within the payment reader and processed by processors and other circuitry of the payment reader.

[0039] Accordingly, numerous types of tamper detection devices such as temperature monitors and voltage monitors are integrated into an exemplary payment reader. These tamper detection devices can sense attempts to gain improper physical access to the payment reader (*e.g.*, by opening the payment reader or drilling into the payment reader to access signals or components), attempts to physically provide electrical signals to the payment reader (*e.g.*, attempts to inject malicious signals into externally accessible pins of the payment reader, such as EMV pins), and attempts to wirelessly introduce malicious signals to the payment reader. Some tamper detection devices may generate a response such as opening a circuit in response to tamper attempt.

[0040] In some embodiments, cryptographic and/or tamper operations may be performed in concert with physically unclonable functions (PUFs) that include characteristics of physical components that may be used to generate unique patterns of bits based on variations in the physical components, and for which those variations are difficult to duplicate. One or more PUFs may be utilized for encryption, for example, as a source of key values, as seed values for encryption, or in other similar manners. Because the PUF value is unique to the physical structure that is the source of the PUF value, it may be possible to acquire the PUF value directly from the physical component, rather than storing such value in memory of the device. In some embodiments, multiple PUF values may be generated from multiple physical structures, and may be combined to make a key or otherwise used to generate key and other cryptographic values. In some

embodiments, at least a portion of the PUF may be based on physical components that respond to tamper attempts, such that any cryptographic keys or other critical information that is generated by or encrypted by the PUF may become unreadable upon the occurrence of a tamper attempt. In some embodiments, error correction methods may be employed to recover PUF data even in the absence of a 100% of the data. Such error correction may be tiered such that only certain operations may be performed (*e.g.*, performing shut down operations, receiving firmware updates, or communicating records of tamper attempts to another device such as a remote server. PUFs may be based on a variety of physical parameters such as startup values of electronic components such as SRAM, delay values of electronic components such as inverters, impedance of traces or physical components such as printed circuit boards, antennas, RF transmission characteristics of antennas and related transmission circuitry, measurements of touch screens or microphones, reflected light or audio signals, vibration sensing, physical responses of electromechanical systems (*e.g.*, microelectromechanical circuits), and other electrical or mechanical systems resident on the devices.

[0041] In an embodiment, a device tamper may include an activity that attempts to alter a pre-defined functionality of a device such as a payment reader, retrieve its protected information, or mimic its identity in a non-authorized way. For example, in a mechanical tamper, the device is opened to expose the critical signals and monitor the information that is transferred using those signals. An electronic chip-level tamper can expose the critical content of the memory to reveal the secret keys preserved in that memory.

[0042] In some instances, a target device for a tamper attempt may include critical information such as a unique ID that facilitates the establishment trust with an authority (*e.g.*, a remote payment service system or payment card issuer) and to allow the device to authenticate itself for certain functions. One way to create a unique ID is based on unique properties of the device (one or more device PUFs) in such a way that these properties remain unique to that device, but they vary device-to-device. An exemplary PUF may be system-based (e.g. it may be derived from the unique property of its printed circuit board electrical traces, discrete components, physical enclosures, etc.) or can be silicon-based (e.g. it can be derived from the unique properties of certain silicon blocks

such as memory or portions thereof). The PUF identifier may act as an electronic fingerprint of the system for performing various operations such as cryptographic operations.

[0043] Exemplary PUFs may sense a tamper attempt and provide a response, for example, by disabling certain functionality or modifying aspects of the PUF itself (*e.g.*, tripping one or more fuses to change the values that may be read for the PUF. This may be performed by the PUF automatically (*e.g.*, the PUF or some portion thereof is itself used for tamper detection) or may be performed based on independent tamper detection and PUF modification. In this manner, the PUF may be able to erase/eliminate any critical information (*e.g.*, its own unique "fingerprint" ID, or the subsequently-derived secret keys) upon a tamper event. In some embodiments, the modification of the PUF or removal of access to the PUF may be modified only temporarily while an analysis of a tamper attempt is performed (*e.g.*, by the device itself and/or a remote server). In other embodiments, the functionality of the PUF (*e.g.*, the unique ID associated with the PUF) can be irreversibly suppressed, if desired, by using an external input that is integrated with the PUF implementation.

[0044] Multiple PUFs may be combined, as may multiple PUF types (*e.g.*, a system-based PUF may be combined with a silicon-based PUF). Such a combination may provide for enhancements to PUF functionality and uniqueness, and may provide for automatic tamper detection even when a portion of the PUF (*e.g.*, a silicon-based PUF) is not easily modified or disabled. In some embodiments, multiple PUF combinations may be available to provide for multiple IDs that may be used for a multiplicity of applications and operational modes.

[0045] Implementing a PUF-based device protection system may alleviate the need to store a secret key in any physical memory, on-chip or off-chip, since the PUF-based unique ID's reside only in hardware on which they are based.

[0046] In some cases, a PUF may be modified (*e.g.*, erased or reprogrammed) to provide a different response to a given input. As an example, the PUF may have one or more fuses that are used to generate a PUF value. In this regard, an input may be applied to the PUF to cause one or more signals to pass through the fuses, and measurements of these signals may be used to calculate or otherwise determine one or more PUF values

provided by the PUF in response to the input. In response to a detected event, such a tamper attempt, the circuitry may be further configured to select one or more of the fuses for modification based on the detected event and to modify each of the selected fuses by transmitting a signal of sufficiently high current or voltage through the fuse to change its resistance, thereby changing a response of the PUF to the input.

[0047] FIG. 1 depicts an illustrative block diagram of a payment system 1 in accordance with some embodiments of the present disclosure. In one embodiment, payment system 1 includes a payment device 10, payment terminal 20, network 30, and payment server 40. Although the PUF-based systems of the present disclosure may be implemented in a variety of devices, in an exemplary embodiment described herein the device may be a payment terminal (*e.g.*, a payment reader of a payment terminal). In an exemplary embodiment, payment server 40 may include a plurality of servers operated by different entities, such as a payment service system 50 and a bank server 60. These components of payment system 1 facilitate electronic payment transactions between a merchant and a customer.

[0048] The electronic interactions between the merchant and the customer take place between the customer's payment device 10 and the merchant's payment terminal 20. The customer has a payment device 10 such as a credit card having magnetic stripe, a credit card having an EMV chip, or a NFC-enabled electronic device such as a smart phone running a payment application. The merchant has a payment terminal 20 such as a payment terminal or other electronic device that is capable of processing payment information (*e.g.,* encrypted payment card data and user authentication data) and transaction information (*e.g.*, purchase amount and point-of- purchase information), such as a smart phone or tablet running a payment application.

[0049] In some embodiments (*e.g.*, for low-value transactions or for payment transactions that are less than a payment limit indicated by a NFC or EMV payment device 10) the initial processing and approval of the payment transaction may be processed at payment terminal 20. In other embodiments, payment terminal 20 may communicate with payment server 40 over network 30. Although payment server 40 may be operated by a single entity, in one embodiment payment server 40 may include any suitable number of servers operated by any suitable entities, such as a payment service

system 50 and one or more banks of the merchant and customer (*e.g.*, a bank server 60). The payment terminal 20 and the payment server 40 communicate payment and transaction information to determine whether the transaction is authorized. For example, payment terminal 20 may provide encrypted payment data, user authentication data, purchase amount information, and point-of-purchase information to payment server 40 over network 30. As described herein, in some embodiments some or all of the encryption and authentication process may be performed based on information obtained from one or more PUFs of the payment terminal 20.

[0050] Payment server 40 may determine whether the transaction is authorized based on this received information as well as information relating to customer or merchant accounts, and responds to payment terminal 20 over network 30 to indicate whether or not the payment transaction is authorized. The authorization may be performed based on predetermined or known information about the one or more PUFs, which may be established based on an initialization process as described herein. Payment server 40 may also transmit additional information such as transaction identifiers to payment terminal 20.

[0051] Based on the information that is received at payment terminal 20 from payment server 40, the merchant may indicate to the customer whether the transaction has been approved. In some embodiments such as a chip card payment device, approval may be indicated at the payment terminal, for example, at a screen of a payment terminal. In other embodiments such as a smart phone or watch operating as a NFC payment device, information about the approved transaction and additional information (*e.g.*, receipts, special offers, coupons, or loyalty program information) may be provided to the NFC payment device for display at a screen of the smart phone or watch or storage in memory.

[0052] In some embodiments, an attacker or other user may attempt to acquire payment information by monitoring transmissions or gaining access to components of payment system 1. As an example, each of these components of payment system 1 may provide an opportunity for an attacker to eavesdrop on payment and transaction information or to inject malicious signals. For example, an attacker may attempt to monitor signals that are relayed between any of payment device 10, payment terminal 20,

network 30, and payment server 40. In some embodiments, transmissions sent or received by components of payment system 1 may be encrypted. In other attacks, an attacker may attempt to substitute a counterfeit component for one of the components of payment system 1, for example, by creating a counterfeit payment device 10 or payment terminal 20, or by attempting to intercept or redirect communications to network 30 or payment server 40. In yet other attacks, an attacker may attempt to modify one of the components of the payment system 1, for example, by modifying one or more of the payment device 10, payment terminal 20, or payment server 40 to eavesdrop or inject malicious signals or extract key values stored in memory.

[0053] The devices of payment system 1 may have a combination of suitable hardware and software to utilize one or more PUFs (*e.g.*, established based on physical components of the payment terminal 20). The PUFs may facilitate authentication of devices and encryption of information in a manner that prevents attacks. Because the keys that are generated by the PUFs are not stored in memory (*i.e.*, the PUF values are "stored" in the physical component itself) an attacker may be unable to obtain useful physical access to ID and/or key information. Multiple PUFs may be utilized together to create keys and IDs, and different keys and IDs may be utilized in a variety of situations. In some embodiments, aspects of the operation of the PUFs and information about tamper attempts may be provided by payment terminal 20 to payment server 40. Payment server 40 may have hardware and software that facilitates the monitoring of the tamper hardware and PUFs and may provide corrective action or provide instructions to modify the manner of operation of the payment terminal 20 and any suitable component thereof. In some embodiments, the payment server 40 may provide firmware that modifies the operation of the payment terminal 20 and PUFs, for example, by utilizing different subsets of PUFs for different operations, modifying error correction thresholds, and changing encryption levels for different operations and communications of the payment terminal 20.

[0054] FIG. 2 depicts an illustrative block diagram of payment device 10 and payment terminal 20 in accordance with some embodiments of the present disclosure. Although it will be understood that payment device 10 and payment terminal 20 of payment system 1 may be implemented in any suitable manner, in one embodiment the

payment terminal 20 may comprise a payment reader 22 and a merchant device 29. However, it will be understood that as used herein, the term payment terminal may refer to any suitable component of the payment terminal, such as payment reader 22. In an embodiment, the payment reader 22 of payment terminal 20 may be a wireless communication device that facilitates transactions between the payment device 10 and a merchant device 29 running a point-of-sale application.

[0055] In one embodiment, payment device 10 may be a device that is capable of communicating with payment terminal 20 (*e.g.*, via payment reader 22), such as a NFC device 12 or an EMV chip card 14. Chip card 14 may include a secure integrated circuit that is capable of communicating with a payment terminal such as payment terminal 20, generating encrypted payment information, and providing the encrypted payment information as well as other payment or transaction information (*e.g.*, transaction limits for payments that are processed locally) in accordance with one or more electronic payment standards such as those promulgated by EMVCo. Chip card 14 may include contact pins for communicating with payment reader 22 (*e.g.*, in accordance with ISO 7816) and in some embodiments, may be inductively coupled to payment reader 22 via a near field 15. A chip card 14 that is inductively coupled to payment reader 22 may communicate with payment reader 22 using load modulation of a wireless carrier signal that is provided by payment reader 22 in accordance with a wireless communication standard such as ISO 14443.

[0056] NFC device 12 may be an electronic device such as a smart phone, tablet, or smart watch that is capable of engaging in secure transactions with payment terminal 20 (*e.g.*, via communications with payment reader 22). NFC device 12 may have hardware (*e.g.*, a secure element including hardware and executable code) and/or software (*e.g.*, executable code operating on a processor in accordance with a host card emulation routine) for performing secure transaction functions. During a payment transaction NFC device 12 may be inductively coupled to payment reader 22 via near field 15 and may communicate with payment terminal 20 by active or passive load modulation of a wireless carrier signal provided by payment reader 22 in accordance with one or more wireless communication standards such as ISO 14443 and ISO 18092.

[0057] Although payment terminal 20 may be implemented in any suitable manner, in one embodiment payment terminal 20 may include a payment reader 22 and a merchant device 29. The merchant device 29 runs a point-of-sale application that provides a user interface for the merchant and facilitates communication with the payment reader 22 and the payment server 40. Payment reader 22 may facilitate communications between payment device 10 and merchant device 29. As described herein, a payment device 10 such as NFC device 12 or chip card 14 may communicate with payment reader 22 via inductive coupling. This is depicted in FIG. 2 as near field 15, which comprises a wireless carrier signal having a suitable frequency (*e.g.*, 13.56 MHz) emitted from payment reader 22.

[0058] In one embodiment, payment device 10 may be a contactless payment device such as NFC device 12 or chip card 14, and payment reader 22 and the contactless payment device 10 may communicate by modulating the wireless carrier signal within near field 15. In order to communicate information to payment device 10, payment reader 22 changes the amplitude and/or phase of the wireless carrier signal based on data to be transmitted from payment reader 22, resulting in a wireless data signal that is transmitted to the payment device. This signal is transmitted by an antenna of payment reader 22 that is tuned to transmit at 13.56 MHz, and if the payment device 10 also has a suitably tuned antenna within the range of the near field 15 (*e.g.*, 0 to 10 cm), the payment device receives the wireless carrier signal or wireless data signal that is transmitted by payment reader 22. In the case of a wireless data signal, processing circuitry of the payment device 10 is able to demodulate the received signal and process the data that is received from payment reader 22.

[0059] When a contactless payment device such as payment device 10 is within the range of the near field 15, it is inductively coupled to the payment reader 22. Thus, the payment device 10 is also capable of modulating the wireless carrier signal via active or passive load modulation. By changing the tuning characteristics of the antenna of payment device 10 (*e.g.* by selectively switching a parallel load into the antenna circuit based on modulated data to be transmitted) the wireless carrier signal is modified at both the payment device 10 and payment reader 22, resulting in a modulated wireless carrier

signal. In this manner, the payment device is capable of sending modulated data to payment reader 22.

[0060] In some embodiments, payment reader 22 also includes an EMV slot 21 that is capable of receiving chip card 14. Chip card 14 may have contacts that engage with corresponding contacts of payment reader 22 when chip card 14 is inserted into EMV slot 21. Payment reader 22 provides power to an EMV chip of chip card 14 through these contacts and payment reader 22 and chip card 14 communicate through a communication path established by the contacts.

[0061] Payment reader 22 may also include hardware for interfacing with a magnetic strip card (not depicted in FIG. 2). In some embodiments, the hardware may include a slot that guides a customer to swipe or dip the magnetized strip of the magnetic strip card such that a magnetic strip reader can receive payment information from the magnetic strip card. The received payment information is then processed by the payment reader 22.

[0062] Merchant device 29 may be any suitable device such as tablet payment device 24, mobile payment device 26, or payment terminal 28. In the case of a computing device such as tablet payment device 24 or mobile payment device 26, a point-of-sale application may provide for the entry of purchase and payment information, interaction with a customer, and communications with a payment server 40. For example, a payment application may provide a menu of services that a merchant is able to select and a series of menus or screens for automating a transaction. A payment application may also facilitate the entry of customer authentication information such as signatures, PIN numbers, or biometric information. Similar functionality may also be provided on a dedicated payment terminal 28.

[0063] Merchant device 29 may be in communication with payment reader 22 via a communication path 23/25/27. Although communication path 23/25/27 may be implemented via a wired (*e.g.*, Ethernet, USB, FireWire, Lightning) or wireless (*e.g.*, Wi-Fi, Bluetooth, NFC, or ZigBee) connection, in one embodiment payment reader 22 may communicate with the merchant device 29 via a Bluetooth low energy interface, such that the payment reader 22 and the merchant device 29 are connected devices. In some embodiments, processing of the payment transaction may occur locally on payment

reader 22 and merchant device 29, for example, when a transaction amount is small or there is no connectivity to the payment server 40. In other embodiments, merchant device 29 or payment reader 22 may communicate with payment server 40 via a public or dedicated communication network 30. Although communication network 30 may be any suitable communication network, in one embodiment communication network 30 may be the internet and payment and transaction information may be communicated between payment terminal 20 and payment server 40 in an encrypted format such by a transport layer security (TLS) or secure sockets layer (SSL) protocol.

[0064] In some embodiments, the application running on the merchant device 29 may receive information about tamper attempts and PUF operations. For example, information about tamper attempts and PUF operations may be provided such that the application of the merchant device requests information about whether a particular tamper attempt is occurring (*e.g.*, such as visual confirmation that the device is not being touched, or instructions for performing operations such as power cycling to modify device status). Information may also be provided by the merchant device 29 to the payment reader 22 to provide information that software of payment reader 22 may utilize to analyze a possible tamper attempt (*e.g.*, geographic information, temperature information, auxiliary sensor information such as sound, video, motion, or infrared data determined from sensors of the merchant device 29, or that content of certain registers in the software that are designed to record the tamper event, etc.).

[0065] FIG. 3 depicts a block diagram of an exemplary payment reader 22 in accordance with some embodiments of the present disclosure. Although particular components are depicted in a particular arrangement in FIG. 3, it will be understood that payment reader 22 may include additional components, one or more of the components depicted in FIG. 3 may not be included in payment reader 22, and the components of payment reader 22 may be rearranged in a suitable manner. In one embodiment, payment reader 22 includes a reader chip 100, a plurality of payment interfaces (*e.g.*, a contactless interface 102 and a contact interface 104), a power supply 106, a wireless communication interface 108, a wired communication interface 110, a signal conditioning device 112 and anti-tamper devices 118. In an embodiment, the reader chip 100 of payment reader 22 may include a general processing unit 120, general memory 122, a cryptographic

processing unit 125 and cryptographic memory 128, an anti-tamper circuit 116, a contact interface 104, and NFC signal conditioning device 112. If desired, all or some of the components of FIG. 3 may reside on a single printed circuit board or other structure. In some embodiments, the components may reside on multiple printed circuit boards or other types of structures.

[0066] In exemplary embodiments, any suitable components or combinations thereof may be utilized to as a source for PUF data, including physical interfaces, circuit traces, wires, discrete components, memories, logical operations, FPGAs, antennas, terminals, enclosures, test points, sensors, cameras, and other similar components. As described herein, the physical components forming the PUF or PUFs may have unique physical characteristics that may be accessed or measured, such as by accessing analog values (*e.g.*, current, voltage, etc.) or digital values associated with the components, measuring physical properties (length, impedance, complex signal characteristics, capacitance, resistance, inductance, RF characteristics, load, initial start-up values, etc.) of components, and performing other suitable analysis or measurements to derive PUF values.

[0067] Although in one embodiment the processing units memories, contact interface 104, signal conditioning device 112, and anti-tamper circuit 116 will be described as packaged in a reader chip 100, and configured in a particular manner, it will be understood that general processing unit 120, general memory 122, a cryptographic processing unit 125 cryptographic memory 128, contact interface 104, signal conditioning device 112, and anti-tamper circuit 116 may be located and configured in other suitable manners to perform the functionality of the payment reader 22 as is described herein. It will also be understood that the functionality of reader chip 100 may be embodied in a single integrated circuit (IC) chip or a plurality of IC chips, each including any suitable combination of processing units, memory, and other components to collectively perform the functionality of reader chip 100 described herein.

[0068] In some embodiments, reader chip 100 may be a suitable chip having a processing unit. Processing unit 120 of reader chip 100 of payment reader 22 may be a suitable processor and may include hardware, software, memory, and circuitry as is necessary to perform and control the functions of payment reader 22. Processing unit

120 may include one or more processors, and may perform the operations of reader chip 100 based on instructions provided from any suitable number of memories and memory types. In some embodiments, processing unit 120 may have multiple independent processing units, for example a multi-core processor or other similar component. In an embodiment, processing unit 120 may execute instructions stored in memory 122 of reader chip 100 to control the operations and processing of payment reader 22. As used herein, a processor or processing unit may include one or more processors having processing capability necessary to perform the processing functions described herein, including but not limited to hardware logic (*e.g.*, hardware designed by software that describes the configuration of hardware, such as hardware description language (HDL) software), computer readable instructions running on a processor, or any suitable combination thereof. A processor may run software to perform the operations described herein, including software accessed in machine readable form on a tangible non-transitory computer readable storage medium. In some embodiments, components of the processing unit (*e.g.*, clock sources, transistors, terminals, etc.) or characteristics of the processing unit (*e.g.*, time to perform different computational operations and workloads) may be utilized to establish PUF values. In an embodiment, the processor may use internal voltage regulator blocks to establish PUF. The processor may use transient I/O values to establish PUF. The processor may also use transient aspect of the electronic system to generate a random number to be used in conjunction with PUF.

[0069] In an exemplary embodiment, the processing unit 120 of reader chip 100 may include two RISC processors configured to operate as a hub for controlling operations of the various components of payment reader 22, based on instructions stored in memory 122. As used herein, memory may refer to any suitable tangible or non-transitory storage medium. Examples of tangible (or non-transitory) storage medium include disks, thumb drives, and memory, etc., but do not include propagated signals. Tangible computer readable storage medium include volatile and non-volatile, removable and non-removable media, such as computer readable instructions, data structures, program modules or other data. Examples of such media include RAM, ROM, EPROM, EEPROM, SRAM, flash memory (embedded or non-embedded), disks or optical storage, magnetic storage, or any other non-transitory medium that stores information that is

accessed by a processor or computing device. In some embodiments one or more memory components may be utilized as a PUF source, *e.g.*, based on fabrication process variation, basic transistor parameters variation, metal layer variation (*e.g.*, change in width of metal strips), etc. Digital or other values for the memory may be read from the memory (*e.g.*, digital values from SRAM) under certain conditions in which the physical state of the memory may correspond to the unique PUF value (*e.g.*, at startup or after certain conditions (applied voltages, currents, control signals, etc.) are applied to the memory.

[0070] Reader chip 100 may also include additional circuitry such as interface circuitry, analog front end circuitry, security circuitry, and monitoring component circuitry. In one embodiment, interface circuitry may include circuitry for interfacing with a wireless communication interface 108 (*e.g.*, Wi-Fi, Bluetooth classic, and Bluetooth low energy), circuitry for interfacing with a wired communication interface 110 (*e.g.*, USB, Ethernet, FireWire, HDMI and Lightning), circuitry for interfacing with other communication interfaces or buses (*e.g.*, I^2C, SPI, UART, and GPIO), and circuitry for interfacing with a power supply 106 (*e.g.*, power management circuitry, power conversion circuitry, rectifiers, and battery charging circuitry). Characteristics of such circuitry including component values and physical measurements of other component characteristics may be utilized to form all or a portion of a PUF value, as may information such as processing or communication speed of components or buses.

[0071] In an exemplary embodiment, reader chip 100 may perform functionality relating to processing of payment transactions, interfacing with payment devices, cryptography, and other payment-specific functionality. In some embodiments, reader chip 100 may include a cryptographic processing unit 125 for handling cryptographic processing operations. Note that each of general processing unit 120 and cryptographic processing unit 125 may have dedicated memory associated therewith (*e.g.*, general memory 122 and cryptographic memory 128). In this manner, specific cryptographic processing and critical security information (*e.g.*, cryptographic keys, passwords, user information, etc.), may be securely stored by cryptographic memory 128 and processed by cryptographic processing unit 125. In some embodiments, cryptographic processing

unit 125 and/or cryptographic memory 128 may function as a PUF in a similar manner as processing unit 120 and/or memory 122, as described herein.

[0072] One or both of general processing unit 120 and cryptographic processing unit 125 of reader chip 100 may communicate with the other (*e.g.*, processing unit 120 may communicate with cryptographic processing unit 125 and *vice versa*), for example, using any suitable internal bus and communication technique. In this manner, reader chip 100 can process transactions and communicate information regarding processed transactions (*e.g.*, with merchant device 29). In some embodiments, characteristics of these communications (*e.g.*, response speed to certain commands or communications) or measurements of characteristics of the buses, traces, and components that facilitate these communications may provide a source for acquiring PUF information. Other characteristics may be protocol based, such as the sequence of ack/nak, parity, CRC, flow control, etc.

[0073] Reader chip 100 may also include circuitry for implementing a contact interface 104 (*e.g.*, power and communication circuitry for directly interfacing with an EMV chip of a chip card 14 that is inserted into slot 21). In some embodiments, reader chip 100 also may also include a signal conditioning FPGA 112 and analog front end circuitry for interfacing with contactless interface 102 (*e.g.*, electromagnetic compatibility (EMC) circuitry, matching circuits, modulation circuitry, and measurement circuitry). Contact interface 104 may be a suitable interface for providing power to a payment chip such as an EMV chip of a chip card 14 and communicating with the EMV chip. Contact interface 104 may include a plurality of contact pins (not depicted in FIG. 3) for physically interfacing with the chip card 14 according to EMV specifications. In some embodiments, contact interface 104 may include a power supply (VCC) pin, a ground (GND) pin, a reset (RST) pin for resetting an EMV card, a clock (CLK) pin for providing a clock signal, a programming voltage (VPP) pin for providing a programming voltage to an EMV card, an input output (I/O) pin for providing for EMV communications, and two auxiliary pins. In this manner, the payment reader and the chip card 14 are able to exchange information such as payment information. Note that, in some embodiments, contact interface 104 may be housed on reader chip 100 and may communicate with the various components of reader chip 100 via any suitable means

(*e.g.*, a common internal bus). Aspects of any of these components may be queried or measured to acquire PUF information as described herein. For example, analog and/or digital values associated with particular operational states of the components of contact interface (*e.g.*, traces, discrete components, card interface, terminals, etc.) may be determined or measured based on initial states or particular applied signals. Other sources for acquiring PUF information may include transient and/or random delay in transmitting bits of information over the contact card interface and variations in voltage levels used to transmit and receive data.

