CONTACTLESS CARD WITH MULTIPLE ROTATING SECURITY KEYS

BACKGROUND

[0001] Contactless cards have become very popular recently because these cards have simplified in-store and online transactions. At the same time, because of the popularity of these cards, hackers actively try to forge contactless cards to conduct unauthorized transactions. As a result, there has been a renewed focus on enhancing the security of these cards.

SUMMARY

[0002] A communication can be encrypted such that an unauthorized recipient would not be able to determine the content of the communication. There are various techniques for encrypting a communication. When using symmetric cryptographic algorithms, such as encryption algorithms, hash-based message authentication code (HMAC) algorithms, and cipher-based message authentication code (CMAC) algorithms, it is important that the key remains secret between the party that originally processes the data that is protected using a symmetric algorithm and the key, and the party who receives and processes the data using the same cryptographic algorithm and the same key.

[0003] A brute-force attack can consist of systematically checking all possible keys until the correct one is found. Hackers oftentimes use brute-force attacks to steal a key stored on a contactless card. As such, it is important that the same key is not used too many times. If a key is used or reused too frequently, that key may be compromised. Each time the key is used, it provides an attacker an additional sample of data which was processed by the cryptographic algorithm using the same key. The more data an attacker has which was processed with the same key, the greater the likelihood that the attacker may discover the value of the key. A key used frequently may be comprised in a variety of different attacks.

[0004] Moreover, each time a symmetric cryptographic algorithm is executed, it may reveal information, such as side-channel data, about the key used during the symmetric cryptographic operation. Side-channel data may include minute power fluctuations which occur as the cryptographic algorithm executes while using the key. Sufficient measurements may be taken of the side-channel data to reveal enough information about the key to allow it to be recovered by the attacker. Using the same key for exchanging data would repeatedly reveal data processed by the same key.

[0005] However, by limiting the number of times a particular key is used, the amount of side-channel data which the attacker is able to gather is limited and thereby exposure to this type of attack is reduced. Therefore, it is an object of this disclosure to implement a cryptographic system which enhances the security of a contactless card against such attacks by implementing multiple security keys. In one example embodiment, a contactless card can include a plurality of keys for a specific operation, e.g., encrypting or signing a communication. The contactless card can also include an applet which uses a key selection module. The key selection module can select one of the plurality of keys and the applet can use the key to, e.g., encrypt or sign a communication using an encryption or signature algorithm. The contactless card can send the encrypted or signed communication to a host computer through a terminal or a client device. The host computer can repeat or replicate the key selection technique of the contactless device to select the same key and thereby decrypt or verify the communication. For example, the host computer can use the same key selection module or algorithm as the contactless card. Thus, the key selection module of the host computer can select the same key as the key selected by the contactless card. Using the same key, the host computer can decrypt or verify the authenticity of the communication.

[0006] In one example embodiment, the key selection module can receive an input and

select the key based on the input. The input can be provided by the contactless card or by an external device, e.g., a terminal or host computer. The key selection module can execute a mathematical algorithm or function which assigns the input to one of the keys stored on the contactless card.

[0007] In one example embodiment, a contactless card can store a plurality of encryption algorithms. Also, the contactless card can include an encryption algorithm selection module. For each encryption operation, the encryption algorithm selection module, when executed, can select one of the plurality of encryption algorithms. Using the selected encryption algorithm and a selected key, the contactless card can encrypt a communication and transmit the encrypted communication to a terminal.

[0008] Further features of the disclosed design, and the advantages offered thereby, are explained in greater detail hereinafter with reference to specific example embodiments described below and illustrated in the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] FIG. 1 illustrates a contactless card according to an example embodiment.

[00010] FIG. 2 illustrates a terminal or client device according to an example embodiment.

[00011] FIG. 3 illustrates exemplary hardware components for a server or host computer.

[00012] FIG. 4 shows an example flowchart for transmission of information from a contactless card to a host computer.

DETAILED DESCRIPTION

[00013] The following description of embodiments provides non-limiting representative examples referencing numerals to particularly describe features and teachings of different aspects of the invention. The embodiments described should be recognized as capable of

implementation separately, or in combination, with other embodiments from the description of the embodiments. A person of ordinary skill in the art reviewing the description of embodiments should be able to learn and understand the different described aspects of the invention. The description of embodiments should facilitate understanding of the invention to such an extent that other implementations, not specifically covered but within the knowledge of a person of skill in the art having read the description of embodiments, would be understood to be consistent with an application of the invention.

[00014] A contactless card can include processing circuitry for storing and processing information. The processing circuitry can include processors, memories, error and parity/CRC checkers, data encoders, anticollision algorithms, controllers, command decoders, security primitives and tamperproofing hardware.

[00015] The size of a contactless card can be the same as the size of a payment card, credit card or a debit card. According to ID-1 of the ISO/IEC 7810 standard, the dimensions of a contactless card can be 85.60 by 53.98 millimeters (3.37 in × 2.13 in). However, a contactless card according to these disclosures can have a different size, and it is not necessary for a contactless card to be implemented in a payment card.

[00016] The storage of information can take place in a memory of the processing circuitry, which can be a read-only memory, write-once read-multiple memory or read/write memory, e.g., RAM, ROM and EEPROM. A contactless card can include one or more of these memories. A read-only memory can be factory programmable as read-