[0074] Contactless interface 102 may provide for NFC communication with a contactless device such as NFC device 12 or chip card 14. Based on a signal provided by reader chip 100, an antenna of contactless interface 102 may output either a carrier signal or a modulated signal. A carrier signal may be a signal having a fixed frequency such as 13.56 MHz. A modulated signal may be a modulated version of the carrier signal according to a modulation procedure such as ISO 14443 and ISO 18092. When the payment reader 22 is inductively coupled to a contactless device, the contactless device may also modulate the carrier signal, which may be sensed by the contactless interface 102 and provided to the reader chip 100 for processing. Based on these modulations of the carrier signal, payment reader 22 and a contactless device are able to communicate information such as payment information. In some embodiments, one or more characteristics of the contactless interface may be measured, or the contactless interface may be used to measure other operational characteristics of the device such as RF emissions. For example, other components of the device may have characteristic RF emissions that may be sensed by the contactless interface when it is not emitting a NFC carrier or data signal. Other components may be cycled through various operational routines (*e.g.*, frequency, power, waveform) that may impact the manner in which a resulting periodic signal is sensed by the contactless interface and provide a source of PUF information. Moreover, the contactless interface 102 transmit and receive paths include one or more antenna portions, matching circuitry, filters, amplifiers, and other similar components that may be directly measured or assessed for obtaining PUF values. Exemplary characteristics that may be utilized to obtain PUF values may include mutual

inductance, electromagnetic coupling factor, electromagnetic permeability of antennas and/or ferrite material, and other similar factors.

[0075] Power supply 106 may include one or more power supplies such as a physical connection to AC power, DC power, or a battery. Power supply 106 may include power conversion circuitry for converting an AC or DC power source into a plurality of DC voltages for use by components of payment reader 22. When power supply 106 includes a battery, the battery may be charged via a physical power connection, via inductive charging, or via any other suitable method. Although not depicted as physically connected to the other components of the payment reader 22 in FIG. 3, power supply 106 may supply a variety of voltages to the components of the payment reader 22 in accordance with the requirements of those components. In certain embodiments, power supply voltages, currents, power outputs, Main battery initial charge value, depletion rate, charge rate, coin cell battery initial charge value, and responses to certain command or query signals may provide unique values that may provide a source of unique PUF information.

[0076] Payment reader 22 may provide an appealing target for an attacker, since, as described above, it provides a central point for receiving payment via multiple interfaces and for communicating that information with other devices (*e.g.*, merchant device 29). Attackers may attempt to tamper with payment reader 22 in order to access internal electrical connections that carry signals to the various payment interfaces or communication interfaces, or processors or other circuitry of payment reader 22. Accordingly, payment reader 22 may include numerous mechanisms for monitoring and preventing attempts to tamper with the hardware of payment reader 22, such as anti-tamper devices 118. For example, in some embodiments, anti-tamper devices 118 of payment reader 22 may include tamper switches that change their electrical state in response to an attempt to open the housing of payment reader 22, insert a device other than a payment card into payment slot 21 or a magnetic stripe reader, place an improper device in proximity to the NFC interface of payment reader 22, or otherwise attempt to gain physical or electrical access to any components of payment reader 22.

[0077] In some embodiments, anti-tamper devices 118 may comprise a tamper switch, which may be a component that changes its electrical state in response to a

physical stimulus. Exemplary tamper switches may be located at various locations of a payment reader 22, such that any attempt to open the enclosure of payment reader 22, or to modify the physical structure of payment reader 22, may cause the tamper switch to change its physical state (*e.g.*, resulting in an open circuit).

[0078] In some embodiments, anti-tamper devices 118 may comprise a tamper switch that changes its electrical state in response to an electrical stimulus. An exemplary payment reader 22 may have a number of connection points at which it is possible to apply an electrical signal to the connection points. For example, in some embodiments a payment slot 21 (FIG. 2) of payment reader 22 may have EMV pins that interface with corresponding pins of an EMV card. An attacker may attempt to access those pins to monitor the pins (*e.g.*, the I/O pin) or to provide malicious signals to payment reader 22 (*e.g.*, by spoofing an EMV card). In some embodiments, a tamper switch may respond to signals that do not match expected signal characteristics (*e.g.*, current, voltage, duty cycle, waveform, capacitance, etc.) and modify its electrical state (*e.g.*, by opening a circuit, closing a circuit, modifying an electrical signal's amplitude or phase, etc.). Although such a tamper switch has been described in the context of the pins of an EMV payment slot 21 (FIG. 2), it will be understood that such a tamper switch may be implemented on any electrical signal lines or connections of payment reader 22.

[0079] In some embodiments, an attacker may attempt an attack that does not require physical access to the payment reader 22, for example, by sending radio frequency (RF) electromagnetic signals in order to create or modify a signal within payment reader 22, or to temporarily or permanently disable or modify the operation of one or more components of the payment reader 22. Exemplary anti-tamper devices 118 may comprise a tamper switch that may respond to sensed characteristics of RF signals that are abnormal or correspond to an attack, such as a signal strength, waveform, frequency, duty cycle, etc. In response to such sensed characteristics the tamper switch may modify its electrical state (*e.g.*, by opening a circuit, closing a circuit, modifying an electrical signal's amplitude or phase, etc.).

[0080] Another exemplary anti-tamper device 118 may comprise a tamper mesh that may provide for a complete enclosure of the internal components of the payment reader 22 or critical components thereof. In some embodiments, a tamper mesh may

include conductive traces in close proximity and creating a pattern that covers the protected components. It may be difficult to gain physical access to the components without damaging the conductive mesh due to the unique and dense pattern of the tamper mash. This results in a change in the electrical state of the tamper mesh (*e.g.*, by opening a circuit, closing a circuit, modifying an electrical signal's amplitude or phase, etc.) that may be used to sense a tamper attempt and take corrective action.

[0081] In some embodiments, an anti-tamper device 118 may comprise an anti-tamper temperature circuit for measuring a temperature within payment reader 22, comparing the measured temperature against one or more threshold temperatures, and performing a response when a tamper attempt is detected. The anti-tamper temperature circuit may comprise temperature sensing components (*e.g.*, polysilicon resistor circuitry) and any combination of hardware, software or otherwise for comparing the temperature within payment reader 22 with a threshold. In some embodiments, anti-tamper temperature circuit may be coupled to other anti-tamper devices 118 (*e.g.*, tamper switch) for controlling operation of the anti-tamper devices 118 (*e.g.*, shutting down the anti-tamper device 118) in response to a measured temperature or a comparison of a measured temperature with one or more pre-defined temperature thresholds.

[0082] Any of the anti-tamper devices 118 or any suitable combination thereof may provide a source for obtaining PUF information. For example, physical characteristics of the anti-tamper devices (*e.g.*, capacitance, response to voltages or currents, impedance, other component measurements, physical configuration or length of tamper traces, physical size of tamper devices, temperature response of components, and other suitable characteristics) may be determined or measured to acquire PUF information. Because the anti-tamper devices 118 change their physical characteristics in response to tamper attempts, utilizing anti-tamper devices to acquire PUF information may result in an automatic response to attacks, since the underlying PUF values may change in a manner that prevents the use of the PUF for encryption and authentication after the tamper event has occurred. In some embodiments, the printed circuit board (PCB) may include special areas of PCB dedicated to PUF sources.

[0083] In some embodiments, monitoring of the anti-tamper devices 118 may be initially performed by an anti-tamper circuit 116 (*e.g.*, that may operate in a low power

mode or based on an alternative low power source). The monitoring may be performed periodically or in some embodiments the timing of monitoring may be randomized (*e.g.*, based on a random number generator) such that the timing of the monitoring is not predictable (*e.g.*, by selectively providing power to the real time clock based on a randomized pattern). By only monitoring the tamper devices for a portion of the time it may be possible to achieve a small average current consumption by the anti-tamper circuit 116 and tamper devices 118.

[0084] In an embodiment, anti-tamper circuit 116 may provide notifications to other components of the payment reader 22 that a tamper attempt has been detected. Notifications may be stored (*e.g.*, in a memory associated with the anti-tamper circuit 116) to be provided to other components of the payment reader 22 (*e.g.*, processing unit 120) when they receive power, or in some embodiments, may be provided (*e.g.*, as an interrupt) in a manner that causes one or more components to wake up. Once a tamper attempt is identified, the tamper attempt may be recorded and/or processed, *e.g.*, by taking corrective action, providing notifications, deleting critical information (*e.g.*, from cryptographic memory 128), disabling communication interfaces, modifying physical characteristics of PUFs or disabling access to PUFs, modifying error correction procedures associated with PUFs, any other suitable response, or any combination thereof. In some embodiments, some or all of this processing may be performed by the anti-tamper circuit 116.

[0085] Wireless communication interface 108 may include suitable wireless communications hardware (*e.g.*, antennas, matching circuitry, etc.) and one or more processors having processing capability necessary to engage in wireless communication (*e.g.*, with a merchant device 29 via a protocol such as Bluetooth low energy) and control associated circuitry, including but not limited to hardware logic, computer readable instructions running on a processor, or any suitable combination thereof. Aspects of any of these components may be queried or measured to acquire PUF information as described herein. For example, analog and/or digital values associated with particular operational states of the components of wireless communication interface 108 (*e.g.*, traces, discrete components, card interface, terminals, etc.) may be determined or measured based on initial states or particular applied signals. PUF values may be

acquired from memory of wireless communication interface 108. In some embodiments, PUF values may be obtained based on electromagnetic (RF) wave propagation patterns measured by a circuitry included in the system.

[0086] Wired communication interface 110 may include any suitable interface for wired communication with other devices or a communication network, such as USB, Lightning, HDMI or mobile HDMI, FireWire, Ethernet, any other suitable wired communication interface, or any combination thereof. In some embodiments, wired communication interface 110 may allow payment reader to communicate with one or both of merchant device 29 and payment server 40. Aspects of wired communication interface 110 may be queried or measured to acquire PUF information as described herein. For example, analog and/or digital values associated with particular operational states of the components of wired communication interface (*e.g.*, traces, discrete components, card interface, terminals, etc.) may be determined or measured based on initial states or particular applied signals.

[0087] In some embodiments, reader chip 100 may include a signal conditioning device 112 coupled to the contactless interface 102 to process signals provided to and received from the contactless interface 102. Although signal conditioning device 112 may include any suitable hardware, software, or any combination thereof, in an exemplary embodiment signal conditioning device may comprise an FPGA. Signal condition device 112 may condition sent and received signals to and from contactless interface 102, such as when a payment device 10 using NFC communication communicates with payment reader 22. In an embodiment, signal conditioning device 112 may operate based on instructions stored at reader chip 100 (*e.g.*, signal conditioning instructions 136) for use in interacting with the contactless interface 102. Characteristics of the signal conditioning interface may be determined or measured, and utilized as a source for PUF values, as described herein (*e.g.*, based on signal propagation patter, NFC blind spots, antenna impedance, etc.).

[0088] In some embodiments, reader 22 may include PUF measurement and control circuitry, which may be separate from reader chip 100, general processing unit 120, and/or cryptographic processing unit 125, or may be at least partially integrated with some or all of these components. In an exemplary embodiment as described herein, PUF

measurement and control circuitry 126 may be integrated within a secure enclave of the reader 22 in a manner that provides multiple levels of physical and logical tamper protection. PUF measurement and control circuitry may provide circuitry and interconnections for performing interfacing with and performing measurements of PUF components, and may provide direct or indirect connections to any such PUF source components. For example, PUF measurement and control circuitry may include digital interfaces for querying memory, C2V converters, voltage and current measurement circuitry, periodic sources, analog sources, digital sources, simulated communications interfaces, battery and power supply measurements, coin cell battery measurements, or other suitable components. The PUF measurement and control circuitry may also control the PUF components, such as changing electrical characteristics of the PUF components in order to erase or reprogram the PUF, as will be described in more detail below.

[0089] In some embodiments, general memory 122 may be any suitable memory as described herein, and may include a plurality of sets of instructions for controlling operations of payment reader 22 and performing general transaction processing operations of payment reader 22, such as operating instructions 130, transaction processing instructions 132, and anti-tamper instructions 138.

[0090] Operating instructions 130 may include instructions for controlling general operations of the payment reader 22, such as internal communications, power management, processing of messages, system monitoring, sleep modes, user interface response and control, operation of the contact interface 104, the wireless interface 108, the wired interface 110, or the signal conditioning device 112, and the management of the other sets of instructions. In one embodiment, the operating instructions 130 may provide the operating system and applications necessary to perform most of the processing operations that are performed by the processing unit 120 of the reader chip 100 of payment reader 22.

[0091] Operating instructions 130 may also include instructions for interacting with a merchant device 29. In one embodiment, the merchant device 29 may be running a point-of-sale application. The operating instructions 130 may include instructions for a complementary application to run on processing unit 120 of reader chip 100, in order to exchange information with the point-of-sale application. For example, the point-of-sale

application may provide a user interface that facilitates a user such as a merchant to engage in purchase transactions with a customer. Menus may provide for the selection of items, calculation of taxes, addition of tips, and other related functionality. When it is time to receive payment, the point-of-sale application may send a message to the payment reader 22 (*e.g.*, via wireless interface 108). The operating instructions 130 facilitate processing of the payment, for example, by acquiring payment information via the contactless interface 102 or contact interface 104, and invoking the various resources of reader chip 100 to process that payment information (*e.g.*, by executing memories stored in cryptographic memory 128 using cryptographic processing unit 125), and by generating responsive messages that are transmitted to the point-of-sale application of the merchant device 29 via wireless communication interface 108 and wired communication interface 110.

[0092] Operating instructions 130 may also include instructions for interacting with a payment service system 50 at a payment server 40. In one embodiment, a payment service system 50 may be associated with the payment reader 22 and the point-of-sale application of the merchant device 29. For example, the payment service system 50 may have information about payment readers 22 and merchant devices 29 that are registered with the payment service system 50 (*e.g.*, based on unique identifiers and/or PUF values). This information may be used to process transactions with servers of the merchant and customer financial institutions, for providing analysis and reports to a merchant, and aggregating transaction data. The payment reader 22 may process payment information (*e.g.*, based on operation of reader chip 100) and communicate the processed payment information to the point-of-sale application, which in turn communicates with the payment service system 50. In this manner, messages from the payment reader 22 may be forwarded to the payment service system 50 of payment server 40, such that the payment reader 22 and payment service system 50 may collectively process the payment transaction.

[0093] Transaction processing instructions 132 may include instructions for controlling general transaction processing operations of the payment reader 22, such as controlling the interaction between the payment reader 22 and a payment device 10 (*e.g.*, for interfacing with a payment device via the contactless interface 102 and contact

interface 104), selecting payment processing procedures (*e.g.*, based on a payment processing entity associated with a payment method), interfacing with the cryptographic processor 125, and any other suitable aspects of transaction processing.

[0094] Transaction processing instructions 132 also may include instructions for processing payment transactions at payment reader 22. In one embodiment, the transaction processing instructions may be compliant with a payment standard such as those promulgated by EMV. Depending on the payment method that is being used (*e.g.*, Europay, Mastercard, Visa, American Express, etc.), a particular processing procedure associated with the payment method may be selected and the transaction may be processed according to that procedure. When executed by processing unit 120, these instructions may determine whether to process a transaction locally, how payment information is accessed from a payment device, how that payment information is processed, which cryptographic functions to perform, the types of communications to exchange with a payment server, and any other suitable information related to the processing of payment transactions. In some embodiments, transaction processing instructions 132 may perform high level processing, and provide instructions for processing unit 120 to communicate with cryptographic processing unit 125 to perform most transaction processing operations. In addition, transaction processing instructions 132 may provide instructions for acquiring any suitable information from a chip card (*e.g.*, via contact interface 104 and cryptographic processing unit 125) such as authorization responses, card user name, card expiration, etc.

[0095] Anti-tamper instructions 138 may include instructions for operating anti-tamper circuit 116 and anti-tamper devices 118, disabling resources of payment reader 22 when a tamper attempt is detected, and in the absence of a tamper attempt, may permit normal operations of the payment reader 22. In some embodiments, anti-tamper instructions 138 may include instructions for monitoring one or more pins of reader chip 100 (not specifically shown) coupled to one or more resources of anti-tamper circuit 116 to identify detection of a tamper attempt by the anti-tamper circuit 116. For example, anti-tamper instructions 138 may include instructions for monitoring a signal provided to a wake-up pin by an anti-tamper circuit 116, as well as signals that are indicative of a tamper attempt or type of tamper attempt. In some embodiments, some or all aspects of

anti-tamper instructions 138 may be stored in cryptographic memory 128 and may be executed by cryptographic processing unit 125.

[0096] Anti-tamper instructions 138 may include instructions for taking action when an output of anti-tamper circuit 116 indicates a tamper attempt. In some embodiments, anti-tamper instructions 138 may include instructions for providing a tamper notification, such as to merchant device 29, payment server 40 via network 30, or to a user of payment terminal 20. The tamper notification may comprise a suitable notification, such as a message transmitted via wireless interface 108 or wired interface 110 of payment reader 22 or an audible, visible, or physical alarm signal. In an embodiment, a tamper notification may be provided via a resource of payment reader 22, and may provide a notification to a user of detection of a tamper attempt (*e.g.*, output of light, sound, mechanical vibration, a combination thereof, or other output).

[0097] In some embodiments, anti-tamper instructions 138 may include instructions for controlling resources of payment reader 22, for example, in order to limit an intruder's access to information of the payment reader 22. For example, in some embodiments, anti-tamper instructions 138 may include instructions for disabling interfaces of payment reader 22 or PUFs of payment reader 22, for example, to prevent further acquisition or transmission of potentially sensitive data. Anti-tamper instructions 138 may include instructions for general processing unit 120 to provide a signal to disable power supply 106. In this regard, general processing unit 120 may selectively disable a supply of power from power supply 106 to various resources of payment reader 22, such as any of the interfaces of payment reader 22 or reader chip 100.

[0098] In some embodiments, anti-tamper instructions 138 may selectively disable resources of payment reader 22 that an attacker may attempt to access in order to acquire potentially sensitive information while permitting other resources (*e.g.*, anti-tamper circuit 116) to continue to operate. For example, anti-tamper instructions 138 may include instructions for removing, erasing, deleting or wiping one or more encryption keys stored in cryptographic memory 128 in order to prevent access to encrypted data when a tamper attempt is detected, causing the provision of signals that may permanently modify a PUF, or removing access to PUF sources. Similarly, anti-tamper instructions 138 may include instructions for removing, erasing, deleting or

wiping any suitable information from general memory 122 or cryptographic memory 128, such as user information (*e.g.*, personally identifiable information, financial account information, or otherwise) in response to detection of a tamper attempt. In this regard, anti-tamper instructions 138 may include instructions for continuing to monitor an output of anti-tamper circuit 116 following detection of a tamper attempt and taking steps to further disable operation of payment reader 22 (*e.g.*, completely power down payment reader 22) if one additional tamper attempt is detected within a pre-determined amount of time. Anti-tamper instructions 138 may include other instructions for performing other operations in other embodiments.

[0099] In some embodiments, anti-tamper instructions 138 may include instructions for collecting tamper attempts that may be identified locally at payment reader 22 or that may be transmitted to an external system (*e.g.*, payment server 40) for storage, analysis, and complex processing of a tamper event (*e.g.*, based on other known tamper events that are occurring in similar circumstances). In some embodiments, such an external analysis may result in a signal being received at general processing unit 120, which may shut off power to one or more components of reader chip 100 or payment reader 22 in response to that input.

[00100] Cryptographic processing unit 125 may be any suitable processor as described herein, and, in some embodiments, may perform cryptographic functions for the processing of payment transactions. For example, in some embodiments a cryptographic processing unit 125 may encrypt and decrypt data based on one or more encryption keys provided by PUFs, in a manner that isolates the encryption functionality from other components of payment reader 22 and protects the PUF values from being exposed to other components of payment reader 22 or being stored permanently in memory.

[00101] In some embodiments, cryptographic memory 128 may be any suitable memory or combination thereof as described herein, and may include a plurality of sets of instructions for performing cryptographic operations, such as payment processing instructions 176, cryptographic instructions 178, and PUF processing instructions. Payment processing instructions 176 may include instructions for performing aspects of payment processing, such as providing for encryption techniques to

be used in association with particular payment procedures, accessing account and processing information, any other suitable payment processing functionality, or any suitable combination thereof. Cryptographic instructions 178 may include instructions for performing cryptographic operations. Cryptographic processing unit 125 may execute the cryptographic instructions 178 to perform a variety of cryptographic functions, such as to encrypt, decrypt, sign, or verify a signature upon payment and transaction information as part of a payment transaction.

[00102] PUF processing instructions 172 may interact with PUF sources and PUF measurement and control circuitry 126 to obtain PUF data and perform processing based on the PUF data. In some embodiments, PUF measurement and control circuitry 126 may obtain PUF data from one or more PUF sources and process the PUF data such that a PUF value (*e.g.*, a series of binary values representative of PUF data) is provided to the cryptographic processing 125. In other embodiments, some or all of the PUF data may be provided as raw data by the PUF measurement and control circuitry as a one or more analog and/or digital values depending on the particular PUF data sources and any additional processing performed by PUF measurement and control circuitry 126.

[00103] In some embodiments, the PUF processing instructions 172 may process the received PUF data or PUF values for use by the cryptographic processing unit 125. In an embodiment where PUF data is provided by multiple PUF data sources, the PUF processing instructions may provide for appropriate processing of the PUF values, for example, to combine the PUF values or perform multi-step processing to generate a final PUF value. In some embodiments, PUF processing instructions may provide for applying error correction codes to received PUF data to extract usable PUF values even if not all received PUF values are correct. Exemplary error correction codes include Binary parity check code, Hamming code e.g. Hamming (7,4), Hamming (63, 57), Hamming (127, 120), and Cyclic Redundancy Check (CRC) codes, *e.g.*, CRC-32. PUF processing instructions 172 may further provide for facilitation of encryption, authentication, initialization, and other steps as provided herein. The PUF values and any encryption keys generated therefrom may only be accessed and stored when necessary, such that they are not stored in non-volatile memory and thus more difficult to access by attackers.

[00104] FIG. 4A depicts an exemplary anti-tamper mesh capacitance-based physically unclonable function in accordance with some embodiments of the present disclosure. In certain embodiments, an anti-tamper mesh may include a pattern of electrical traces that form an overall mesh structure that makes it difficult to access underlying components. Signal traces may be in a variety of patterns and in some embodiments may include one or more series traces that form an open circuit when the series electrical path in broken. The traces may overly each other as depicted in a top view from FIG. 4A, in which vertical lines one represent one series-connected path and horizontal lines represent another series-connected circuit path. In other embodiments additional connections may be provided such that a determination of a tamper attempt is based on other measured parameters such as impedance or frequency response.

[00105] Each of the traces of the anti-tamper mesh may be at a potential and may have a particular location with respect to adjacent traces. By connecting adjacent portions of the traces to measurement circuitry (*e.g.*, C2V converter measurement circuitry) a capacitance that is representative of the capacitance between multiple adjacent points of the tamper mesh may be determined. In this manner, an anti-tamper mesh may have numerous capacitance values that may be measured and that may be dependent upon manufacturing processes in a unique and non-repeatable manner. The values may be provided as analog or digital PUF data, and in some embodiments, may be compared to a threshold to establish 0 or 1 binary values associated with a comparison between the measured capacitance and a capacitance threshold.

[00106] FIG. 4B depicts an exemplary anti-tamper coating-based physically unclonable function in accordance with some embodiments of the present disclosure. In an embodiment, some or all of one or more interior or exterior surfaces of the device (*e.g.*, payment reader 22) may be coated with one or more layers having known conductive properties (*e.g.*, a single partially conductive layer or a plurality of interleaved conductive and non-conductive layers). A number of measurement points (*e.g.*, measurement points 401 and 402) may be provide on one or more of the layers to measure characteristics of the PUF coating, for example, by measuring voltage, impedance, of applying signals to the PUF coating. In an embodiment, dozens or hundreds of measurement points may selectively apply predetermined signals and

predetermined signal patterns to the conductive layer, the measurement of which may provide analog or digital PUF data and/or binary 0 and 1 values based on comparison with thresholds. In addition to providing a PUF value, the application of signals to the PUF coating may also provide for tamper detection based on changes in sensed signal values. In some embodiments, the tamper detection may execute automatically as the resulting PUF value may not be successfully determined in response to a tamper attempt.

[00107] FIG. 5A depicts an exemplary memory-based physically unclonable function (PUF) in accordance with some embodiments of the present disclosure. A memory-based PUF may be constructed of a variety of memory technologies in a manner such that the physical memory structure (*e.g.*, as implemented in silicon) returns to a default state in response to a standard condition, such as the application or removal of an operational voltage for the memory. For example, upon an initial startup condition in which voltage is applied to the memory, the bits representing the state of the memory may return to default state that is based on the structure of the underlying silicon and memory technology. In some embodiments, once the default PUF values are extracted from the memory-based PUF, the memory may be utilized in a normal manner (*e.g.*, as RAM) to operate the device.

[0100] FIG. 5B depicts an exemplary ring oscillator-based physically unclonable function in accordance with some embodiments of the present disclosure. A ring oscillator may operate at different frequencies based on manufacturing variances that occur during the fabrication of the ring oscillators. Although these frequency differences may not be functionally significant, they may occur with the required randomness, uniqueness, and per-PUF repeatability under default conditions to provide information that may be used to generate PUF values. In an exemplary embodiment, the ring-oscillator PUF values (*e.g.*, binary 0 or 1 representing unique ID or key values) may be based on frequency comparisons for different ring oscillators.

[0101] In an exemplary embodiment, N ring oscillators may result in N! different orderings of the oscillators based on the relative frequency of each of the N oscillators. As a result of independent comparisons of these N oscillators, it may therefore be possible to generate $\log_2(N!)$ independent bits (*e.g.*, 25 oscillators may produce 133 bits, 128 oscillators may produce 716 bits, and 256 oscillators may produce 1687 bits). One

exemplary embodiment for querying the oscillators for these bits is depicted in FIG. 5B. Each of the oscillators 1 . . . N is coupled to two multiplexers. The multiplexers selectively provide different combinations of the oscillator outputs to respective counters for a suitable time (*e.g.*, with sufficient resolution to provide different counter outputs for each of a range of frequencies for the ring oscillators, factoring in error correction for oscillators having frequencies of high similarity). For each combination of oscillators, the counter values may be provided to a comparator that outputs a 1 or a 0, based on which of the oscillators has the higher frequency as indicated by the counters. It will be understood that other processing possibilities may be provided such as a multiple sets of parallel-connected counters and comparators for faster processing or greater frequency resolution. Moreover, in some embodiments initial PUF values may be determined based on a lower sampling time, and if error correction is unable to extract an acceptable PUF value, additional sampling may be performed.

[0102] FIG. 5C depicts an exemplary arbiter-based physically unclonable function in accordance with some embodiments of the present disclosure. Electronic components such as inverters, transistors, logic gates, diodes, multiplexers, and other similar components may have different delays that may not be critical for underlying signal processing operations but that may be utilized to create PUF data have required randomness, uniqueness, and per-PUF repeatability. In an exemplary embodiment, multiple delay paths may be provided through otherwise functionally identical components having different fabrication-based delays and PUF detection circuitry may compare the delays to determine PUF values. A number of delay elements and PUF detection circuitry may be selected in a manner that provides sufficient resolution based on the known delay variances that are imparted by the manufacturing process and the operation of the PUF detection circuitry. In an embodiment the inputs to the PUF detection circuitry may be set to an initial state based on one or more source signals provided to the delay elements, the source signal may be changed (*e.g.*, a rising-edge signal), and the PUF value determined may be determined based on the relative time of arrival of the rising edge signal through multiple delay paths.

[0103] An exemplary embodiment of an arbiter-based PUF is depicted in FIG. 5C. In FIG. 5C, K sets of 2 parallel multiplexers are arranged in series. A c-bit challenge

is provided to each set of multiplexers, which facilitates numerous delay paths through the multiplexers. Each multiplexer receives one of two source signals (*e.g.*, identical rising edge source signals in the example of FIG. 5C, but other source signals may be provided with different delay elements and PUF detection circuitry), and selects which of the two signals to provide as an output based on the MUX input. The MUXes have complementary inputs such that each of the two source signals is propagated through the MUX chain. These outputs are then provided to each subsequent set of MUXes and eventually to PUF detection circuitry such as a D flip flop, which outputs a 1 or a zero based on which path through the MUXes (*e.g.*, for a particular c-bit challenge). Different combinations of c-bit challenges may be provided to extract different PUF values for different MUX delay paths.

[0104] FIG. 6A depicts an exemplary line capacitance-based physically unclonable function measurement in accordance with some embodiments of the present disclosure. In an embodiment, the components and circuitry depicted in FIG. 6A may correspond to a capacitance monitoring system to detect capacitance of components such as a tamper mesh, chip card interface circuitry, or other components and circuitry of a device such as payment reader 22. In one embodiment, the capacitance monitoring system includes at least an oscillator (OSC), a reference capacitor (C_{REF}) and a capacitance measuring circuit to measure a capacitance (C_{MEAS}) associated with one or more components of the device.

[0105] In an exemplary device of a payment reader 22, the components of the capacitance monitoring system can be incorporated in the reader chip 100 and/or elsewhere in the payment reader 22. The capacitance monitoring system can be arranged as a capacitance divider that uses the capacitance measuring circuit to measure or determine changes in the component capacitance (C_{MEAS}). Different capacitance measurement points (*e.g.*, from a tamper mesh, touchscreen, chip card interface, or other source) may be provided as C_{MEAS}. The capacitance measuring circuit can include a data acquisition circuit and one or more sensors. The oscillator (OSC) can provide an output signal at a single fixed frequency or at a variable frequency that can be varied or selected from a range of frequencies. In one embodiment, the output signal provided by the oscillator (OSC) can be supplied by a clock of the reader chip 100. In other

embodiments, the oscillator (OSC) can provide a pulse that can be phase and/or amplitude shifted as desired. If the oscillator is providing a pulse as the output signal, then the capacitance measuring circuit may incorporate an A/D converter to digitize the corresponding measured signal, which can then be processed to determine a capacitance value. The reference capacitor (C_{REF}) can have a fixed capacitance in one embodiment. However, in other embodiments, the reference capacitor (C_{REF}) can have a variable capacitance that can be selected by a user. In one embodiment, the variable capacitance can be provided by selectively engaging and disengaging capacitors in a bank of capacitors to obtain the desired capacitance for the reference capacitor (C_{REF}).

[0106] The capacitance measuring circuit can measure the capacitance between one or more components. For example, the capacitance measuring circuit can selectively measure capacitances of a tamper mesh such as that depicted in FIG. 4, a touchscreen, or an interface such as a chip card interface as is depicted in FIG. 6B. For example, in FIG. 6B, the capacitance measuring circuit can measure the capacitance (C_{MEAS}) between any two pins of a chip card interface, such as the voltage interface 502, the reset interface 504, the clock interface 506, the I/O interface 508, the ground interface 510, the programming interface 512, or a parallel plate 514. The capacitance measuring circuit the measured component capacitance (C_{MEAS}) to the processing unit 120 for further processing and storage in memory 122. In one embodiment, the capacitance measuring circuit 402 can be operated in synchronicity with the clock and the oscillator (OSC) in order to perform phase-matched measurements.

[0107] In some embodiments, capacitance values may be used to establish PUF values based on absolute values (*e.g.*, converting to a multi-bit digital value for capacitance) or comparisons between capacitances. Moreover, changes in capacitance may also provide tamper detection, as an attacker will often attempt to thwart a tamper mesh or gain access through components such as a card or user interface. In some embodiments, the processing unit 120 may establish a baseline for the component capacitance (C_{MEAS}) for each capacitance of the contact interface 104 to be monitored and then compare subsequent determinations of the component capacitance (C_{MEAS}) to the baseline that is stored in memory 122. In other embodiments, the use of the capacitance

values for a PUF may provide automatic tamper detection, as tampering may prevent authentication and key generation.

[0108] FIG. 6C depicts an exemplary line time domain reflectometry-based physically unclonable function measurement in accordance with some embodiments of the present disclosure. Time domain reflectometry may be used to measure characteristics of any suitable signal path within the device and may provide information based on the amplitude, phase, and other characteristics of reflections. These characteristics may be used to generate PUF values based on individual characteristics of signal paths (*e.g.*, multi-bit digital values or binary phase and/or amplitude comparisons) or based on comparisons of reflections between multiple signal paths. In some embodiments, such values may also be used for independent tamper detection based on changes in reflected characteristics (*e.g.*, representing the introduction of unexpected elements into the signal path) or may provide automatic tamper detection based on the failure of PUF values generated therefrom to provide authentication and/or proper key generation.

[0109] In an embodiment, the components and circuitry depicted in FIG. 6C may correspond to a TDR monitoring system to determine characteristics of various signal paths that may be coupled to the TDR monitoring system (*e.g.*, via a variety of multiplexed paths, etc.). In one embodiment, the TDR monitoring system 450 includes at least a TDR circuit 652, a transmitter, 654, a detector 656, and a coupler 658. The TDR circuit 652 may be coupled to a transmitter 654 to transmit a pulse or signal on a respective signal path 662 via a coupler such as a multiplexer. In some embodiments, multiple transmitters 654 can be coupled to transmit pulses on multiple signal paths simultaneously and comparison circuitry (not depicted) may be utilized to compare responses of similar signal paths to extract PUF values. In embodiments, the pulse or signal sent by the transmitter can be either an electrical signal or an optical signal.

[0110] The TDR circuit 652 can monitor the transmission of pulses and the corresponding reflections returned from the signal path 662. In addition to determining PUF values based on characteristic reflections, the TDR circuit may also identify tamper attempts and/or automatically change PUF values based on tamper attempts. For example, a pulse was transmitted to signal path 662 at time T_0 may provide a first

expected or normal reflection response at time T_1. However, a second reflection may be received based on a tamper device 664 coupled to the signal path at location 660. As a result, the overall amplitude and/or phase of the response may be changed, resulting in determination of a tamper attempt or a change in the PUF value generated from the response.

[0111] FIG. 7A depicts an exemplary PUF reliability determination in accordance with some embodiments of the present disclosure. Although the PUF reliability determination is based on an exemplary memory-based PUF, it will be understood that a similar determination may be made with a variety of suitable PUFs. As described herein, any PUF may not provide an identical response at all times and under all conditions. For example, differences in supply voltage, temperature, external noise sources, or wear over time may result in different marginal results for some PUF components (*e.g.*, memory-based PUF values that drift over a threshold for a binary output, changes in delay time, changes in oscillator frequency, changes in capacitance, or changes in reflection characteristics). Accordingly, error correction procedures such as error correction codes may be used to extract usable PUF values from imperfect PUF results. It may be desirable to maintain a PUF error rate below a maximum which may dictate the selection of error correction procedures. In some embodiments there may be multiple allowable error rates for different operations or circumstances and an associated multiple error correction operations.

[0112] An error rate may be based on a comparison to a stored PUF response to a measured PUF response prior to error correction. The stored PUF response may be stored at a suitable location (*e.g.*, created and stored during manufacturing, testing, or an initialization procedure) such as a remote server in order to prevent attacker access and local long-term storage of PUF values. In an embodiment, PUF values may be read from the PUF and transmitted in encrypted form for comparison to the stored PUF values (*e.g.*, based on encryption provided by the error-corrected PUF itself or by other PUF sources). In the exemplary embodiment depicted in FIG. 7A, the error rate of 6.25% corresponds to two error bits. Based on the error rate it may be determined whether the PUF source may continue to be used to generate PUF values. In some embodiments, PUF values may be monitored over time to identify PUF error patterns. If only certain subsets of bits

repeatedly supply errors and a sufficient number of correct bits remain, the error bits may be ignored. Error correction procedures may be modified or updated based on probabilities or patterns in error bits, and additional PUF sources may be introduced or combined with the initial PUF source to provide additional PUF values.

[0113] FIG. 7B depicts an exemplary PUF uniqueness determination in accordance with some embodiments of the present disclosure. As described herein, it may be desirable that the PUFs exhibit a threshold level of uniqueness between different particular PUFs of a single PUF source type. Although such a uniqueness analysis may be performed for any suitable PUF, in the exemplary embodiment, of FIG. 7B two memory-type PUFs may be compared to determine whether the PUF is sufficiently unique to function as a PUF (*e.g.*, a predictable PUF may be easier to attack). As described herein, a PUF may have components that are fabricated with non-deterministic differences that can be analyzed to create a suitable PUF source. In an exemplary embodiment, PUF sources may be analyzed at one or more times (*e.g.*, prior to installation in the device, after installation in the device, in the field based on information transmitted from multiple devices to servers, etc.) to determine whether the required uniqueness between PUFs exists. In some embodiments, multiple PUF sources of the same type (*e.g.*, memory devices, delay elements, oscillators, tamper meshes, capacitive features, signal path features, etc.) to confirm whether different devices have a high enough degree of uniqueness – *e.g.*, such that each device has at least a threshold % of differences with any other device (*e.g.*, 45%, 48%, 49%, etc.) and that no portions of the device (*e.g.*, a particular subset of memory regularly have a single value over numerous multiple devices. Depending on uniqueness values determined, the PUF may be used for only limited purposes (*e.g.*., lower security operations or values) or other PUF sources may be utilized. In some embodiments, uniqueness and other measured values may be weighed against other aspects of PUF operation such as a security score (*e.g.*, based on difficulty of accessing the PUF and/or tamper protections for the PUF (PUF-enabled or peripheral), lack of variances under operating conditions, etc.). In some embodiments where PUF data is compared to thresholds or other data, or is based on input stimulus such as signals, aspects of the thresholds or inputs may be modified to adjust the uniqueness.

[0114] FIG. 8A depicts an exemplary PUF randomness determination in accordance with some embodiments of the present disclosure. In addition to providing values that are reproducible and unique, it may be desirable to ensure that a particular PUF source exhibits a sufficient degree of randomness in how the unique PUF values are distributed. Thus, even if a PUF source provides values that appear to be unique vis-à-vis other PUF sources of the same type, the PUF source may not provide randomness in the distribution of those PUF values (*e.g.*, as a result of portions or sections having changing PUF values in a similar way). Accordingly, an ideal PUF source should ultimately supply PUF values that have an equal ability to provide a 1 or 0 response. As depicted in FIG. 8A, 1 – n devices are represented as defining a bit space. Changing any one bit in a challenge (*e.g.*, for certain PUF types that utilize challenge bits) should alter approximately half of the response bits. FIG. 8B depicts an exemplary PUF bit-aliasing determination in accordance with some embodiments of the present disclosure. Similar to the randomness determination, any bit or set of bits should have approximately 50% probability of having a PUF value of 0 or 1. As is depicted in FIG. 8B. any particular bit location within a bit space for a set of devices 1 – n can be identified for PUF sources of the same type, and should have a value that exceeds a bit aliasing threshold (*e.g.*, 45%, 48%, 49%, etc.) Checks for randomness and bit aliasing may be performed at various times, including during manufacturing or based on tests performed at devices and information provided from multiple devices to servers. Depending on randomness values determined, the PUF may be used for only limited purposes (*e.g.*, lower security operations or values) or other PUF sources may be utilized. In some embodiments, randomness and other measured values may be weighed against other aspects of PUF operation such as a security score (*e.g.*, based on difficulty of accessing the PUF and/or tamper protections for the PUF (PUF-enabled or peripheral), lack of variances under operating conditions, etc.). In some embodiments where PUF data is compared to thresholds or other data, or is based on input stimulus such as signals, aspects of the thresholds or inputs may be modified to adjust the randomness.

[0115] FIG. 9A depicts an exemplary diagram of a process flow for device authentication based on a PUF in accordance with some embodiments of the present disclosure. During an initialization or other setup of a particular Device A, a series of

challenges and responses may be provided to the PUF and recorded, for example, within a memory device or at a remote device. Because the internal structure of a PUF source of Device A causes particular responses, these challenge and response values may be provided to an internal PUF or remote device to determine whether the PUF is authentic, *i.e.*, it can return the proper responses to particular challenges. Because the challenges and responses are unknown except to the device that originally stored the challenges and responses, the authenticity of Device A can be confirmed by issuing sets of challenges and determining whether the corresponding responses match (*e.g.*, whether a current response matches a previous response).

[0116] FIG. 9B depicts an exemplary diagram of a process flow for PUF initialization and key generation in accordance with some embodiments of the present disclosure. To the left side of FIG. 9B is depicted an initialization procedure for a particular PUF source. The PUF values are output to an error correction code encoding circuit which creates error correction codes for the particular PUF output. Once the ECC is initialized with an error correction code, the PUF source may be operated in the field to generate a key. As depicted on the right side of FIG. 9B, a PUF source is queried and outputs PUF values. Those PUF values are provided to a ECC decoding circuit that applies ECC decoding to the PUF values. The ECC-encoded PUF values may function as a key or other identifier, or in an embodiment as depicted in FIG. 9B, hashed and provided as an input to a key generation algorithm. If the PUF is operational within the limitations of the ECC decoding (*i.e.*, the PUF values output during re-generation, after ECC decoding, match the PUF values from initialization), the key may be utilized for encrypted communications between the device having the PUF source and other devices with the correct PUF-based key.

[0117] FIG. 10A depicts an exemplary diagram of a process flow for PUF source initialization with a fuzzy extractor in accordance with some embodiments of the present disclosure. As is depicted in FIG. 10A, a PUF source 1000 may output a reference response to a fuzzy extractor 1010. The fuzzy extractor 1010 may collectively perform key generation and ECC encoding. The key generation may be performed based on a privacy amplification process, which may compress and/or hash the PUF values to create

a full-entropy cryptographic key. The fuzzy extractor may also create a public syndrome mask that may be stored at the device as public helper data 1030 for ECC decoding.

[0118] FIG. 10B depicts an exemplary diagram of a process flow for PUF key reconstruction in accordance with some embodiments of the present disclosure. A similar fuzzy extractor 1020 may work in conjunction with the PUF source 1000, ECC decoding, and helper data 1030 to create a corrected reference response based on the PUF response and ECC decoding. The privacy amplification process may then be executed on the corrected PUF data to generate the key. If the PUF is operational within the limitations of the ECC decoding (*i.e.*, the PUF values output during re-generation, after ECC decoding, match the PUF values from initialization), the key may be utilized for encrypted communications between the device having the PUF source and other devices with the correct PUF-based key.

[0119] In view of the structures and devices described *supra*, methods that can be implemented in accordance with the disclosed subject matter will be better appreciated with reference to the flowcharts of FIGS. 11-12. While, for purposes of simplicity of explanation, the methods are shown and described as a series of steps, it is to be understood and appreciated that such illustrations or corresponding descriptions are not limited by the order of the steps, as some steps may occur in different orders and/or concurrently with other steps from what is depicted and described herein. Any non-sequential, or branched, flow illustrated via a flowchart should be understood to indicate that various other branches, flow paths, and orders of the steps, can be implemented which achieve the same or a similar result. Moreover, not all illustrated steps may be required to implement the methods described hereinafter.

[0120] FIG. 11 depicts exemplary steps for utilizing PUFs for device security in a device in accordance with some embodiments of the present disclosure. At step 802, one or more PUF data sources may be accessed as described herein. As described herein, multiple PUF data sources may be accessible in a single device. In some embodiments, the selection of the PUF sources may be based on a particular use case for the PUF, such as for ID, authentication, tamper detection, encryption, key generation, seed values, or other similar operations. Once the PUFS are accessed, processing may continue to step 804.

[0121] At step 804, error correction may be performed on the accessed PUF data as described herein. In some embodiments, the error correction may be tiered for different PUF sources, applications, or use cases. In some cases, multiple error correction results may be provided for particular PUFs and different security levels or operations performed based on the success of different types or levels of error correction. For example, a low-resilience error correction (*e.g.*, requiring higher-accuracy PUF data) may be utilized for critical security operations while a higher-resilience error correction (*e.g.*, requiring lower-accuracy PUF data) may be utilized for less critical operations. For example, a single PUF source may provide PUF data to both ECCs, and only particular operations may be performed based on which ECC successfully processes the data.

[0122] As a further example, a first ECC may be capable of correcting up to a first threshold number of errors in the PUF data, and a second ECC may be capable of correcting up to a second threshold number of errors in the PUF data. If the first ECC is able to successfully correct each error in the PUF data, then a first set (one or more) secure operations may be permitted. If the second ECC is able to successfully correct each error in the PUF data, then a second set (one or more) secure operations may be permitted. In some embodiments, a tamper event may result in a change to the PUF data acquired from the PUF source such that a given ECC is unable to successfully correct each error in the PUF data. The inability of the ECC to successfully correct at least some of the errors in the PUF data may be used to identify an occurrence of the tamper event. In other examples, other techniques for performing error correction and using the results of the error correction processes may be used.

[0123] At step 806, information such as a key may be generated from the PUF values that are output at steps 802 and 804. In some embodiments, multiple PUF values from multiple sources may be used to generate a single key or multiple keys, based on multiple levels of key generation steps. PUF values may be also be used for various other purposes such as providing digital signatures, identifying tamper attempts, and various other data and processing operations as described herein.

[0124] At step 808, it may be determined whether the generation of information (*e.g.*, a key) has been successful. This may be based on information such as raw PUF

values, error correction results, communications with other processes or devices, or other similar operations. If all of the information was generated successfully, processing may continue to step 810 and processing operations may be performed based on the PUF-generated information. If all information was not generated successfully, processing may continue to step 812.

[0125] At step 812 it may be determined whether there is a possible remedy for the PUF-generated information that was not successfully generated, such as applying alternative ECC operations, accessing an alternative PUF source, lowering a security or other operational tier, performing additional attempts with the same PUF source and ECC, or other similar operations as described herein. If a possible remedy is available, processing may return to step 802 based on any revised parameters, if any. If a possible remedy is not available, processing may continue to step 814.

[0126] At step 814, one or more corrective actions may be applied to the device. In some embodiments, a choice of corrective action may be based on which of multiple tiered PUF sources and/or tiered ECC operations successfully generated PUF-generated information, if any. Different corrective actions of different severities may be applied based on such tiered successful operations, as well on as other available data such as number of failed attempts, operational or environmental data associated with the device, the circumstances (*e.g.*, transaction processing operations, location, time of day, etc.) of the device, and information and commands provide by other devices such as a server or merchant device. Corrective action can include various operations as described herein, including but not limited to disabling access to PUF sources, destroying PUF source, disabling access to communication interfaces, providing error messages, providing error displays, providing counter-measures to interfere with tamper devices, disabling access to cryptographic processes, destroying memory devices or erasing critical information described therein, requesting a firmware update, providing detailed log data to a remote server, and other similar operations. Once corrective action has been taken at step 814, the processing of FIG. 11 may end.

[0127] FIG. 12 depicts steps for testing, establishing, and initializing a PUF source and ECC in accordance with some embodiments of the present disclosure. Although steps of FIG. 12 may be described as being applied to a single PUF source, it

will be understood that the steps of FIG. 12 may be applied to multiple PUF sources and/or types at the same time, *e.g.*, to test the operation of the PUF sources and types together and in multi-step PUF processing operations.

[0128] At step 902 data may be obtained from a PUF source as described herein. Data may be obtained directly from the PUF source by applying relevant initial conditions to the PUF source as well as applying relevant signals (*e.g.*, challenge data) to the PUF source. In some embodiments, a similarly configured PUF source type (*e.g.*, a similarly manufactured SRAM, arbiter, oscillator, capacitive circuit, TDR circuit, etc.) may be in multiple similar devices, and data may be acquired from a variety of PUF sources from different devices. In addition, data may be obtained from any PUF source repeatedly and under different environmental and operating conditions. In some embodiments, ECC test codes or a variety of ECC types may be applied to the PUF data. In this manner, a variety of data may be acquired from the PUF source or PUF sources to facilitate different PUF testing operations in steps 904, 906, and 908. For example, in step 904 reliability testing may be performed as described herein, *e.g.*, based on multiple data acquisition steps of PUF data from the same PUF source and under a variety of operating, environmental, and ECC conditions. At step 906, multiple PUFs may be examined as described herein, based on multiple sets of PUF data from multiple PUF sources, and under a variety of operating, environmental, and ECC conditions. At step 908, PUF uniformity and bit-alias may be tested as described herein, based on multiple sets of PUF data from multiple PUF sources, and under a variety of operating, environmental, and ECC conditions. In addition, other relevant tests may be applied to PUF source or sources such as to determine life cycle effects and other responses.

[0129] At step 910 it may be determined whether a particular PUF source or PUF sources are a suitable PUF source. In some embodiments, the various test results may be weighted to arrive at an overall PUF score representing the quality of the PUF source as a PUF. In some embodiments, certain tests may have minimum threshold values under which a PUF source must be rejected, such as a minimum reliability. In some embodiments PUF sources or ECC applied to PUF sources may be selected from tiered operation based on the outcome of step 910. If at step 910 it is determined that the PUF source is a suitable source for some purpose, processing may continue to step 912. If not

processing may end. At step 912, the PUF source may be initialized as described herein, for example by generating information such as associated ECC values for the PUF based on operations such as performed by a fuzzy extractor. Once the PUF source and other information are initialized, the processing of FIG. 12 may end.

[0130] As indicated above, there may be times when it is desirable to destroy, erase, reprogram or otherwise modify a PUF source. For example, a PUF source may be destroyed, erased, reprogrammed or otherwise modified in response to a detection of a tamper attempt. In another embodiment, it may desirable to reprogram a PUF source from time-to-time, such as at various stages of product development. As an example, a chip manufacturer may obtain a PUF value from a PUF source, and this value may be later used to authenticate the chip, such as by a product manufacturer when the chip is being incorporated in to a product being manufactured. The product manufacturer may then reprogram the PUF source to provide a different PUF value that can be later used to authenticate the product. In another example, a PUF source may be reprogrammed after expiration of a certain amount of time or number of accesses in an effort to enhance security of the PUF data generated by the PUF source. There are many other reasons why it may be desirable to erase, destroy, reprogram or otherwise modify a PUF source such that it provides a different response to a given input (*e.g.*, challenge). As used herein, a PUF source capable of selective modification by circuitry to change the PUF source's response to a given input shall be referred to as a "programmable PUF source."

[0131] In some embodiments, a PUF source of a device can be destroyed, erased, reprogrammed or otherwise modified through the use of one or more fuses embedded within the device, and these fuses can be controlled to permanently change their electrical properties, thereby altering the PUF source's response to a given input. As an example, an input (*e.g.*, challenge data, an analog or digital input signal, or other type of input), referred to hereafter as "challenge input," may be applied to the PUF source such that a signal passes through at least one of its fuses, and a parameter (*e.g.*, voltage or current) of such signal may be measured and used to generate a PUF value. When destruction, erasing, reprogramming or other modification of the PUF source is desired, another input may be applied to the PUF source such that a signal (*e.g.*, pulse) of sufficiently high current or voltage flows through the fuse to permanently alter the electrical characteristics

of the fuse. As an example, the fuse's resistance may be increased or decreased in response to a signal of high voltage or current. Thereafter, when the challenge input is again applied to the PUF source, a different voltage or current of a signal passing through the fuse may be measured, thereby changing the PUF source's response to the challenge input.

[0132] FIG. 13 depicts an exemplary embodiment of a PUF source 1100 that comprises a plurality of fuses 1111-1113 having electrical characteristics that can be modified in order or provide for destruction, erasing, reprogramming or other modification of the PUF source 1100, as will be described in more detail hereafter. For simplicity of illustration, FIG. 13 shows three fuses 1111-1113, but any number of fuses may be used in other embodiments. As shown by FIG. 13, the fuses 1111-1113 may be respectively coupled to a plurality a sensors 1121-1123, and each sensor 1121-1123 may be configured to measure a voltage or current of a signal passing through the corresponding fuse to which the respective sensor is coupled. As shown by FIG. 13, the fuses 1111-1113 and sensors 1121-1123 are coupled to PUF measurement and control circuitry 1125. If desired, the components of FIG. 13 may be incorporated into and used within a payment reader, such as the payment reader 22 depicted by FIG. 3. As an example, the PUF measurement and control circuitry 1125 may be incorporated within the reader chip 100 of FIG. 3, and the fuses 1111-1113 and sensors 1121-1123 may be off-chip (*i.e.*, external to the reader chip 100). As an example, the fuses 1111-1113 and sensors 1121-1123 may be formed on or embedded in a PCB, such as the PCB on which the reader chip 100 resides, or the fuses 1111-11113 may be implemented in IC chips external to the reader chip 100. In other embodiments, other configurations of the PUF source 1100 and uses of the PUF source 1100 in other types of devices are possible. As an example, the fuses 1111-1113 and sensors 1121-1123 may be incorporated in the same IC chip (*e.g.*, reader chip 100) as the PUF measurement and control circuitry 1125. Yet other configurations are also possible.

[0133] Each fuse 1111-1113 has electrical characteristics, such as resistance, that vary randomly from device-to-device due to variations in manufacturing processes used to fabricate the fuses 1111-1113. As an example, each of the fuses 1111-1113, as will be described in more detail below, may comprise one or more layers, the thickness of which

may control an electrical property (*e.g.*, resistance) of the fuse. These thicknesses and, thus, the electrical characteristics of the fuses 1111-1113 may randomly vary within certain tolerances during manufacturing such that the fuses 1111-1113 may be used to generate a PUF value.

[0134] When a PUF value is to be generated by the PUF source 1100, the PUF measurement and control circuitry 1125 may be configured to apply a challenge input to the PUF source 1100 for causing a signal to flow through each fuse 1111-1113, and each of the sensors 1121-1123 may be configured to measure a parameter (*e.g.*, current or voltage) of the signal passing through the respective fuse 1111-1113 coupled to it. For illustrative purposes, assume that each of the sensors 1111-1113 measures a current of the signal passing through the respective fuse 1111-1113 to which it is coupled. The PUF measurement and control circuitry 1125 is configured to determine at least one PUF value based on at least one of the sensor measurements.

[0135] As an example, the PUF measurement and control circuitry 1125 may simply use a raw measurement value (*e.g.*, a measurement of current) from any sensor 1121-1123 as a PUF value. In other embodiments, the PUF measurement and control circuitry 1125 may process the raw measurement value to generate a PUF value. For example, the PUF measurement and control circuitry 1125 may use a raw measurement value from a sensor 1121-1123 to calculate a resistance of the corresponding fuse 1111-1113, and the PUF measurement and control circuitry 1125 may then use the calculated resistance value as a PUF value. In yet other embodiments, the PUF measurement and control circuitry 1125 may use the raw measurement value according to any desired algorithm to calculate a PUF value. If desired, the PUF measurement and control circuitry 1125 may combine the measurements from multiple sensors 1121-1123 in order to generate a PUF value.

[0136] In some embodiments, the PUF measurement and control circuitry 1125 may determine a binary value for each fuse 1111-1113 and combine binary values for multiple fuses 1111-1113 to form a digital word to be used as a PUF value. As an example, for each fuse 1111-1113, the PUF measurement and control circuitry 1125 may compare the raw measurement value from the fuse's respective sensor 1121-1123 to a threshold and determine that the fuse 1111-1113 is associated with a logical high value

(*e.g.*, 1) if the threshold is exceed or a logical low value (*e.g.*, 0) if the threshold is not exceeded. The PUF measurement and control circuitry 1125 may then use the determined value as a respective bit in a multi-bit word that is based on some or all of the fuses 1111-1113. As an example, *x* number of fuses may be used to generate a digital word of *x* bits where each bit is based on the electrical characteristics of a single one of the fuses. In other embodiments, yet other techniques for calculating or otherwise determining a PUF value based on the electrical characteristics of the fuses 1111-1113 are possible.

[0137] As will be described in more detail, regardless of how the PUF value from a fuse 1111-1113 is determined, it is possible for that PUF value to change when the fuse 1111-1113 is "burned" by passing a signal (*e.g.*, a pulse) of high current or voltage through the fuse. Note that when multiple fuses 1111-1113 are used to define a PUF value, it is unnecessary for each fuse 1111-1113 to provide a different PUF value after burning relative to its PUF value prior to burning. In some embodiments, which of the fuses 1111-1113 that change their responses to a given input challenge when burned is random, thereby enhancing the randomness of the PUF value derived from all of the fuses 1111-1113.

[0138] As an example, in the embodiment described above where each fuse 1111-1113 is used to define essentially a one-bit PUF value of a multi-bit word, it is unnecessary for the fuses 1111-1113 to be designed such that the PUF response from each fuse 1111-1113 is changed when the fuses 1111-1113 are burned. In this regard, as described above, the response from each fuse 1111-1113 may be compared to a threshold to determine whether the PUF value from the respective fuse 1111-1113 is a logical high value or a logical low value. This threshold may be set and the fuses 1111-1113 designed such that the one-bit PUF value from each fuse 1111-1113 has about a 50% chance of changing when the fuses 1111-1113 are burned by passing a certain signal (*e.g.*, a pulse having a predefined current or voltage) through each fuse 1111-1113. As an example, a thickness of a dielectric layer of the fuse, as described in more detail below, may be selected for a fuse 1111-11113 such that the PUF value from such fuse has about a 50% chance of changing when the fuse is burned depending on manufacturing process variations in the thickness of the dielectric layer from fuse-to-fuse. Designing the fuses

1111-1113 such that each fuse 1111-1113 has about a 50% chance of changing its response to a challenge input helps to enhance the randomness of the multi-bit word provided by the fuses 1111-1113.

[0139] FIG. 14 depicts an exemplary embodiment of the fuses 1111-1113. As shown by FIG. 14, each fuse 1111-1113 has a conductive layer 1210, referred to herein as a "gate," and a dielectric layer 1211 formed on a substrate 1212. In one embodiment, the substrate 1212 is a silicon substrate or other semiconductive substrate having a doped region 1251 below the dielectric layer 1211 so that the layer 1211 is sandwiched between a pair of conductors allowing current to flow through the dielectric layer 1211 when a voltage is applied across the gate 1210 and doped region 1251. Though not shown for simplicity of illustration, the PUF measurement and control circuitry 1125 may be formed on the substrate 1212 and electrically coupled to the doped region 1251 and the gate 1210 of each fuse 1111-1113. In one embodiment, the dielectric layer 1211 is a thin oxide having a thickness of about 10 nanometers (nm) between the gate 1210 and substrate 1212, and the gate 1210 may be a layer of polysilicon. However, other materials and arrangements of the fuses 1111-1113 are possible in other embodiments.

[0140] The material of the dielectric layer 1211 may have a relatively high resistance such that the layer 1211 generally acts as insulator between the gate 1210 and substrate 1211. However, by keeping the layer 1211 thin, a small leakage current is allowed to flow between the gate 1210 and the substrate 1211. This signal formed by the leakage current passing through a fuse 1111-1113 may be measured by a corresponding sensor 1121-1123 and used to generate a PUF value, as described above. In this regard, as described above, the PUF measurement and control circuitry 1125 may be configured to apply a challenge input to each fuse 1111-1113 and measure the resulting leakage current in one or more fuses to provide one or more measurements that may be used to determine a PUF value.

[0141] When the PUF source 1100 is to be modified so that it will generate a different PUF value in response to a given challenge input, the PUF measurement and control circuitry 1125 may be configured to select one or more of the fuses 1111-1113 for modification. For each selected fuse 1111-1113, the PUF measurement and control circuitry 1125 may be configured to apply a signal (*e.g.*, pulse) of relatively high voltage

that exceeds the breakdown voltage of the dielectric layer 1211. Application of such a signal to a fuse 1111-1113 permanently changes the electrical characteristics of the fuse. Specifically, it reduces the resistance of the dielectric layer 1211 such that this layer 1211 becomes electrically conductive (*i.e.*, a short circuit). The process of applying a sufficiently high voltage or current to a fuse in order to change its electrical state from substantially insulating to conductive (*i.e.*, to decrease resistance) may be referred to as a "burn" of the fuse. Fuses, like the ones shown by FIG. 14, that transition to a short circuit rather than an open circuit when burned are sometimes referred to as "antifuses."

[0142] FIG. 15 depicts another exemplary embodiment of the fuses 1111-1113. In the embodiment shown by FIG. 15, each fuse 1111-1113 has a thin layer 1310 of amorphous silicon sandwiched between two conductive layers 1311 and 1312 formed on a substrate 1315, such as a silicon substrate. Though not shown for simplicity of illustration, the PUF measurement and control circuitry 1125 may be formed on the substrate 1315 and electrically coupled to the conductive layers 1311 and 1312 of each fuse 1111-1113. Like the dielectric layer 1211 described above, the layer 1310 of amorphous silicon may have a relatively high resistance allowing a small amount of leakage current to flow through the fuse. When modification of the PUF source 1100 is desired, one or more of the fuses 1111-1113 of FIG. 15 may be burned in essentially the same manner as described above for the embodiment shown by FIG. 14. Specifically, when a fuse 1111-1113 is to burned, the PUF measurement and control circuitry 1125 may apply a signal (*e.g.*, pulse) of sufficiently high voltage to turn the amorphous silicon of layer 1310 into polycrystalline silicon-metal alloy with low resistance, thereby permanently transitioning the layer 1310 to a conductor (*i.e.*, a short circuit). Thus, using essentially the same techniques described above for the embodiment of FIG. 14, the fuses 1111-1113 may be selectively burned in order to modify the PUF source so that it provides a different PUF value in response to a given challenge input. In yet other embodiments, other materials and arrangements of the fuses 1111-1113 are possible.

[0143] An exemplary use of the PUF source 1100 depicted by FIG. 13 for generating and protecting a cryptographic key will now be described below.

[0144] In performing secure operations, such as encryption or decryption of data for a payment transaction or other type of transaction, the cryptographic unit 125 of FIG.

3 may utilize a cryptographic key. When needing such a key, the cryptographic processing unit 125 may transmit to the PUF measurement and control circuitry 1125 a command instructing the circuitry 1125 to return a PUF value from the PUF source 1100. In response, the PUF measurement and control circuitry 1125 may apply a challenge input for causing current to flow through the fuses 1111-1113 and determine a PUF value based on the measurements by the sensors 1121-1123, as described above. The PUF measurement and control circuitry 1125 may then transmit the PUF value to the cryptographic processing unit 125, which may execute the PUF processing instructions 172 in order to process the PUF value as may be desired in order to provide the cryptographic key. As an example, the cryptographic processing unit 125 may use the PUF value as a seed to generate a cryptographic key according to known key generation algorithms. If desired, the cryptographic processing unit 125 may perform this same process each time it requires use of the cryptographic key so that it is unnecessary to store the cryptographic key in memory.

[0145] At some point, assume that the anti-tamper circuit 116 of FIG. 3 detects a tamper attempt based on the anti-tamper devices 118 in step 1410 of FIG. 16. In response, the general processing unit 120 may execute the anti-tamper instructions 138, which cause the general processing unit 120 to trigger a modification of the PUF source 1100. In this regard, the general processing unit 120 may transmit to the PUF measurement and control circuitry 1125 a command instructing the circuitry 1125 to modify the PUF source 1100. The PUF measurement and control circuitry 1125 may respond to the command by selecting one or more of the fuses 1111-1113 to burn in step 1415 of FIG. 16. There are various techniques that could be used to select fuses 1111-1113 to burn. For example, in one embodiment, the PUF measurement and control circuitry 1125 may select all of the fuses 1111-1113 of the PUF source 1100. In another embodiment, the PUF measurement and control circuitry 1125 may select some of the fuses 1111-1113 according to any desired algorithm for selecting fuses. In addition, the selection of fuses for burning may be based the type of event that triggers the modification. As an example, for a detection of a tamper event, as described for the instant example, the fuses to be selected for burning may be predefined. However, if the PUF source 1100 is to be reprogrammed for another purpose or in response to a different

triggering event, the PUF measurement and control circuitry 1125 may randomly select fuses 1111-1113. Yet other techniques and algorithms for selecting the fuses to be burned are possible in other embodiments.

[0146] In step 1420 of FIG. 16, the PUF measurement and control circuitry 1125 burns the selected fuses by applying a pulse of sufficiently high voltage to alter the electrical characteristics of the selected fuses. When the fuses are configured as shown by the embodiment of FIG. 14 or FIG. 15, the pulse reduces the resistance of each fuse through which the pulse passes. Thus, burning one or more of the fuses 1111-1113 may have the effect of destroying the capability of recovering the cryptographic key from the PUF source 1100. In this regard, when the cryptographic unit 125 requests a PUF value from the PUF source 1100 after the select fuses have been burned, the PUF measurement and control circuitry 1125 will return a different PUF value since the electrical characteristics of at least some of the fuses 1111-1113 have changed, thereby changing the measurement values used to derive the PUF value. Thus, the cryptographic processing unit 125 may be prevented from generating the same cryptographic key used prior to the tamper attempt once the PUF source 1100 has been altered in response to a detection of the tamper attempt.

[0147] In other embodiments, similar techniques may be used to modify the PUF source 1100 for other purposes or in response to other types of events. As an example, as further described above, the PUF value from the PUF source 1100 may be used as a unique value, referred to herein as an "authentication token" or may be used to calculate or otherwise determine an authentication token for use in authenticating the device in which the PUF source 1100 is being used. In this regard, the authentication token may be sent to a remote device, which compares the authentication token to an authentication token previously generated by the PUF source 1100 in order to authenticate the device. In some cases, it may be desirable to reprogram PUF source 1100 from time-to-time or in response to a trigger event so that a new authentication token is generated. For example, in response to a tamper attempt or a user input indicating that the authentication token is to be changed, the PUF source 1100 may be altered so that the device can no longer be authenticated based on a previous authentication token. In another example, the PUF source 1100 may be altered to provide a new authentication token for authenticating the

device on a going-forward basis. In yet other embodiments, the PUF source 1100 may be modified for other reasons.

[0148] Note that, as described above, it is possible to use multiple PUF values from multiple PUF sources to generate a random value that may be used for various purposes, such as device authentication or generation of a cryptographic key, as described above. Although the same types of PUF sources may be used to generate multiple PUF values or multiple portions of the same PUF value, it is unnecessary for the same types of PUF sources to be used in all embodiments.

[0149] As an example, FIG. 17 shows an exemplary embodiment in which processing circuitry 1510 (*e.g.*, general processing unit 120, cryptographic processing unit 125, and/or PUF measurement and control circuitry 126 of FIG. 3) is coupled to at least one programmable PUF source 1515, such as the PUF source 1100 having fuses 1111-1113 depicted by FIG. 13, and at least one non-programmable PUF source 1520. The non-programmable PUF source 1520 may be any PUF source described herein for which the PUF value provided by such PUF source is not programmable. As an example, a non-programmable PUF source may be a memory-based PUF, a ring oscillator-based PUF, an arbiter-based PUF, a line capacitance-based PUF, or a line time domain reflectometry-based PUF, as described above with reference to FIGs. 5A through 6A and 6C.

[0150] In the embodiment depicted by FIG. 17, the processing circuitry 1510 may obtain at least one PUF value from the programmable PUF source 1515 and at least one PUF value from the non-programmable PUF source 1520 and generate a random value based on the PUF values from both PUF sources 1515 and 1520. As an example, when the processing circuitry 1510 is generating a cryptographic key or other unique value, the processing circuitry 1510 may combine at least one PUF value from the programmable PUF source 1515 and at least one PUF value from the non-programmable PUF source 1520 to provide a combined value. For example, the processing circuitry 1510 may form a combined value where a portion (*e.g.*, half) of the combined value is from the programmable PUF source 1515 and another portion (*e.g.*, half) of the combined value is from the non-programmable PUF source 1520. The processing circuitry 1510 may then use this combined value as a random value as may be desired. For example, when

generating a cryptographic key, the processing circuitry 1510 may use the combined value as a seed to generate a cryptographic key or other unique value.

[0151] As indicated above, it is possible for PUF sources to be on-chip or off-chip, such as on a PCB. FIG. 18 shows an exemplary embodiment of a PCB 1801 having at least one PUF source 1805 (referred to hereafter as "on-board PUF source"), which may be formed or otherwise positioned on a surface of the PCB 1801 or embedded within the PCB 1801. As shown by FIG. 18, a reader chip 1807 (such as the reader chip 100 depicted by FIG. 3) may be mounted on the PCB 1801 and electrically connected to the on-board PUF source 1805. The reader chip 1807 may have at least one PUF source 1811, referred to hereafter as "on-chip PUF source," and processing circuitry 1815 electrically coupled to the on-board PUF source 1805 and the on-chip PUF source 1811.

[0152] The processing circuitry 1815 may include one or more of the general processing unit 120, cryptographic processing unit 125, and/or the PUF measurement and control circuitry 126 of FIG. 3, as well as any other circuitry for performing the functions described herein for the processing circuitry 1815. Using any of the techniques described herein, the processing circuitry 1815 may be configured to interact with and obtain PUF data from the PUF sources 1805 and 1811. In embodiments for which either or both of the PUF sources 1805 and 1811 are programmable, the processing circuitry 1805 and 1811 may be configured to reprogram, erase, or otherwise modify either of the PUF sources 1805 and 1811 using any of the PUF modification techniques described herein. As an example, one or more of the PUF sources 1805 and 1811 may have a fuse that can be modified (*e.g.*, "burned") by transmitting an electrical signal through the fuse, as described above for the embodiment depicted by FIG. 13.

[0153] In some embodiments, the processing circuitry 1815 may be configured to obtain PUF data from the on-board PUF source 1805 and the on-chip PUF source 1811 and to combine such PUF data for the purpose of performing a secure operation. As an example, the processing circuitry 1815 may obtain PUF data from the on-board PUF source 1805 by submitting a challenge to the PUF source 1805 and measuring or otherwise determining a response, as shown by block 1903 of FIG. 19. Similarly, the processing circuitry 1815 may obtain PUF data from the on-chip PUF source 1811 by submitting a challenge to the PUF source 1811 and measuring or otherwise determining a

response, as shown by block 1906 of FIG. 19. The processing circuitry 1815 may then combine the PUF data obtained from the on-board PUF source 1805 with the PUF data obtained from the on-chip PUF source 1811 to form a combined PUF value, as shown by block 1915 of FIG. 19. As shown by block 1922 of FIG. 19, the processing circuitry 1815 may use this combined PUF value to generate or otherwise provide a cryptographic key or other value (*e.g.*, authentication token) that can be used to encrypt or decrypt data (*e.g.*, payment information used in a payment transaction, as described above), to authenticate the reader chip 1807 and/or the PCB 1801, or to perform another secure operation.

[0154] In combining the PUF data in block 1915, the processing circuitry 100 may simply append one or more bits of PUF data from one PUF source to one or more bits of PUF data from the other PUF source to form a combined value. Alternatively, more complex algorithms may be used. As an example, bits from one PUF source may be interleaved with bits from the other PUF source, or the PUF data from each PUF source may be used as an input to a mathematical algorithm to calculate a value that is based on PUF data from both PUF sources. The value resulting the combination may be used as a cryptographic key or as a seed for generating a cryptographic key. Yet other techniques for combining and using the PUF data from either or both of the on-board PUF source and the on-chip PUF source may be employed in other embodiments.

[0155] Use of PUF data from the on-board PUF source 1805 or from a combination of the on-board PUF source 1805 and the on-chip PUF source 1811 may provide cryptographic joinder of the reader chip 1807 and the PCB 1801 on which the chip 1807 is positioned. As an example, the processing circuitry 1815 may be configured to provide a valid key for a secure operation only when it is mounted on the PCB 1801 and has access to the on-board PUF source 1805. Thus, if the reader chip 1807 is removed from the PCB 1801, it may be prevented from performing at least some secure operations that rely on or use a valid identifier (e.g., cryptographic key or authentication token) derived from the on-board PUF source 1805. In addition, if the on-chip PUF source 1811 is also used to derive a valid identifier, then a valid identifier may be generated only when the reader chip 1807 is paired with the PCB 1801 on which the on-board PUF source 1805 resides. That is, without access to the on-chip PUF source 1811,

a different reader chip (not shown) connected to the PCB 1801 would be unable to use the on-board PUF source 1805 to provide a valid identifier.

[0156] As an example, during manufacturing or some other time, the processing circuitry 1815 may be configured to obtain PUF data from the on-board PUF source 1805 and PUF data from the on-chip PUF source 1811 and then use the PUF data from both PUF sources to define a cryptographic key or other unique value to be used for encryption, authentication, or some other secure operation. If a hacker removes the reader chip from the PCB 1801, tampers with the PCB in a manner that changes the on-board PUF source 1805, or tampers with the reader chip 1807 in a manner that changes the on-chip PUF source 1811, then the processing circuitry 1815 may be prevented from generating the aforementioned key or value based on the PUF sources 1805 and 1811. Thus, when such a tamper attempt occurs, the processing circuitry 1815 may be prevented from performing at least one secure operation that relies on or uses the key or value, thereby helping to protect sensitive data within or processed by the reader chip 1807.

[0157] To illustrate the foregoing in more detail, assume that a hacker removes the reader chip 1807 from its PCB 1801 and mounts the reader chip 1807 on another PCB (not shown) having components designed to obtain sensitive information from the reader chip 1807. Upon initialization, the processing circuitry 1815 may be configured to obtain PUF data from the on-board PUF source 1805 and use such data to provide a key (*e.g.*, authentication token) used for authentication, encryption, or other secure operation. If the reader chip 1807 has been moved to a different PCB by a hacker, then the electrical (*e.g.*, impedance) characteristics of the new board is likely to be different than that of the PCB 1801 and, specifically, the on-board PUF source 1805. Thus, when the processing circuitry 1815 initializes and attempts to interrogate the on-board PUF source 1805, the PUF data obtained by the processing circuitry 1815 is likely to be different relative to when the reader chip 1815 was previously mounted on the PCB 1801 so that the processing circuitry 1815 is unlikely to provide a valid key for authentication, encryption, or other secure operation. In such case, one or more secure operations by the reader chip 1807 may be prevented helping to protect unauthorized access of sensitive information.

[0158] Note that there are various types of components that may be used to implement the on-board PUF source 1805. As an example, in some embodiments, the on-board PUF source 1805 may include one or more passive components, such a resistor, capacitor, or inductor, and/or conductive connections formed on or embedded in the PCB 1801. In such an embodiment, the processing circuitry 1815 may include a circuit for measuring, sensing, or analyzing impedance characteristics of a path that includes the PUF source 1805 in order to derive one or more values of PUF data from such impedance characteristics.

[0159] As an example, FIG. 20 shows an exemplary embodiment in which the processing circuitry 1815 includes a time-domain reflectometer (TDR) 2001 and a processing unit 2011, such as the cryptographic processing unit 125 depicted by FIG. 3. The TDR 2001 may be configured to transit an electrical signal (*e.g.*, a pulse) along a path 2018 that includes the on-board PUF source 1805. As the signal propagates along the path, portions of the signal reflect back toward and are measured by the TDR 2001. In general, impedance discontinuities along the path 2018 change the amplitude of the reflections that reflect from such points such that the reflections over time define a signature of the path 2018. Thus the presence of passive components, such as resistors, inductors, and capacitors, in the path, as well as the length and design (*e.g.*, width and thickness) of the conductive connections, affect the signature measured by the TDR 2001. Further, variances in the manufacturing process of these components cause the signature to vary randomly from board-to-board make it possible to use these components as a source for PUF data.

[0160] There are various techniques that can be used to derive PUF data from the measurements of the TDR 2001. As an example, it is possible for the TDR 2001 to take measurements of the returns at predefined times after transmission of a pulse or other signal along the path 2018 and to then algorithmically combine the measurements to derive a value to be used as PUF data. In other embodiments, other techniques for determining PUF data from TDR measurements are possible.

[0161] In some embodiments, the configurations or shapes of the traces formed on the PCB 1801 may be varied or otherwise controlled in order to affect the signature measured by the TDR 2001. As an example, the configurations or shapes of the traces of

the on-board PUF source 1805 (or other PUF source) may be intentionally varied for different PCBs in order to provide unique TDR signatures that can be used to authenticate or otherwise identify the PCB 1801. Further, variations in the configurations or shapes of the traces from board-to-board resulting from manufacturing process variations may enhance the randomness of the PUF data.

[0162] To better illustrate the foregoing, refer to FIG. 23 which shows a pair of exemplary conductive traces 2052 and 2053 that may be formed on the PCB 1801. Trace 2052 has a widened area 2062, referred to herein as a "flag," that provides an increased surface area for facilitating the drilling of one or more holes, as will be described in more detail hereafter. Trace 2053 similarly has a flag 2063. For simplicity of illustration, FIG. 23 shows two traces 2052 and 2053 with each trace having a single flag. In other embodiments, there may be any number of traces with any of the traces having any number of flags as may be desired.

[0163] Each flag 2062 and 2063 may be drilled to form holes, as illustrated by FIG. 24. In this regard, FIG. 24 shows the traces 2052 and 2053 of FIG. 23 with two holes 2071 and 2072 drilled in the flag 2062 and three holes 2073-2075 drilled in the flag 2063. For each flag 2062 and 2063, any number of holes may be drilled into it according to any desired pattern. By removing a portion of the conductive material forming a trace, the drilling that forms each hole alters the trace's impedance discontinuity at its respective flag. That is, a flag (or other portion of a trace) having a hole drilled therein will have a different reflection characteristic relative to the same trace prior to drilling. Further, such reflection characteristic will depend on the pattern of the holes drilled into the flag. Thus, the reflection measurement made by the TDR 2001 at the time that a reflection from the flag 2062 arrives at the TDR 2001 will be different due to the presence of the holes 2071 and 2072, and similarly the reflection measurement made by the TDR 2001 at the time that a reflection from the flag 2063 arrives at the TDR 2001 will be different due to the presence of the holes 2073-2075. As a result, the signature measured by the TDR 2001 and, hence, the PUF data derived from the PUF source 1805 having the traces 2062 and 2063 will be different due to the presence of the holes 2071-2075 in the traces analyzed by the TDR 2001.

[0164] As noted above, the pattern of the holes formed in the flags 2062 and 2063 may be intentionally varied from board-to-board so that each PCB 1801 has a different trace pattern. Further, the selection of the hole pattern may be randomized from board-to-board in an effort to enhance the randomness of the PUF data generated from the PUF source defined by the traces 2052 and 2053. Regardless of whether the pattern of the holes is intentionally varied, variations in the drilling process may result in small-scale random variations in the hole patterns that help to randomize the PUF data from board-to-board. Thus, in some embodiments, the same drilling pattern may be applied to each board, but variations in the drilling patterns may result in the formation of a PUF source for generating PUF data. The techniques of using randomized hole patterns to define a PUF source, such as the on-board PUF source 1805, may be used in conjunction with or separately from the use of passive components, as described in more detail herein.

[0165] In other embodiments, other techniques may be used to change or otherwise control the geometry of the traces on the PCB 1801 without the use flags and/or without drilling holes. Changing the geometry of a trace, regardless of the techniques used to form or alter the trace, affects the impedance characteristics of the trace and, therefore, the signature measured by the TDR 2001. Further, it is also possible to change the geometries of other types of structures embedded in or formed on the PCB 1801 within a signal path analyzed by the TDR 2001 in order to affect TDR measurements in a similar manner as described above for the traces 2052 and 2053.

[0166] Note that use of the on-board PUF source 1805 may facilitate detection of tamper attempts. For example, in the embodiment depicted by FIG. 20, any alteration of the path 2018 may change the impedance at one or more points along the path, thereby changing the signature detected by the TDR 2001. Indeed, if a hacker attempts to electrically connect hacking equipment or other external devices to the path 2018, the impedance at the connection points will be changed, thereby changing the signature measured by the TDR 2001. Thus, to detect tamper attempts, the TDR 2001 may be configured to interrogate the path 2018 and measure a signature of the returns and to then store the signature as a baseline for future measurements. Thereafter, when the TDR 2001 interrogates the path 2018 and measures a signature of the returns, the TDR 2001 may compare the current signature to the baseline signature previously measured by the

TDR 2001. Based on such comparison, the TDR 2001 may detect a tamper attempt if the current signature is materially different than the baseline signature.

[0167] In addition, such tamper attempts affecting the impedance of the path 2018 may similarly affect the PUF data that is obtained from the PUF source 1805, and the processing circuitry 1815 may similarly detect a tamper event in response to a change in PUF data or the key derived from the PUF data. As an example, the processing circuitry 1815 may obtain PUF data from the on-board PUF source 1805 using the TDR 2001 or otherwise, and store such PUF data as a baseline for future comparisons. Thereafter, when the processing circuitry 1815 obtains PUF data from the on-board PUF source 1805, the processing circuitry 1815 may compare the current PUF data to the baseline PUF data and detect a tamper event if the compared data does not match. Also, by changing the PUF data, a tamper event may prevent the processing circuitry 1815 from generating a valid key, thereby preventing it from performing at least one secure operation that relies on or uses the key, as described above.

[0168] In some embodiments, such as for example when the on-board PUF source 1805 is implemented using passive components, the on-board PUF source 1805 may be implemented within data paths between the reader chip 1807 and other components. As an example, FIG. 21 shows an embodiment in which the on-board PUF source 1805 is within a signal path between the reader chip 1807 and another component (*e.g.*, IC chip) 2100 mounted on the PCB 1801, such as any of the interfaces 102, 108, or 110 or the power source 106 depicted by FIG. 3. Alternatively, the on-board PUF source 1805 may be within a dedicated path for the PUF source 1805, as shown by FIG. 22, where other components that communicate with the reader chip 1807 are not electrically coupled to such path.

[0169] In some embodiments, the TDR 2001 may be coupled to a tamper mesh, such as any of the tamper meshes described above, and used to determine a signature based on the impedance characteristics of the tamper mesh. The TDR 2001 may be configured to detect a tamper attempt when a change to the tamper mesh changes its impedance and, thus, the signature measured by the TDR 2001, as described above for the on-board PUF source 1805 depicted by FIG. 20. If desired, the tamper mesh used to detect tamper attempts may include one or more flags formed in the traces defining the

tamper mesh with randomized hole patterns drilled into the flags, as further described above.

[0170] It should be noted that use of a TDR 2001 to measure or otherwise determine impedance characteristics of PUF sources is unnecessary, and it is possible for other types of devices to measure or otherwise determine the impedance characteristics of a PUF source for obtaining PUF data or detecting tamper attempts. In addition, the processing circuitry 1815 is described in several embodiments above as residing within a reader chip 1807, but it is possible for the processing circuitry 1815 to reside at other locations, such as in other types of IC chips.

Example Clauses

[0171] 1. A method for a device to engage in secure operations, the device having a physically unclonable function ("PUF") source configured to provide PUF data, comprising: acquiring the PUF data from the PUF source, wherein the PUF source is configured such that the PUF data provided by the PUF source changes in response to the PUF source experiencing a tamper attempt; correcting, at first error correction code circuitry of the device, the acquired PUF data based on an error correction code, wherein the error correction code is capable of correcting up to a threshold number of errors in the acquired PUF data; performing, by processing circuitry of the device, secure operations based on the corrected PUF data; correcting, at second error correction code circuitry of the device, the acquired PUF data based on a second error correction code, wherein the second error correction code is capable of correcting up to a second threshold number of errors in the acquired PUF data; performing, by the processing circuitry of the device, second secure operations based on the second corrected PUF data; and identifying, by the processing circuitry, the tamper attempt when the first error correction code is not capable of correcting each error in the acquired PUF data

[0172] 2. A method for a device to engage in secure operations, comprising: acquiring, from a physically unclonable function ("PUF") source of the device, PUF data, wherein the PUF source is associated with predetermined PUF data, and wherein the PUF source is configured such that the predetermined PUF data changes in response to the PUF source experiencing a tamper attempt; correcting, at error correction code circuitry of the device, the PUF data based on an error correction code, wherein the error

correction code is capable of correcting up to a threshold number of errors in PUF data as compared to the predetermined PUF data; and performing, by processing circuitry of the device, secure operations based on the corrected PUF data.

[0173] 3. The method of clause 2, further comprising: identifying, by the processing circuitry, the tamper attempt when the error correction code is not capable of correcting the errors in the PUF data.

[0174] 4. The method of clause 2, further comprising: correcting, at second error correction code circuitry of the device, the PUF data based on a second error correction code, wherein the second error correction code is capable of correcting up to a second threshold number of errors in PUF data as compared to the predetermined PUF data.

[0175] 5. The method of clause 4, further comprising: performing, by the processing circuitry of the device, second secure operations based on the second corrected PUF data.

[0176] 6. The method of clause 5, further comprising: identifying, by the processing circuitry, the tamper attempt when the error correction code is not capable of correcting the errors in the PUF data.

[0177] 7. The method of clause 2, wherein the PUF source comprises a memory device, an oscillator, an arbiter, a capacitance sensing circuit, or a time-domain reflection circuit.

[0178] 8. The method of clause 2, further comprising: acquiring, from a second PUF source of the device, second PUF data, wherein the second PUF source is associated with predetermined second PUF data.

[0179] 9. The method of clause 8, wherein the PUF source and the second PUF source are of different PUF source types.

[0180] 10. The method of clause 9, wherein each of the PUF source types is selected from the group comprising a memory device, an oscillator, an arbiter, a capacitance sensing circuit, or a time-domain reflection circuit.

[0181] 11. The method of clause 8, further comprising: combining the PUF data and the second PUF data prior to correcting, wherein the correcting corrects the combined PUF data and second PUF data.

[0182] 12. The method of clause 8, further comprising: correcting, at second error correction code circuitry of the device, the second PUF data based on a second error correction code, wherein the second error correction code is capable of correcting up to a threshold number of errors in the second PUF data as compared to the predetermined second PUF data; and performing, by the processing circuitry of the device, second secure operations based on the second corrected PUF data.

[0183] 13. A method for a device to engage in secure operations, the device having a physically unclonable function ("PUF") source configured to provide PUF data, comprising: acquiring the PUF data from the PUF source, wherein the PUF source is configured such that the PUF data provided by the PUF source changes in response to the PUF source experiencing a tamper attempt; correcting the acquired PUF data based on an error correction code; and performing, by processing circuitry of the device, secure operations based on the corrected PUF data.

[0184] 14. The method of clause 13, further comprising:

identifying, by the processing circuitry, the tamper attempt based on a change to the PUF data provided by the PUF source.

[0185] 15. The method of clause 13, wherein the error correction code is capable of correcting up to a threshold number of errors in the acquired PUF data, and wherein the method further comprises: correcting the acquired PUF data based on a second error correction code, wherein the second error correction code is capable of correcting up to a second threshold number of errors in the acquired PUF data.

[0186] 16. The method of clause 15, further comprising: determining, by the processing circuitry, whether to perform at least one secure operation based on whether the second error correction code successfully corrects each error in the acquired PUF data.

[0187] 17. The method of clause 13, further comprising: acquiring second PUF data from a second PUF source of the device, wherein the second PUF source is configured such that the second PUF data provided by the second PUF source changes in response to the PUF source experiencing a tamper attempt, and wherein the PUF source and the second PUF source are of different PUF source types; and combining the PUF data and the second PUF data.

[0188] 18. The method of clause 17, wherein each of the PUF source types is selected from the group comprising a memory device, an oscillator, an arbiter, a capacitance sensing circuit, or a time-domain reflection circuit.

[0189] 19. A device for engaging in secure operations, comprising: a physically unclonable function ("PUF") source configured to provide PUF data, wherein the PUF source is configured such that the PUF data provided by the PUF source changes in response to the PUF source experiencing a tamper attempt; processing circuitry configured to acquire the PUF data from the PUF source and to use the PUF data to perform secure operations; and error correction code circuitry configured to correct errors in the acquired PUF data prior to use of the PUF data in the secure operations.

[0190] 20. The device of clause 19, wherein the processing circuitry is configured to identify the tamper attempt based on a change to the PUF data provided by the PUF source.

[0191] 21. The device of clause 19, wherein the error correction code circuitry is configured to correct errors in the acquired PUF data based on first error correction code that is capable of correcting up to a threshold number of errors in the acquired PUF data, and wherein the device further comprises: second error correction circtuitry configured to correct errors in the acquired PUF data based on second error correction code that is capable of correcting up to a second threshold number of errors in the acquired PUF data.

[0192] 22. The device of clause 21, wherein the processing circuitry is configured to determine whether to perform at least one secure operation based on whether the second error correction code successfully corrects each error in the acquired PUF data.

[0193] 23. The device of clause 19, further comprising: a second PUF source configured to provide second PUF data, wherein the second PUF source is configured such that the second PUF data provided by the second PUF source changes in response to the second PUF source experiencing a tamper attempt, wherein the processing circuitry is configured to combine the PUF data and the second PUF data, and wherein the PUF source and the second PUF source are of different PUF source types.

[0194] 24. The device of clause 23, wherein each of the PUF source types is selected from the group comprising a memory device, an oscillator, an arbiter, a capacitance sensing circuit, or a time-domain reflection circuit.

[0195] 25. A payment reader, comprising: an interface for receiving payment information for a payment transaction from a payment device; a physically unclonable function (PUF) source; PUF measurement circuitry electrically coupled to the PUF source and configured to obtain PUF data from the PUF source; an anti-tamper device having an electrical characteristic that changes in response to an attempt by an unauthorized user to tamper with the payment reader; anti-tamper circuitry electrically coupled to the anti-tamper device and configured to detect the attempt by the unauthorized user to tamper with the payment reader based on a change to the electrical characteristic; a general processing unit having at least a first processor; and a cryptographic processing unit having at least a second processor configured to receive the PUF data, generate an encryption key based on the PUF data, and encrypt the payment information based on the encryption key, wherein the first processor is configured to send the encrypted payment information to a payment server for approval of the payment transaction, and wherein the cryptographic processing unit is configured to erase or modify the PUF data or the encryption key in response to the attempt detected by the anti-tamper circuitry.

[0196] 26. A payment reader, comprising: an interface for receiving payment information for a payment transaction from a payment device; a physically unclonable function (PUF) source; PUF measurement circuitry electrically coupled to the PUF source and configured to obtain PUF data from the PUF source; and at least one processing unit having at least a first processor configured to send the payment information to a payment server for approval of the payment transaction, the at least one processing unit configured to perform a secure operation for processing the payment information based on the PUF data.

[0197] 27. The payment reader of clause 26, wherein the interface has an antenna for wirelessly communicating with the payment device to receive the payment information.

[0198] 28. The payment reader of clause 26, wherein the interface has an EMV slot for receiving the payment device, and wherein the interface is configured to communicate with an EMV chip of the payment device to receive the payment information.

[0199] 29. The payment reader of clause 26, wherein the interface has a magnetic strip reader for reading the payment information from a magnetic strip of the payment device.

[0200] 30. The payment reader of clause 26, wherein the at least one processing unit includes a general processing unit having the first processor, wherein the at least one processing unit includes a cryptographic processing unit having a second processor, and wherein the second processor is configured to generate a key for encrypting the payment information based on the PUF data.

[0201] 31. The payment reader of clause 26, wherein the PUF measurement circuitry is integrated within a secure enclave of the payment reader.

[0202] 32. The payment reader of clause 26, further comprising: an anti-tamper device having an electrical characteristic that changes in response to a tamper attempt; and anti-tamper circuitry electrically coupled to the anti-tamper device and configured to detect the tamper attempt based on a change to the electrical characteristic.

[0203] 33. The payment reader of clause 32, wherein the payment reader is configured to modify the PUF source in response to the detected tamper attempt.

[0204] 34. The payment reader of clause 32, wherein the payment reader is configured to modify or erase a value derived from the PUF data in response to the detected tamper attempt.

[0205] 35. The payment reader of clause 32, wherein the at least one processing unit includes a general processing unit having the first processor, wherein the at least one processing unit includes a cryptographic processing unit having a second processor, wherein the second processor is configured to (1) perform a cryptographic operation for processing the payment information based on a value derived from the PUF data and (2) store the value in memory of the cryptographic processing unit, and wherein the cryptographic processing unit is configured to erase the value from the memory or modify the value in response to the detected tamper attempt.

[0206] 36. The payment reader of clause 32, wherein the anti-tamper device comprises the PUF source.

[0207] 37. The payment reader of clause 32, wherein the anti-tamper device comprises a tamper mesh, and wherein the tamper mesh comprises the PUF source.

[0208] 38. The payment reader of clause 32, wherein the at least one processing unit is configured to transmit a notification to the payment server in response to the detected tamper attempt.

[0209] 39. The payment reader of clause 38, wherein the at least one processing unit is configured to transmit a notification to a merchant device associated with the payment transaction in response to the detected tamper attempt.

[0210] 40. A method for use in a payment reader to process a payment transaction, comprising: receiving, by an interface of the payment reader, payment information for the payment transaction from a payment device; obtaining physically unclonable function (PUF) data from a PUF source of the payment reader; performing a secure operation for processing the payment information within the payment reader based on the PUF data; and sending the payment information from the payment reader to a payment server for approval of the payment transaction.

[0211] 41. The method of clause 40, wherein the receiving comprises wirelessly receiving the payment information with an antenna of the payment reader.

[0212] 42. The method of clause 40, further comprising receiving the payment device with an EMV slot of the payment reader, wherein the receiving the payment information comprises receiving the payment information from an EMV chip of the payment device.

[0213] 43. The method of clause 40, wherein the receiving comprises reading a magnetic strip of the payment device with a magnetic strip reader of the payment reader.

[0214] 44. The method of clause 40, wherein the performing the secure operation comprises generating a key for encrypting the payment information based on the PUF data.

[0215] 45. The method of clause 44, wherein the sending is performed by a processor of a general processing unit of the payment reader, and wherein the generating is performed by a processor of a cryptographic processing unit of the payment reader.

[0216] 46. The method of clause 40, wherein the obtaining is performed by PUF measurement circuitry of the payment reader, wherein the PUF measurement circuitry is integrated within a secure enclave of the payment reader.

[0217] 47. The method of clause 40, further comprising detecting a tamper attempt in response to a change in an electrical characteristic of an anti-tamper device of the payment reader.

[0218] 48. The method of clause 47, further comprising modifying the PUF source in response to the detecting.

[0219] 49. The method of clause 47, further comprising modifying or erasing a value derived from the PUF data in response to the detecting.

[0220] 50. The method of clause 47, wherein the performing the secure operation is performed by a processor of a cryptographic processing unit of the payment reader based on a value derived from the PUF data, and wherein the method comprises:

storing the value in memory of the cryptographic processing unit; and

in response to the detecting, erasing the value from the memory or modifying the value.

[0221] 51. The method of clause 47, wherein the anti-tamper device comprises the PUF source.

[0222] 52. The method of clause 47, wherein the anti-tamper device comprises a tamper mesh, and wherein the tamper mesh comprises the PUF source.

[0223] 53. The method of clause 47, further comprising transmitting a notification from the payment reader to the payment server in response to the detecting.

[0224] 54. The method of clause 47, further comprising transmitting a notification from the payment reader to a merchant device associated with the payment transaction in response to the detecting.

[0225] 55. A method for modifying a physically unclonable function (PUF) source of a device by changing a resistance of a fuse of the PUF source in response to a tamper attempt, the method comprising: transmitting a first signal through the fuse of the PUF source; measuring a parameter of the first signal with a sensor of the device; generating a pre-tamper PUF value using the parameter of the first signal measured by the sensor; generating a cryptographic key using the pre-tamper PUF value; detecting an

attempt to tamper with the device; modifying the PUF source in response to detection of the attempt, the modifying comprising transmitting through the fuse a second signal of sufficiently high current or voltage to change a resistance of the fuse; transmitting a third signal through the fuse after the modifying; measuring a parameter of the third signal with the sensor of the device; and generating a post-tamper PUF value using the parameter of the third signal measured by the sensor.

[0226] 56. The method of clause 55, wherein the fuse is included in a plurality of fuses, and wherein the modifying randomly changes responses of the plurality of fuses to the third signal.

[0227] 57. The method of clause 55, wherein the device is a payment reader, and wherein the method further comprises using the cryptographic key to perform a payment transaction.

[0228] 58. A method for modifying a physically unclonable function (PUF) source of a device, the PUF source having at least one fuse embedded in the device, the method comprising: transmitting a first signal through the at least one fuse of the PUF source; measuring a parameter of the first signal with a sensor; providing a PUF value from the PUF source based on the parameter of the first signal measured by the sensor; processing the PUF value within the device to perform an operation; detecting an event at the device subsequent to the processing; determining, with processing circuitry of the device, to modify the PUF source based on the detected event; and modifying the PUF source in response to the determining, the modifying comprising transmitting through the at least one fuse a second signal of sufficiently high current or voltage to change a resistance of the at least one fuse.

[0229] 59. The method of clause 58, further comprising applying an input to the PUF source, wherein the transmitting is performed in response to the input, and wherein the modifying changes a response of the PUF source to the input.

[0230] 60. The method of clause 58, wherein the at least one fuse comprise a plurality of fuses, wherein the method further comprises applying an input to the PUF source, wherein the transmitting is performed in response to the input, and wherein the modifying randomly changes responses of the plurality of fuses to the input.

[0231] 61. The method of clause 58, wherein the event is a reception of a user input by the device.

[0232] 62. The method of clause 58, wherein the event is an attempt to tamper with the device.

[0233] 63. The method of clause 58, wherein the device is a payment reader, and wherein the operation is performance of a payment transaction.

[0234] 64. The method of clause 58, further comprising authenticating the device based on the PUF value.

[0235] 65. The method of clause 58, wherein the processing comprises generating a cryptographic key based on the PUF value.

[0236] 66. The method of clause 58, wherein the processing comprises generating an authentication token based on the PUF value.

[0237] 67. The method of clause 58, wherein the at least one fuse has a dielectric layer, and wherein the voltage of the second signal exceeds a breakdown voltage of the dielectric layer.

[0238] 68. The method of clause 58, wherein the at least one fuse has a layer of amorphous silicon, and wherein the voltage of the second signal is sufficiently high to convert the amorphous silicon to a polycrystalline silicon-metal alloy.

[0239] 69. A device, comprising: a physically unclonable function (PUF) source having at least one fuse, the PUF source responsive to an input for providing a PUF value based on measurement of a parameter of a first signal transmitted through the at least one fuse; and circuitry configured to process the PUF value to perform an operation within the device, the circuitry further configured to select the at least one fuse for modification based on an event detected by the circuitry and to modify the at least one fuse by transmitting a second signal of sufficiently high current or voltage to change a resistance of the at least one fuse, thereby changing a response of the PUF source to the input.

[0240] 70. The device of clause 69, wherein the event is a reception of a user input by the device.

[0241] 71. The device of clause 69, wherein the event is an attempt to tamper with the device.

[0242] 72. The device of clause 69, wherein the device is a payment reader, and wherein the operation is performance of a payment transaction.

[0243] 73. The device of clause 69, wherein the circuitry is configured to generate a cryptographic key based on the PUF value.

[0244] 74. The device of clause 69, wherein the circuitry is configured to generate an authentication token based on the PUF value.

[0245] 75. The device of clause 69, wherein the at least one fuse has a dielectric layer, and wherein the voltage of the second signal exceeds a breakdown voltage of the dielectric layer.

[0246] 76. The device of clause 69, wherein the at least one fuse has a layer of amorphous silicon, and wherein the voltage of the second signal is sufficiently high to convert the amorphous silicon to a polycrystalline silicon-metal alloy.

[0247] 77. A method for modifying a physically unclonable function (PUF) source of a device, the PUF source having at least one fuse embedded in the device, the method comprising: applying an input to the PUF source, thereby causing current to flow through the at least one fuse of the PUF source; measuring the current with a sensor; providing a PUF value from the PUF source based on the measured current; processing the PUF value within the device to perform an operation; detecting an event at the device subsequent to the processing; determining, with processing circuitry of the device, to modify the PUF source based on the detected event; and modifying the PUF source in response to the determining, the modifying comprising transmitting through the at least one fuse a sufficient amount of current to change a resistance of the at least one fuse, thereby changing a response of the PUF source to the input.

[0248] 78. The method of clause 77, wherein the device is a payment reader, and wherein the operation is performance of a payment transaction.

[0249] 79. The method of clause 77, wherein the processing comprises generating a cryptographic key based on the PUF value.

[0250] 80. The method of clause 77, wherein the processing comprises generating an authentication token based on the PUF value.

[0251] 81. A payment reader device, comprising: a payment chip with processing circuitry to perform a secure payment operation; and a physically unclonable function

(PUF) component located outside of the payment chip but within the payment reader device, the PUF component configured to generate PUF data used by the payment chip to perform the secure payment operation.

[0252] 82. The payment reader device of clause 81, wherein the PUF component comprises a passive device embedded in a printed circuit board of the payment reader device.

[0253] 83. The payment reader device of clause 81, wherein the processing circuitry is configured to combine the PUF data with another PUF data generated by another PUF component located inside of the payment chip to form combined PUF data, and wherein the payment chip uses the combined PUF data for the secure payment operation.

[0254] 84. The payment reader device of clause 81, wherein the secure payment operation includes encrypting payment card data.

[0255] 85. The payment reader device of clause 81, wherein the secure payment operation includes authenticating the payment reader device.

[0256] 86. The payment reader device of clause 81, wherein the processing circuitry comprises a time-domain reflectometer configured to transmit an electrical signal through the first PUF source and to measure returns of the electrical signal, and wherein the processing circuitry is configured to determine the PUF data based on the measured returns.

[0257] 87. An electronic device, comprising: a printed circuit board having a first physically unclonable function (PUF) source; and an integrated circuit (IC) chip positioned on the printed circuit board, the IC chip having processing circuitry, the processing circuitry configured to receive first PUF data from the first PUF source, the processing circuitry further configured to determine a cryptographic key or authentication token using the first PUF data, wherein the first PUF source is embedded in or formed on the printed circuit board external to the IC chip.

[0258] 88. The electronic device of clause 87, wherein the first PUF source comprises a passive device.

[0259] 89. The payment reader of clause 87, wherein the processing circuitry comprises a time-domain reflectometer configured to transmit an electrical signal through

the first PUF source and to measure returns of the electrical signal, and wherein the processing circuitry is configured to determine the first PUF data based on the measured returns.

[0260] 90. The electronic device of clause 87, wherein the IC chip has a second PUF source, wherein the processing circuitry is configured to receive second PUF data from the second PUF source, and wherein the determined cryptographic key or authentication token is based on the second PUF data.

[0261] 91. The payment reader of clause 90, wherein at least one of the first PUF source and the second PUF source has a fuse, and wherein the processing circuitry is configured to modify the at least one of the first PUF source and the second PUF source by transmitting through the fuse an electrical signal of sufficiently high current or voltage to change a resistance of the fuse.

[0262] 92. The electronic device of clause 87, wherein the electronic device is a payment reader, and wherein the IC chip is a reader chip configured to receive payment data read by the payment reader and to process the payment data based on the determined cryptographic key or authentication token.

[0263] 93. The electronic device of clause 92, wherein the processing circuitry is configured to combine the first PUF data and the second PUF data to form combined PUF data, and wherein the determined cryptographic key or authentication token is based on the combined PUF data.

[0264] 94. The electronic device of clause 92, wherein the secure operation includes encrypting the payment data.

[0265] 95. The electronic device of clause 92, wherein the secure operation includes authenticating the reader chip,

[0266] 96. A method for use with an electronic device having a printed circuit board, wherein the printed circuit board has a first physically unclonable function (PUF) source, the method comprising: determining first PUF data from the first PUF source with processing circuitry of an integrated circuit (IC) chip residing on the printed circuit board, wherein the first PUF source is embedded in or formed on the printed circuit board external to the IC chip; determining a cryptographic key or authentication token with the processing circuitry based on the first PUF data; and performing at least one secure

operation within the IC chip using the determined cryptographic key or authentication token.

[0267] 97. The method of clause 96, wherein the first PUF source comprises a passive device.

[0268] 98. The method of clause 96, further comprising: transmitting an electrical signal from a time-domain reflectometer of the processing circuitry through the first PUF source; and measuring returns of the electrical signal with the time-domain reflectometer, wherein the determining the first PUF data is based on the measured returns.

[0269] 99. The method of clause 96, wherein the IC chip has a second PUF source, and wherein the method further comprises: determining second PUF data with the processing circuitry based on the second PUF source, wherein the determining the cryptographic key or authentication token is based on the second PUF data.

[0270] 100. The method of clause 99, wherein at least one of the first PUF source and the second PUF source has a fuse, and wherein the method further comprises modifying the at least one of the first PUF source and the second PUF source by transmitting through the fuse an electrical signal of sufficiently high current or voltage to change a resistance of the fuse.

[0271] 101. The method of clause 96, wherein the electronic device is a payment reader, wherein the IC chip is a reader chip, and wherein the method further comprises: receiving, at the reader chip, payment data read by the payment reader; and processing the payment data with the processing circuitry based on the determined cryptographic key or authentication token.

[0272] 102. The method of clause 101, further comprising: combining the first PUF data and the second PUF data to form combined PUF data, wherein the determining the cryptographic key or authentication token is based on the combined PUF data.

[0273] 103. The method of clause 101, wherein the performing the secure operation comprises encrypting the payment data.

[0274] 104. The method of clause 101, wherein the performing the secure operation comprises authenticating the reader chip.

[0275] The foregoing is merely illustrative of the principles of this disclosure and various modifications may be made by those skilled in the art without departing from the scope of this disclosure. The above described embodiments are presented for purposes of illustration and not of limitation. The present disclosure also can take many forms other than those explicitly described herein. Accordingly, it is emphasized that this disclosure is not limited to the explicitly disclosed methods, systems, and apparatuses, but is intended to include variations to and modifications thereof, which are within the spirit of the following claims.

[0276] As a further example, variations of apparatus or process parameters (*e.g.*, dimensions, configurations, components, process step order, *etc.*) may be made to further optimize the provided structures, devices and methods, as shown and described herein. In any event, the structures and devices, as well as the associated methods, described herein have many applications. Therefore, the disclosed subject matter should not be limited to any single embodiment described herein, but rather should be construed in breadth and scope in accordance with the appended claims.

CLAUSES SECTION

What is claimed is:

1. A method for modifying a physically unclonable function (PUF) source of a device, the PUF source having at least one fuse embedded in the device, the method comprising:

transmitting a first signal through the at least one fuse of the PUF source;

measuring a parameter of the first signal with a sensor;

providing a PUF value from the PUF source based on the parameter of the first signal measured by the sensor;

processing the PUF value within the device to perform an operation;

detecting an event at the device subsequent to the processing;

determining, with processing circuitry of the device, to modify the PUF source based on the detected event; and

modifying the PUF source in response to the determining, the modifying comprising transmitting through the at least one fuse a second signal of sufficiently high current or voltage to change a resistance of the at least one fuse.

2. The method of claim 1, further comprising applying an input to the PUF source, wherein the transmitting is performed in response to the input, and wherein the modifying changes a response of the PUF source to the input.

3. The method of claim 1, wherein the at least one fuse comprise a plurality of fuses, wherein the method further comprises applying an input to the PUF source, wherein the transmitting is performed in response to the input, and wherein the modifying randomly changes responses of the plurality of fuses to the input.

4. The method of claim 1, wherein the event is a reception of a user input by the device.

5. The method of claim 1, wherein the event is an attempt to tamper with the device.

6. The method of claim 1, wherein the device is a payment reader, and wherein the operation is performance of a payment transaction.

7. The method of claim 1, wherein the processing comprises generating a cryptographic key based on the PUF value.

8. The method of claim 1, wherein the processing comprises generating an authentication token based on the PUF value.

9. The method of claim 1, wherein the at least one fuse has a dielectric layer, and wherein the voltage of the second signal exceeds a breakdown voltage of the dielectric layer.

10. The method of claim 1, wherein the at least one fuse has a layer of amorphous silicon, and wherein the voltage of the second signal is sufficiently high to convert the amorphous silicon to a polycrystalline silicon-metal alloy.

11. A device, comprising:

a physically unclonable function (PUF) source having at least one fuse, the PUF source responsive to an input for providing a PUF value based on measurement of a parameter of a first signal transmitted through the at least one fuse; and

circuitry configured to process the PUF value to perform an operation within the device, the circuitry further configured to select the at least one fuse for modification based on an event detected by the circuitry and to modify the at least one fuse by transmitting a second signal of sufficiently high current or voltage to change a resistance of the at least one fuse, thereby changing a response of the PUF source to the input.

12. The device of claim 11, wherein the event is an attempt to tamper with the device.

13. The device of claim 11, wherein the device is a payment reader, and wherein the operation is performance of a payment transaction.

14. The device of claim 11, wherein the at least one fuse has a dielectric layer, and wherein the voltage of the second signal exceeds a breakdown voltage of the dielectric layer.

15. The device of claim 11, wherein the at least one fuse has a layer of amorphous silicon, and wherein the voltage of the second signal is sufficiently high to convert the amorphous silicon to a polycrystalline silicon-metal alloy.

16. An electronic device, comprising:

a printed circuit board having a first physically unclonable function (PUF) source; and

an integrated circuit (IC) chip positioned on the printed circuit board, the IC chip having processing circuitry, the processing circuitry configured to receive first PUF data from the first PUF source, the processing circuitry further configured to determine a cryptographic key or authentication token using the first PUF data, wherein the first PUF source is embedded in or formed on the printed circuit board external to the IC chip.

17. The electronic device of claim 16, wherein the first PUF source comprises a passive device.

18. The payment reader of claim 16, wherein the processing circuitry comprises a time-domain reflectometer configured to transmit an electrical signal through the first PUF source and to measure returns of the electrical signal, and wherein the processing circuitry is configured to determine the first PUF data based on the measured returns.

19. The electronic device of claim 16, wherein the IC chip has a second PUF source, wherein the processing circuitry is configured to receive second PUF data from the second PUF source, and wherein the determined cryptographic key or authentication token is based on the second PUF data.

20. The electronic device of claim 16, wherein the electronic device is a payment reader, and wherein the IC chip is a reader chip configured to receive payment data read by the payment reader and to process the payment data based on the determined cryptographic key or authentication token.

21. The electronic device of claim 20, wherein the processing circuitry is configured to combine the first PUF data and the second PUF data to form combined PUF data, and wherein the determined cryptographic key or authentication token is based on the combined PUF data.

22. A method for use with an electronic device having a printed circuit board, wherein the printed circuit board has a first physically unclonable function (PUF) source, the method comprising:

determining first PUF data from the first PUF source with processing circuitry of an integrated circuit (IC) chip residing on the printed circuit board, wherein the first PUF source is embedded in or formed on the printed circuit board external to the IC chip;

determining a cryptographic key or authentication token with the processing circuitry based on the first PUF data; and

performing at least one secure operation within the IC chip using the determined cryptographic key or authentication token.

23. The method of claim 22, wherein the first PUF source comprises a passive device.

24. The method of claim 22, further comprising:

transmitting an electrical signal from a time-domain reflectometer of the processing circuitry through the first PUF source; and

measuring returns of the electrical signal with the time-domain reflectometer,

wherein the determining the first PUF data is based on the measured returns.

25. The method of claim 22, wherein the IC chip has a second PUF source, and wherein the method further comprises:

determining second PUF data with the processing circuitry based on the second PUF source,

wherein the determining the cryptographic key or authentication token is based on the second PUF data.

26. The method of claim 22, wherein the electronic device is a payment reader, wherein the IC chip is a reader chip, and wherein the method further comprises:

receiving, at the reader chip, payment data read by the payment reader; and

processing the payment data with the processing circuitry based on the determined cryptographic key or authentication token.

27. The method of claim 22, further comprising:

combining the first PUF data and the second PUF data to form combined PUF data,

wherein the determining the cryptographic key or authentication token is based on the combined PUF data.

28. The method of claim 22, wherein the performing the secure operation comprises encrypting the payment data.

29. A method for a device to engage in secure operations, the device having a physically unclonable function ("PUF") source configured to provide PUF data, comprising:

acquiring the PUF data from the PUF source, wherein the PUF source is configured such that the PUF data provided by the PUF source changes in response to the PUF source experiencing a tamper attempt;

correcting the acquired PUF data based on an error correction code; and

performing, by processing circuitry of the device, secure operations based on the corrected PUF data.

30. The method of claim 29, further comprising:

identifying, by the processing circuitry, the tamper attempt based on a change to the PUF data provided by the PUF source.

31. The method of claim 29, wherein the error correction code is capable of correcting up to a threshold number of errors in the acquired PUF data, and wherein the method further comprises:

correcting the acquired PUF data based on a second error correction code, wherein the second error correction code is capable of correcting up to a second threshold number of errors in the acquired PUF data.

32. The method of claim 29, further comprising:

determining, by the processing circuitry, whether to perform at least one secure operation based on whether the second error correction code successfully corrects each error in the acquired PUF data.

33. The method of claim 29, further comprising:

acquiring second PUF data from a second PUF source of the device, wherein the second PUF source is configured such that the second PUF data provided by the second PUF source changes in response to the PUF source experiencing a tamper attempt, and wherein the PUF source and the second PUF source are of different PUF source types; and

combining the PUF data and the second PUF data.

34. The method of claim 33, wherein each of the PUF source types is selected from the group comprising a memory device, an oscillator, an arbiter, a capacitance sensing circuit, or a time-domain reflection circuit.

35. A device for engaging in secure operations, comprising:

a physically unclonable function ("PUF") source configured to provide PUF data, wherein the PUF source is configured such that the PUF data provided by the PUF source changes in response to the PUF source experiencing a tamper attempt;

processing circuitry configured to acquire the PUF data from the PUF source and to use the PUF data to perform secure operations; and

error correction code circuitry configured to correct errors in the acquired PUF data prior to use of the PUF data in the secure operations.

36. The device of claim 35, wherein the processing circuitry is configured to identify the tamper attempt based on a change to the PUF data provided by the PUF source.

37. The device of claim 35, wherein the error correction code circuitry is configured to correct errors in the acquired PUF data based on first error correction code that is capable of correcting up to a threshold number of errors in the acquired PUF data, and wherein the device further comprises:

second error correction circtuitry configured to correct errors in the acquired PUF data based on second error correction code that is capable of correcting up to a second threshold number of errors in the acquired PUF data.

38. The device of claim 37, wherein the processing circuitry is configured to determine whether to perform at least one secure operation based on whether the second error correction code successfully corrects each error in the acquired PUF data.

39. The device of claim 35, further comprising:

a second PUF source configured to provide second PUF data, wherein the second PUF source is configured such that the second PUF data provided by the second PUF source changes in response to the second PUF source experiencing a tamper attempt, wherein the processing circuitry is configured to combine the PUF data and the second PUF data, and wherein the PUF source and the second PUF source are of different PUF source types.

40. The device of claim 39, wherein each of the PUF source types is selected from the group comprising a memory device, an oscillator, an arbiter, a capacitance sensing circuit, or a time-domain reflection circuit.

41. A payment reader, comprising:

an interface for receiving payment information for a payment transaction from a payment device;

a physically unclonable function (PUF) source;

PUF measurement circuitry electrically coupled to the PUF source and configured to obtain PUF data from the PUF source; and

at least one processing unit having at least a first processor configured to send the payment information to a payment server for approval of the payment transaction, the at least one processing unit configured to perform a secure operation for processing the payment information based on the PUF data.

42. The payment reader of claim 41, wherein the interface has an EMV slot for receiving the payment device, and wherein the interface is configured to communicate with an EMV chip of the payment device to receive the payment information.

43. The payment reader of claim 41, wherein the at least one processing unit includes a general processing unit having the first processor, wherein the at least one processing unit includes a cryptographic processing unit having a second processor, and

wherein the second processor is configured to generate a key for encrypting the payment information based on the PUF data.

44. The payment reader of claim 41, wherein the PUF measurement circuitry is integrated within a secure enclave of the payment reader.

45. The payment reader of claim 41, further comprising:

an anti-tamper device having an electrical characteristic that changes in response to a tamper attempt; and

anti-tamper circuitry electrically coupled to the anti-tamper device and configured to detect the tamper attempt based on a change to the electrical characteristic.

46. The payment reader of claim 45, wherein the at least one processing unit includes a general processing unit having the first processor, wherein the at least one processing unit includes a cryptographic processing unit having a second processor, wherein the second processor is configured to (1) perform a cryptographic operation for processing the payment information based on a value derived from the PUF data and (2) store the value in memory of the cryptographic processing unit, and wherein the cryptographic processing unit is configured to erase the value from the memory or modify the value in response to the detected tamper attempt.

47. The payment reader of claim 45, wherein the anti-tamper device comprises the PUF source.

48. The payment reader of claim 45, wherein the anti-tamper device comprises a tamper mesh, and wherein the tamper mesh comprises the PUF source.

49. A method for use in a payment reader to process a payment transaction, comprising:

receiving, by an interface of the payment reader, payment information for the payment transaction from a payment device;

obtaining physically unclonable function (PUF) data from a PUF source of the payment reader;

performing a secure operation for processing the payment information within the payment reader based on the PUF data; and

sending the payment information from the payment reader to a payment server for approval of the payment transaction.

50. The method of claim 49, wherein the performing the secure operation comprises generating a key for encrypting the payment information based on the PUF data, wherein the sending is performed by a processor of a general processing unit of the payment reader, and wherein the generating is performed by a processor of a cryptographic processing unit of the payment reader.

51. The method of claim 49, wherein the obtaining is performed by PUF measurement circuitry of the payment reader, wherein the PUF measurement circuitry is integrated within a secure enclave of the payment reader.

52. The method of claim 49, further comprising detecting a tamper attempt in response to a change in an electrical characteristic of an anti-tamper device of the payment reader, wherein the anti-tamper device comprises the PUF source.

53. The method of claim 49, further comprising detecting a tamper attempt in response to a change in an electrical characteristic of an anti-tamper device of the payment reader, wherein the anti-tamper device comprises a tamper mesh, and wherein the tamper mesh comprises the PUF source.

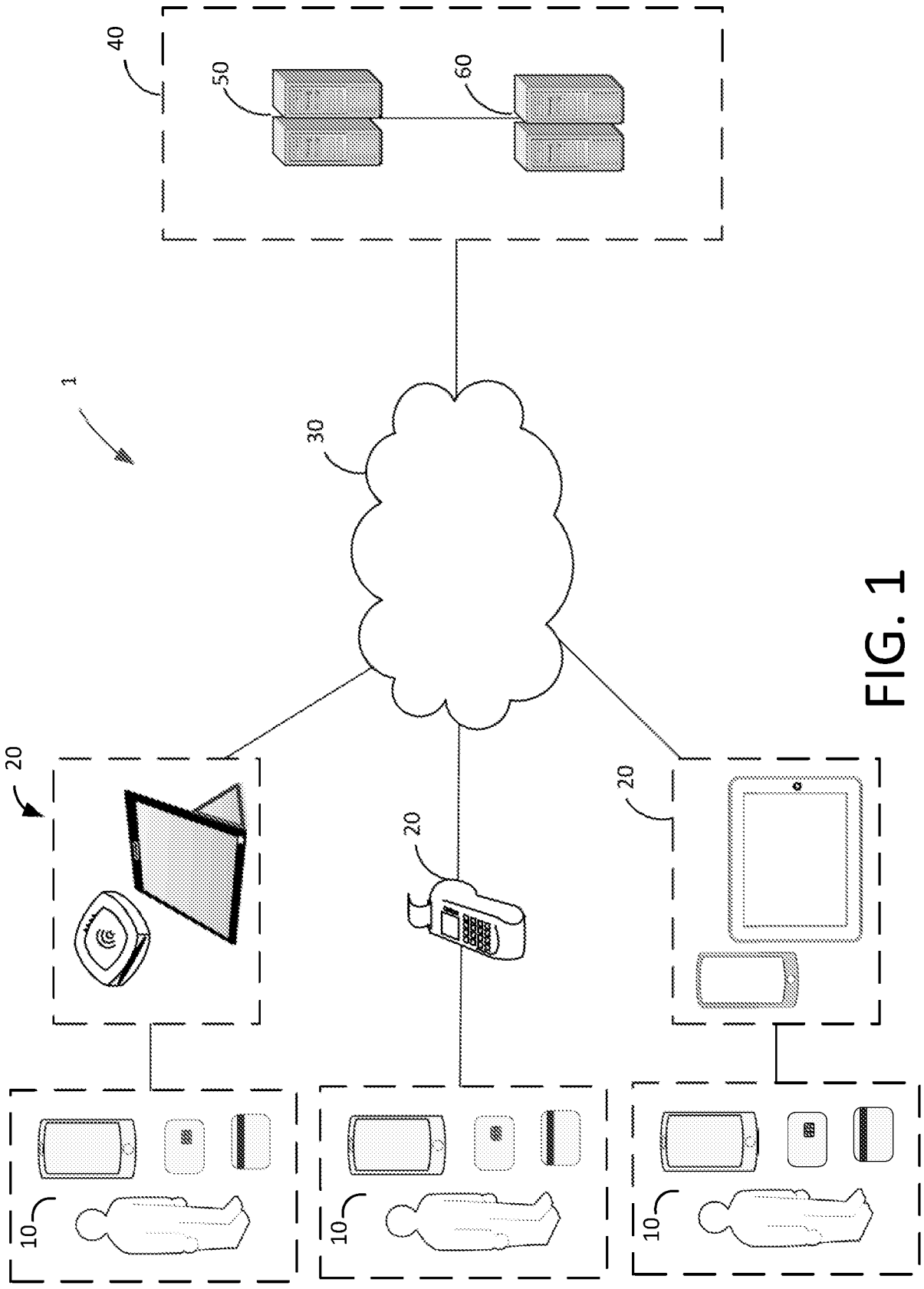
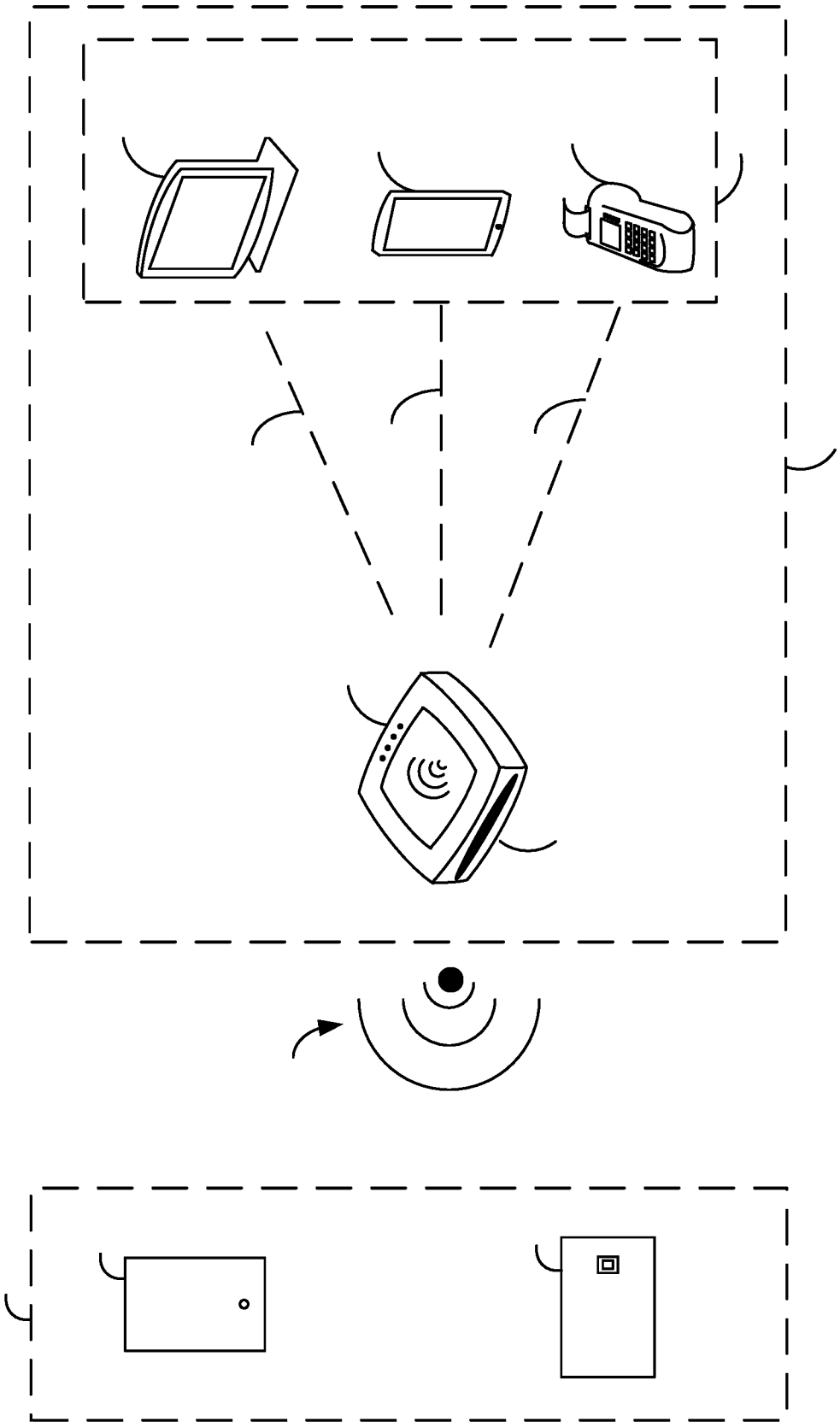
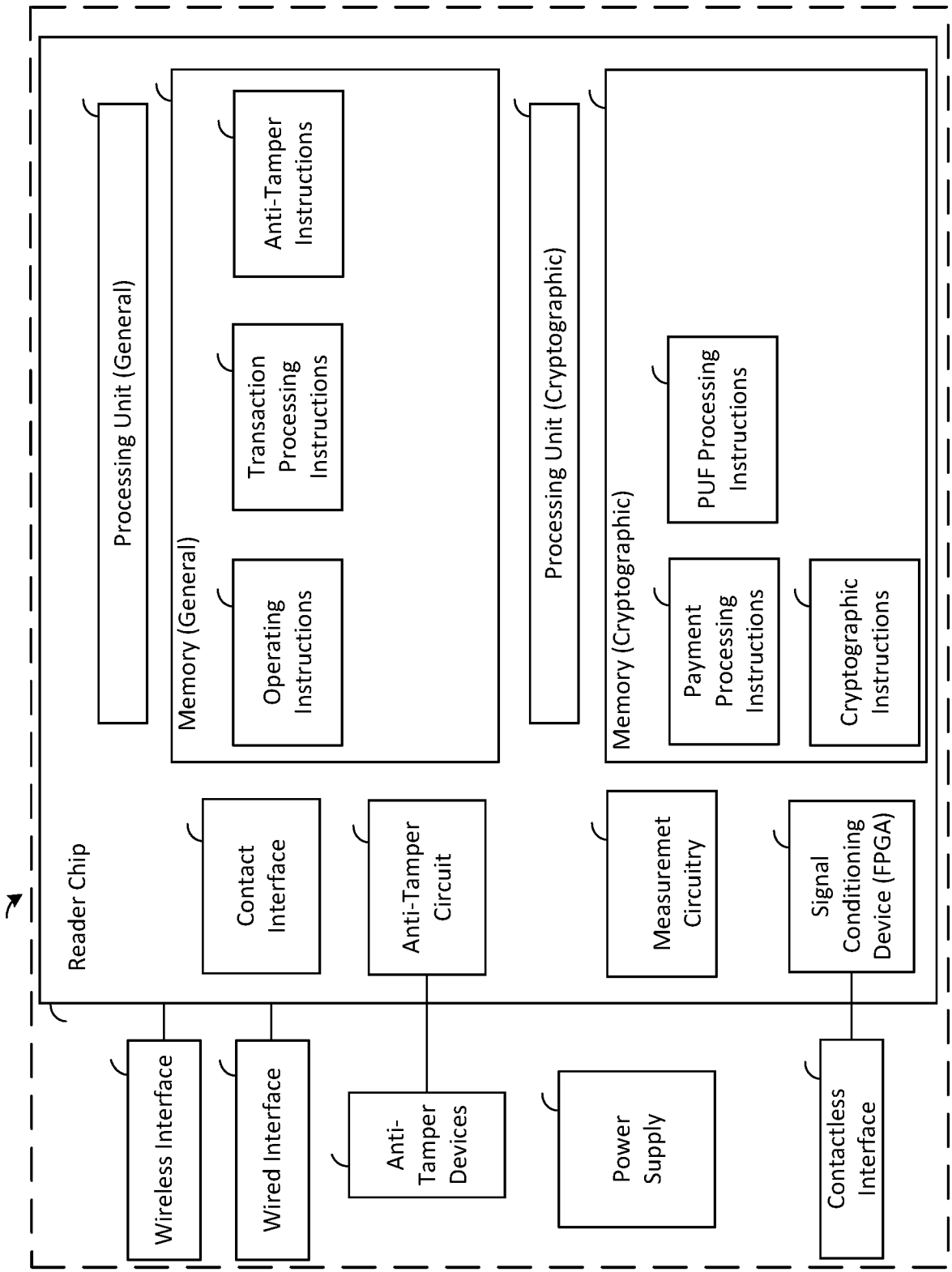
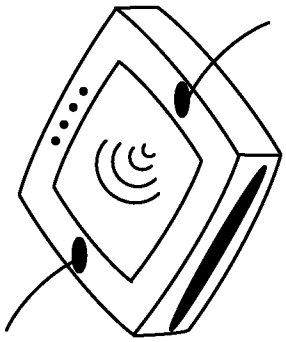


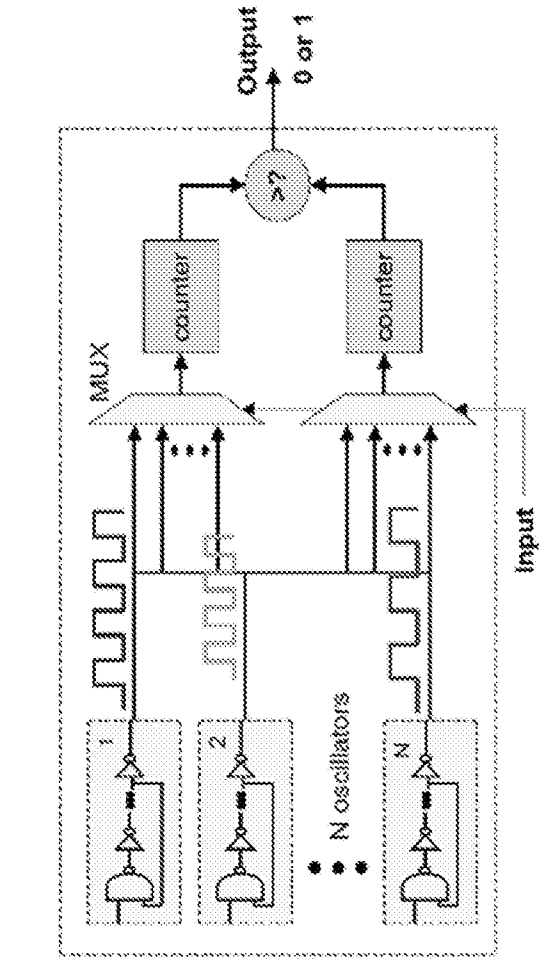
FIG. 1

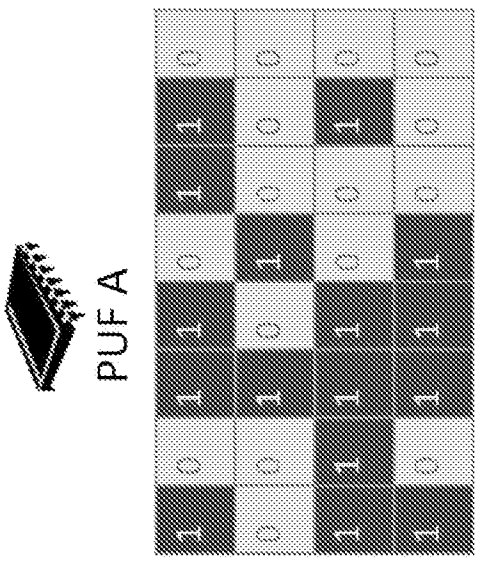


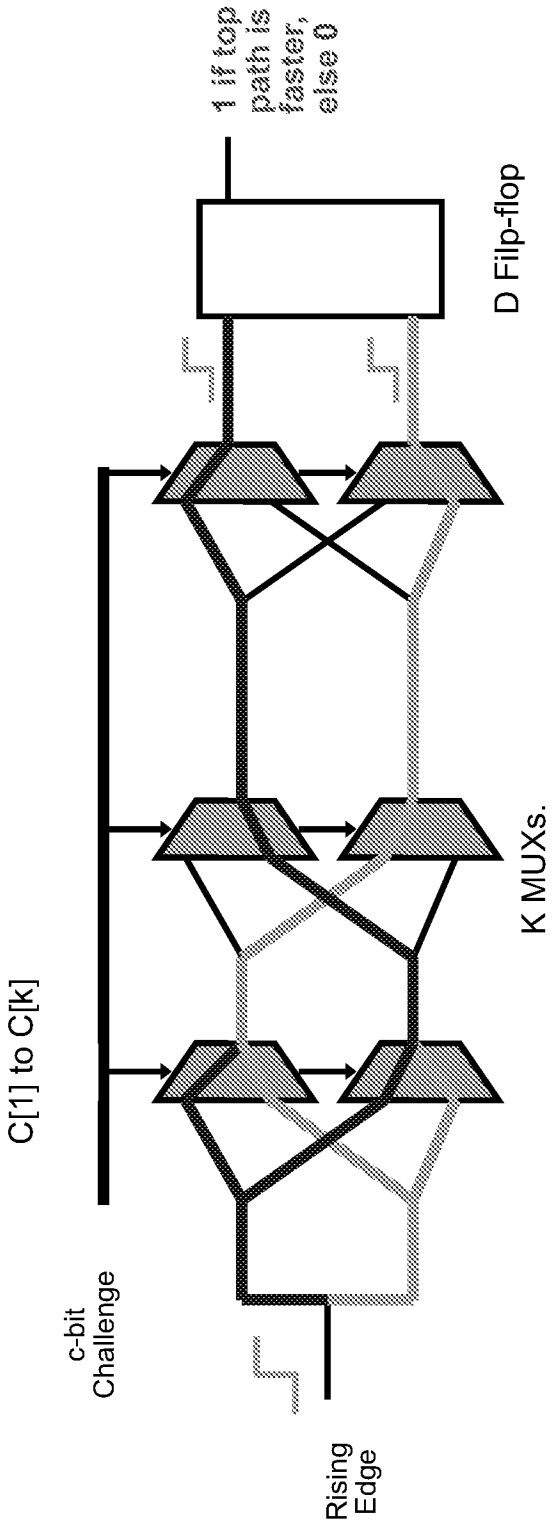

Reader Chip
Processing Unit (General)
Memory (General)
Anti-Tamper Instructions
Transaction Processing Instructions
Operating Instructions
Processing Unit (Cryptographic)
Memory (Cryptographic)
PUF Processing Instructions
Payment Processing Instructions
Cryptographic Instructions
Contact Interface
Anti-Tamper Circuit
Measuremet Circuitry
Signal Conditioning Device (FPGA)
Wireless Interface
Wired Interface
Anti-Tamper Devices
Power Supply
Contactless Interface

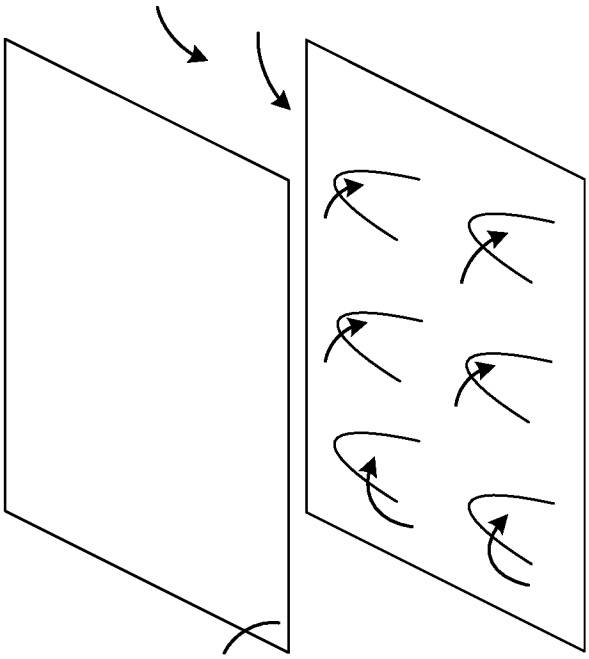


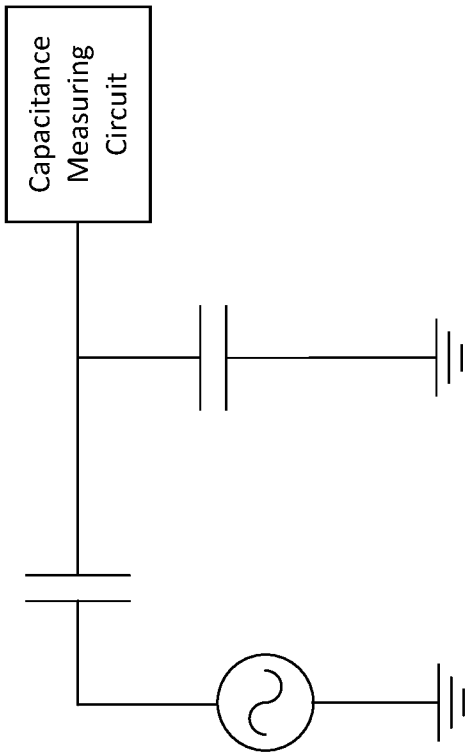


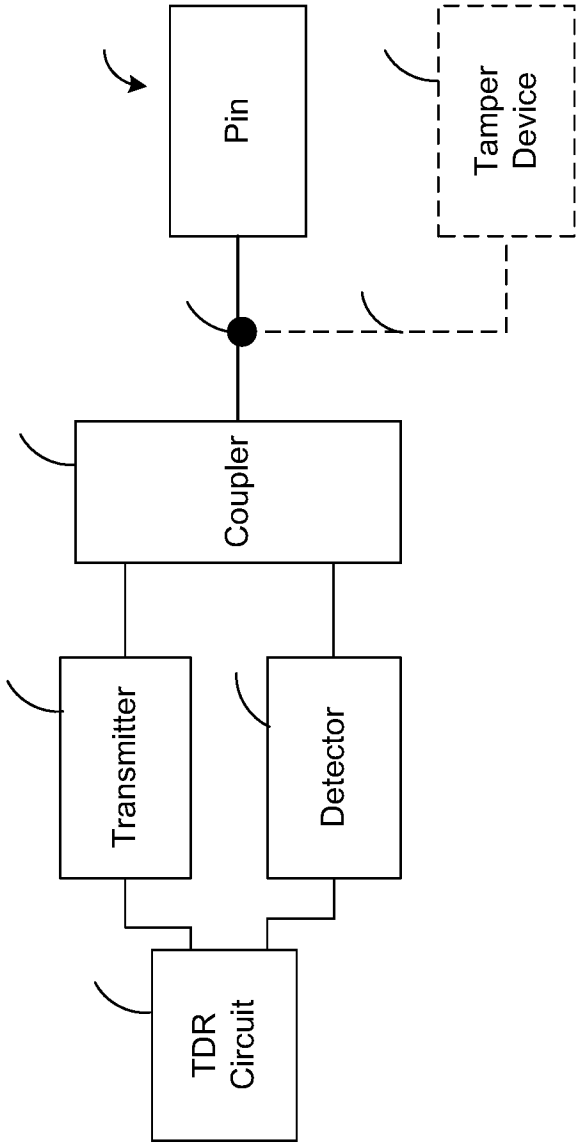

Output
0 or 1
>?
counter
counter
MUX
N oscillators
Input

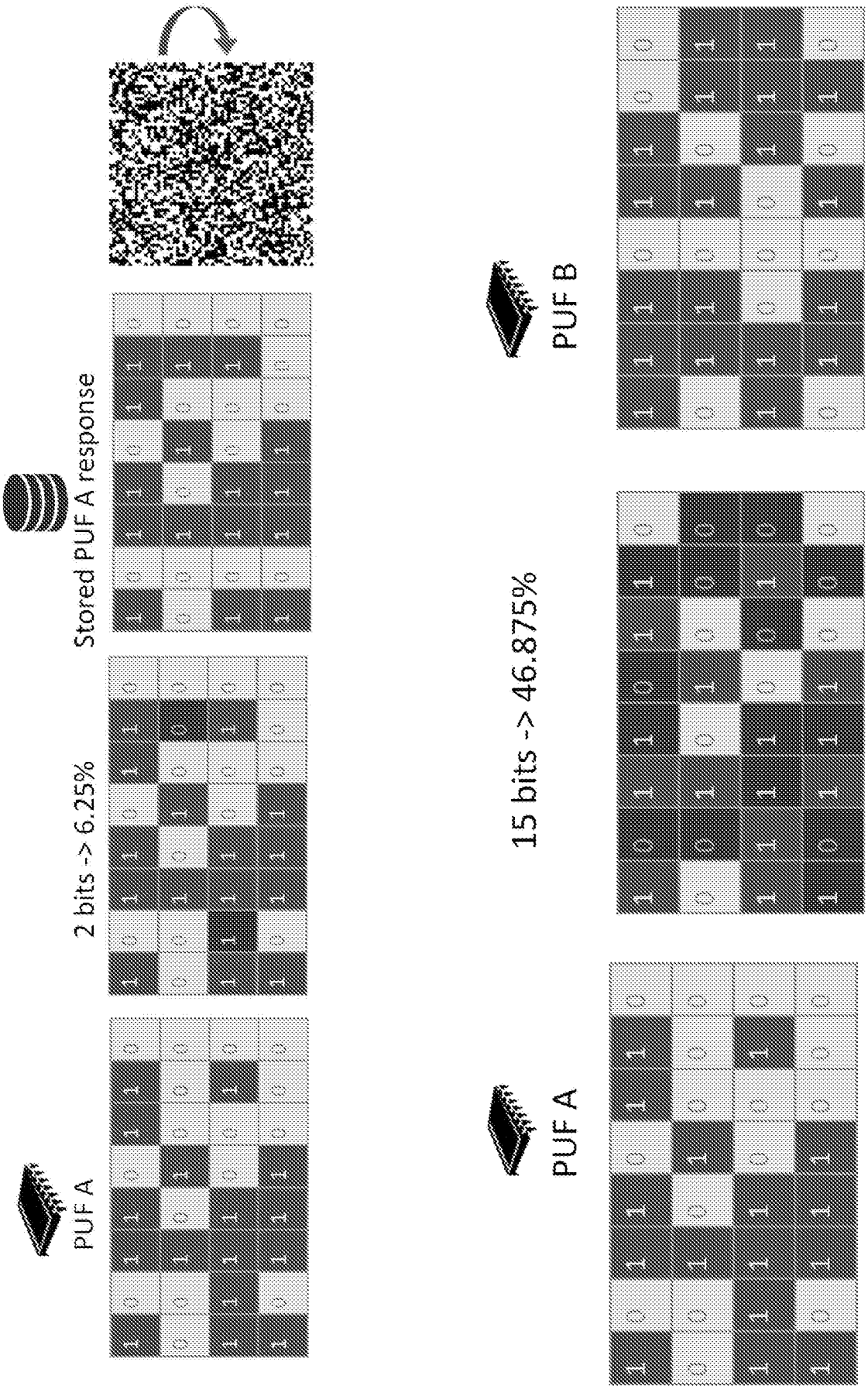

PUF A

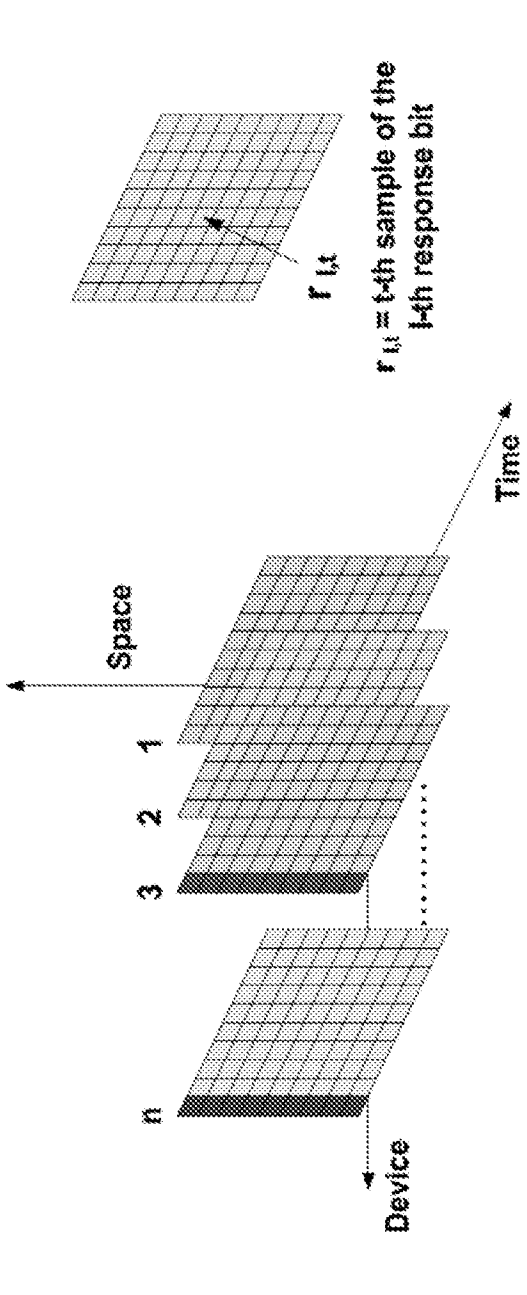

1 if top path is faster, else 0
D Filp-flop
K MUXs.
C[1] to C[k]
c-bit Challenge
Rising Edge

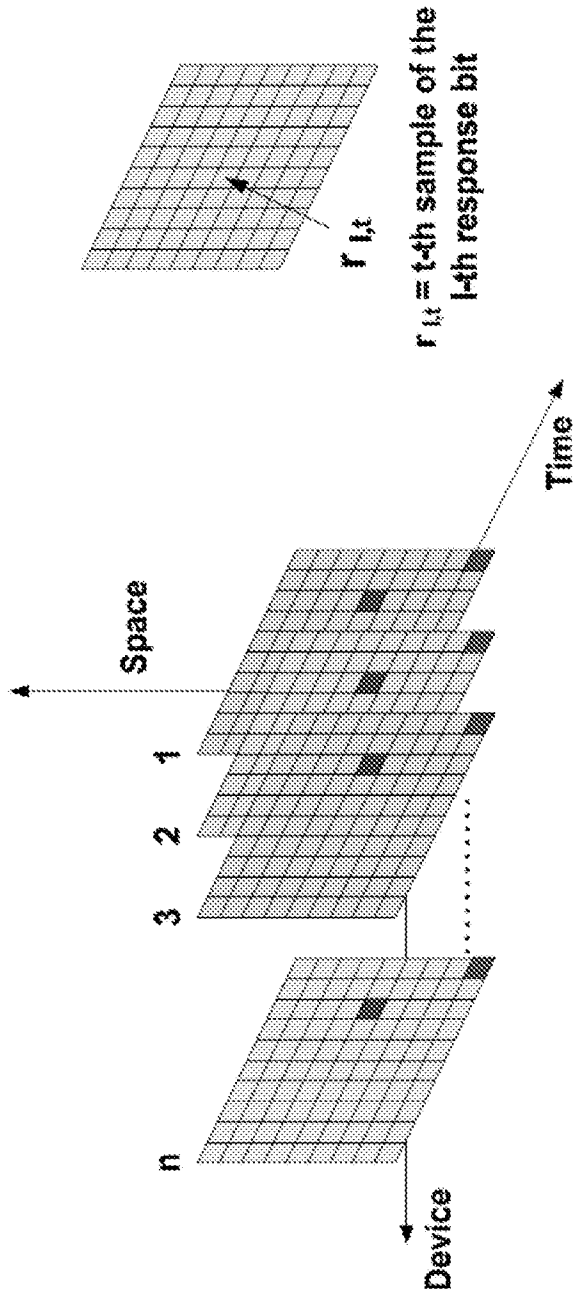


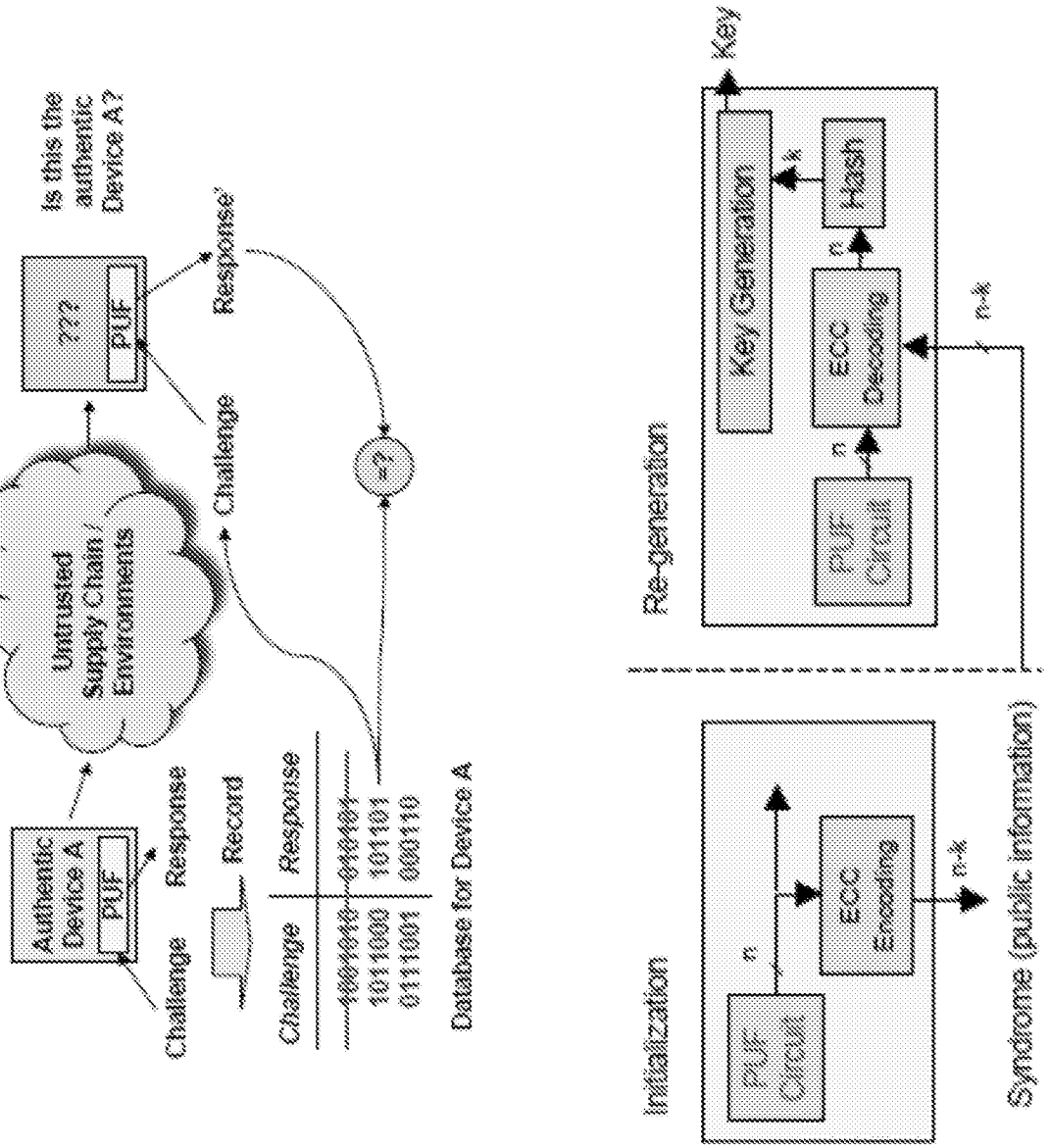

Capacitance Measuring Circuit


Pin
Tamper Device
Coupler
Transmitter
Detector
TDR Circuit


PUF A
2 bits -> 6.25%
Stored PUF A response
PUF A
15 bits -> 46.875%
PUF B


$r_{i,t}$ = t-th sample of the i-th response bit
$r_{i,t}$
Time
Space
1
2
3
n
Device


$r_{i,t}$ = t-th sample of the i-th response bit
$r_{i,t}$
Time
Space
1
2
3
n
Device


Authentic Device A
PUF
Challenge
Response
Untrusted Supply Chain / Environments
Is this the authentic Device A?
???
PUF
Challenge
Response'
Record
Challenge
Response
1011000
0111001
=?
Database for Device A
Initialization
PUF Circuit
n
ECC Encoding
n-k
Syndrome (public information)
Re-generation
PUF Circuit
n
ECC Decoding
n
Hash
n
k
Key Generation
k
Key
n-k

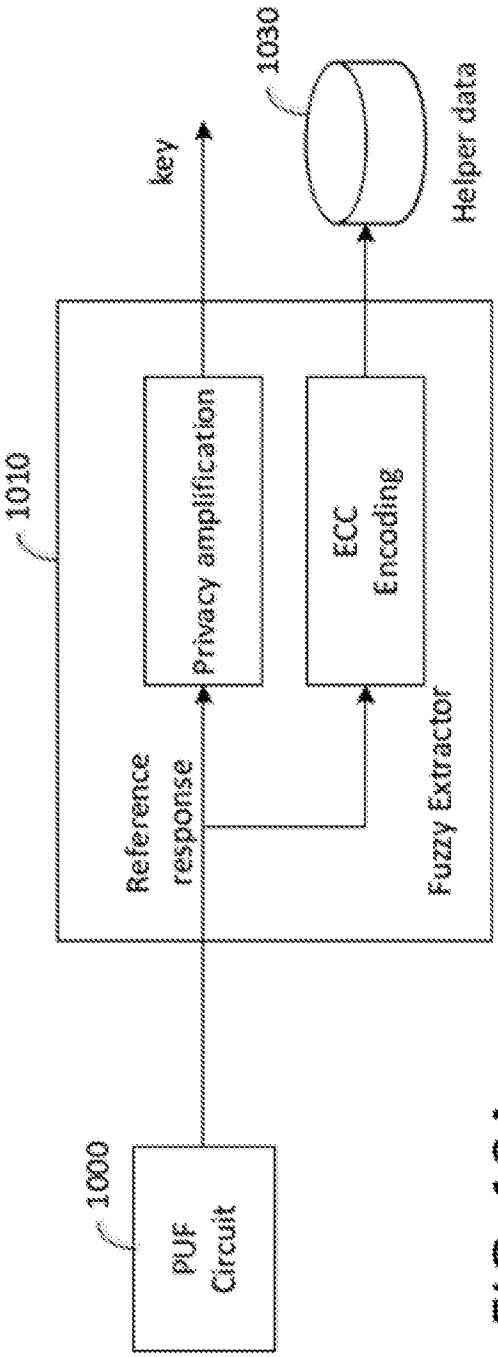


FIG. 10A

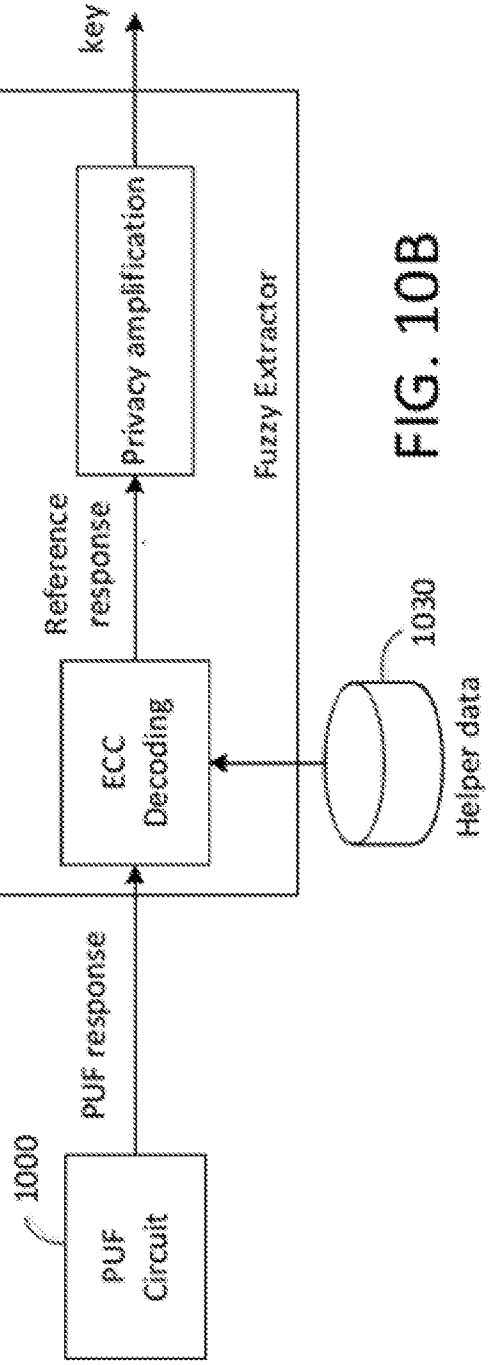
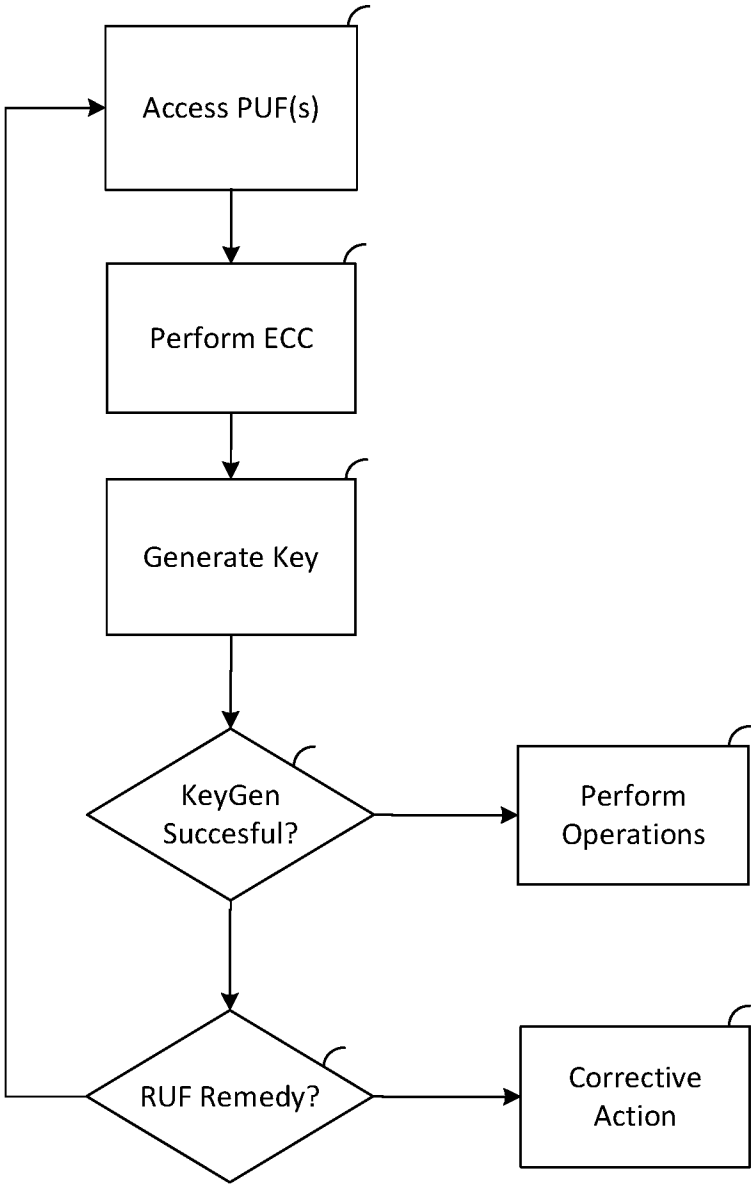
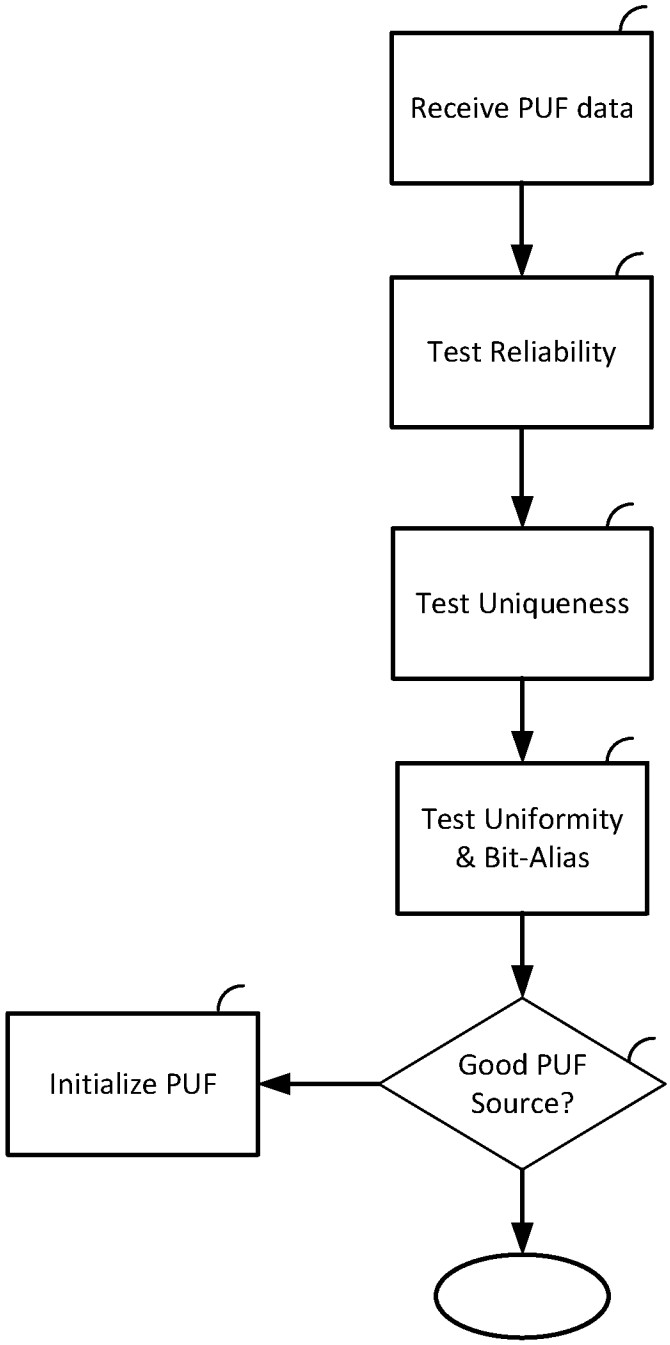
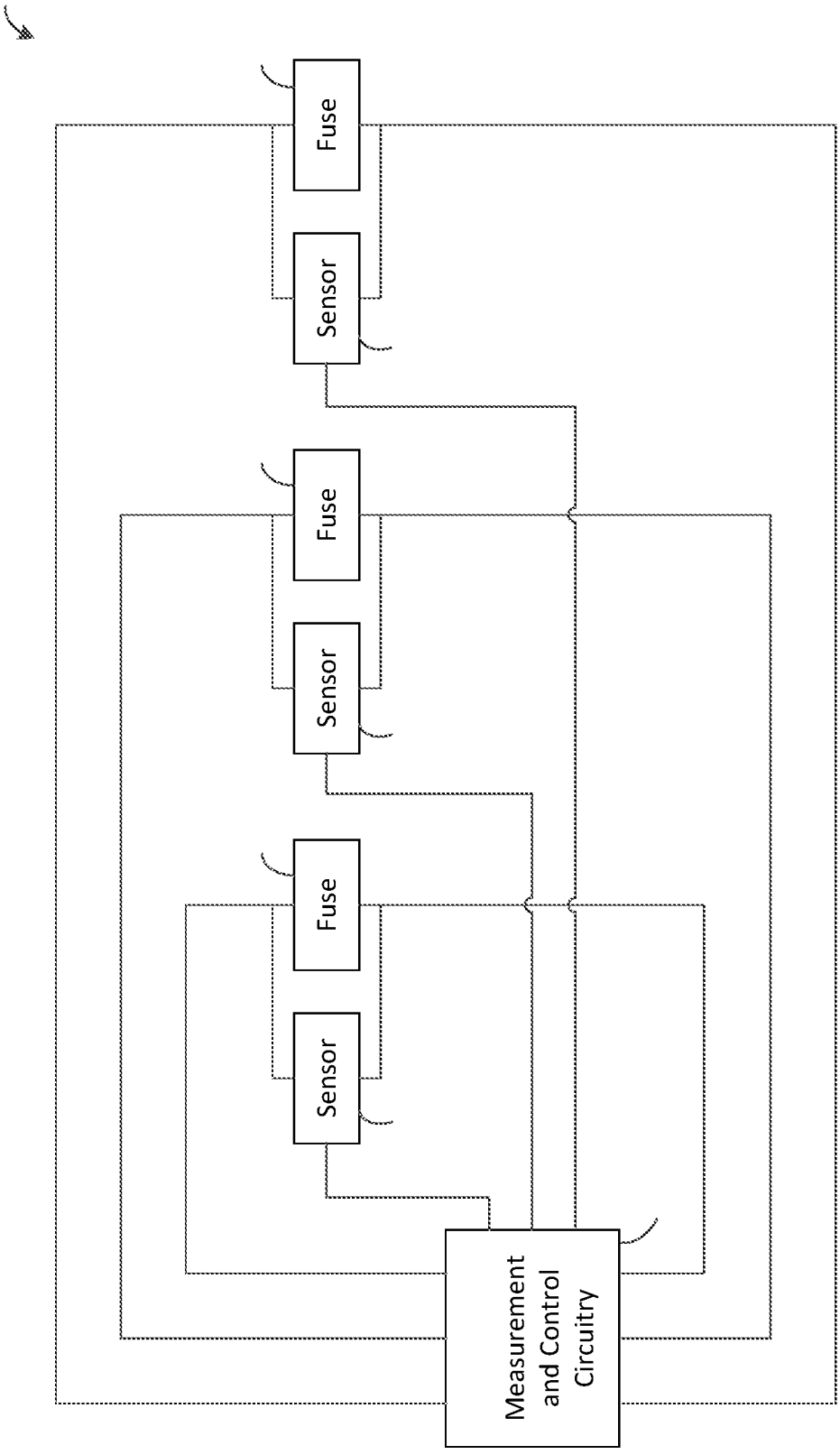
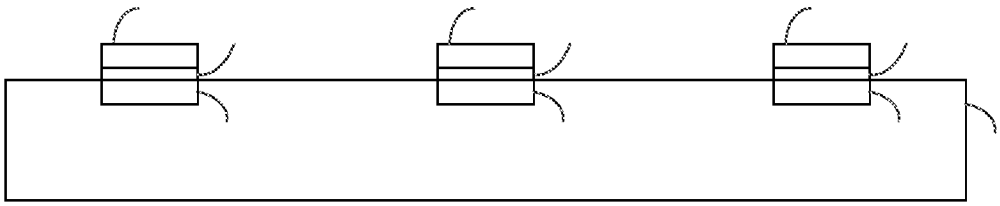


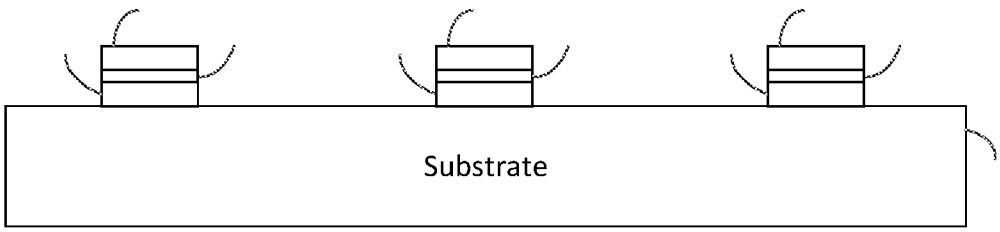
FIG. 10B

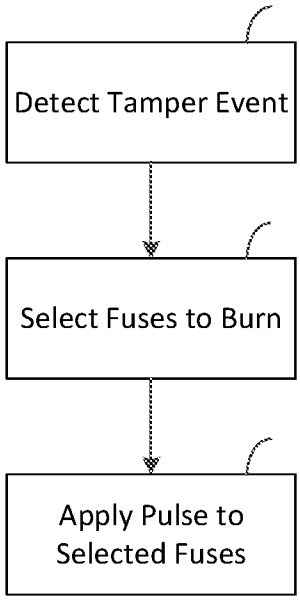

Access PUF(s)
Perform ECC
Generate Key
KeyGen Succesful?
Perform Operations
RUF Remedy?
Corrective Action

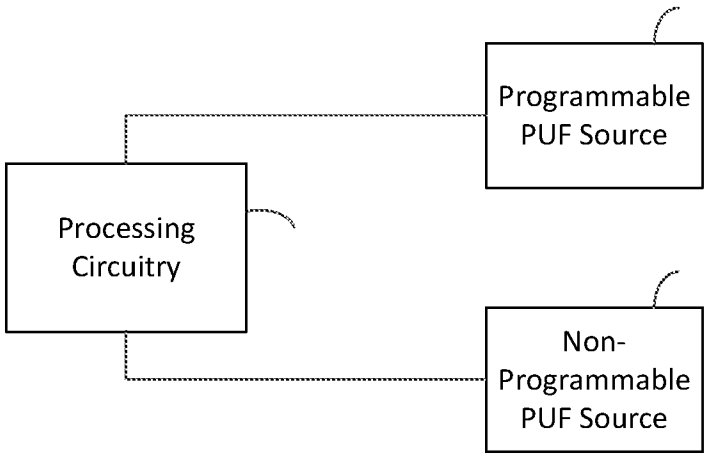

Receive PUF data
Test Reliability
Test Uniqueness
Test Uniformity & Bit-Alias
Good PUF Source?
Initialize PUF

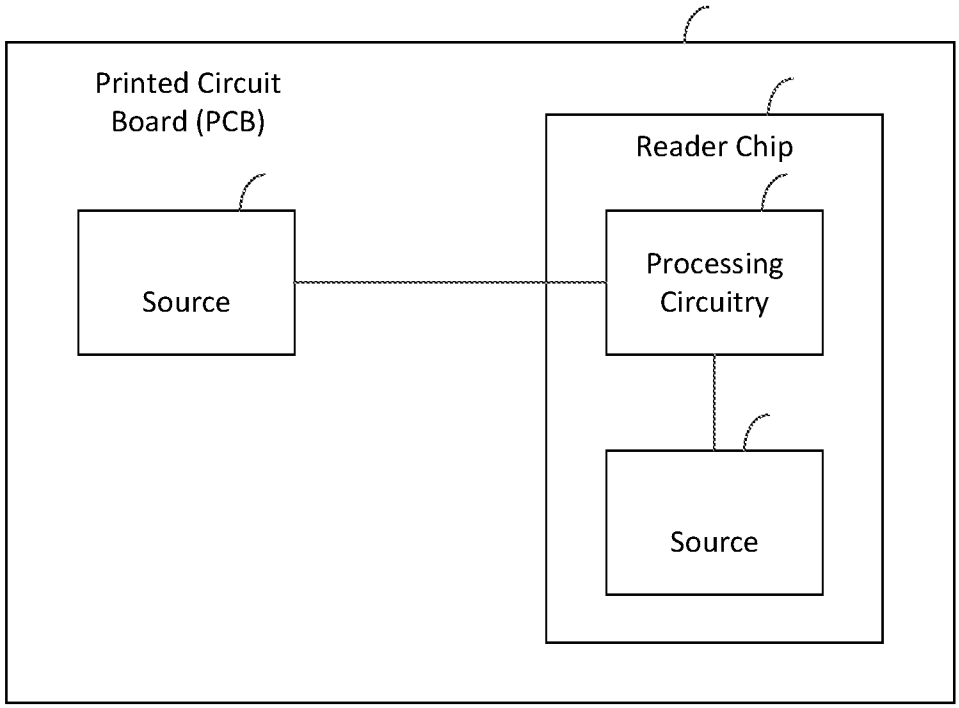

Fuse
Sensor
Fuse
Sensor
Fuse
Sensor
Measurement and Control Circuitry

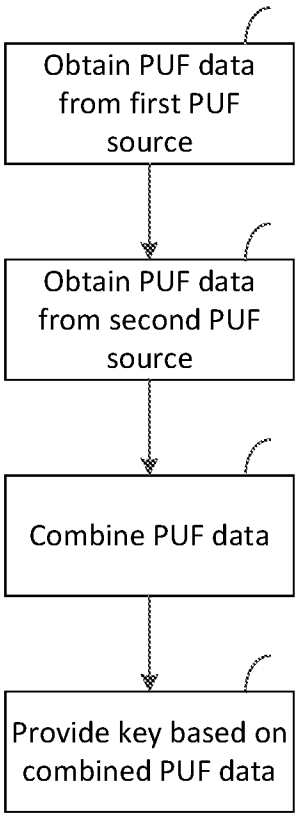


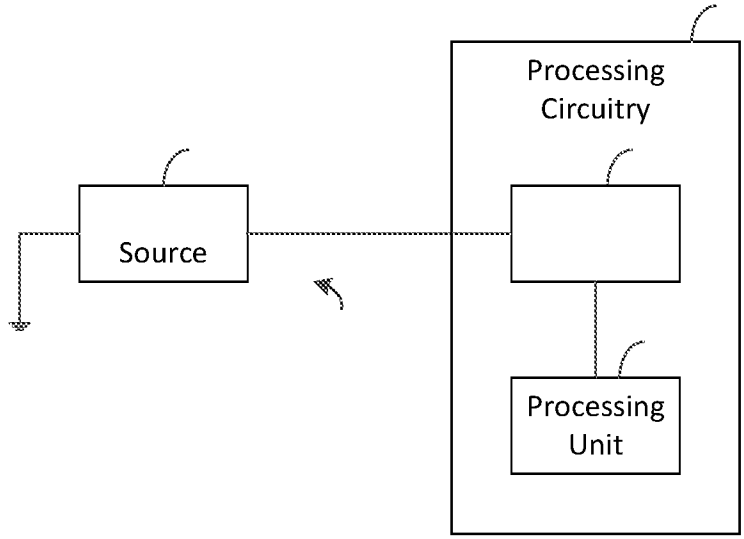

Substrate

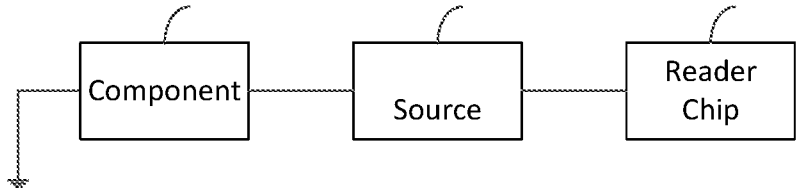

Detect Tamper Event
Select Fuses to Burn
Apply Pulse to Selected Fuses

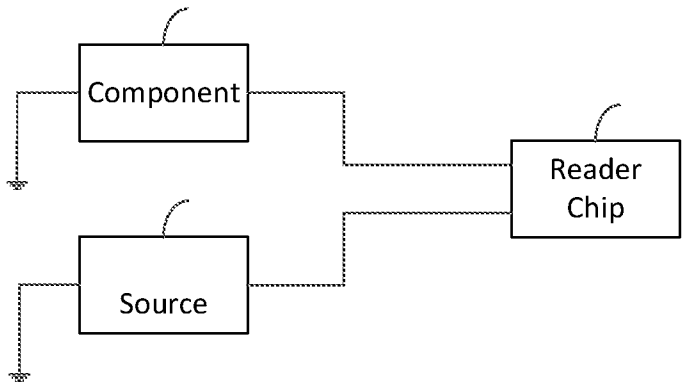

Programmable PUF Source
Processing Circuitry
Non-Programmable PUF Source

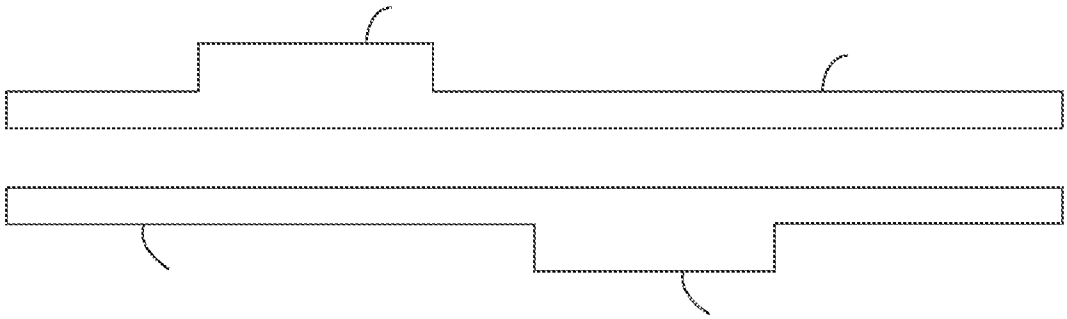

Printed Circuit Board (PCB)
Reader Chip
Source
Processing Circuitry
Source

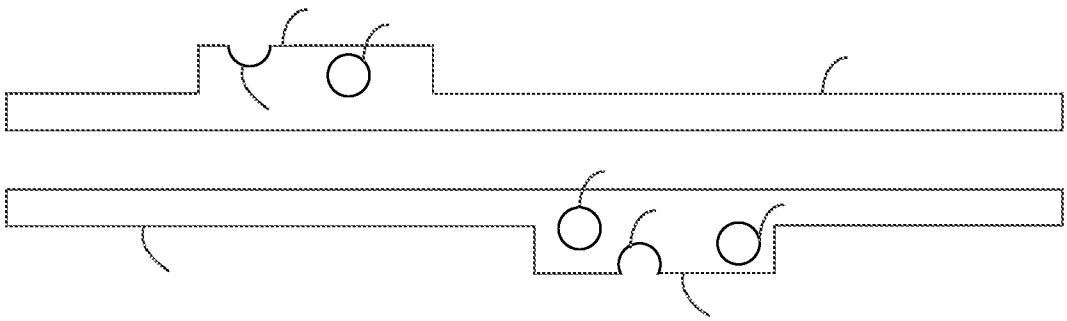

Obtain PUF data from first PUF source
Obtain PUF data from second PUF source
Combine PUF data
Provide key based on combined PUF data


Processing Circuitry
Source
Processing Unit


Component
Source
Reader Chip


Component
Source
Reader Chip





INTERNATIONAL SEARCH REPORT

International application No
PCT/US2018/042741

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

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

B. FIELDS SEARCHED

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

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2013/141137 A1 (KRUTZIK CHRISTIAN [US] ET AL) 6 June 2013 (2013-06-06) abstract paragraphs [0010] - [0019] paragraphs [0032] - [0080] -----	1-40, 42-48, 50-53
X	US 2016/182045 A1 (MAI KENNETH WEI-AN [US] ET AL) 23 June 2016 (2016-06-23) abstract paragraphs [0014] - [0025] -----	1-16, 22-53
X	US 2010/176920 A1 (KURSAWE KLAUS [NL] ET AL) 15 July 2010 (2010-07-15) abstract paragraphs [0007] - [0057] paragraphs [0068] - [0072] -----	1-16, 22-53

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

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

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

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

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

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

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

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

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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
6 September 2018	18/09/2018

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Di Felice, M

1

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2018/042741

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2016/080158 A1 (GEHRER STEFAN [DE]) 17 March 2016 (2016-03-17) abstract paragraphs [0012] - [0041] -----	1-16, 22-53
X	KR 101 566 949 B1 (KOREA ELECTRONICS TELECOMM [KR]) 13 November 2015 (2015-11-13) abstract paragraphs [0001] - [0023] -----	1-16, 22-53

1

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2018/042741

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2013141137 A1	06-06-2013	NONE	
US 2016182045 A1	23-06-2016	US 2016182045 A1	23-06-2016
		WO 2015027070 A1	26-02-2015
US 2010176920 A1	15-07-2010	EP 2174255 A1	14-04-2010
		ES 2632958 T3	18-09-2017
		US 2010176920 A1	15-07-2010
		WO 2008152577 A1	18-12-2008
US 2016080158 A1	17-03-2016	DE 102014218218 A1	17-03-2016
		US 2016080158 A1	17-03-2016
KR 101566949 B1	13-11-2015	NONE	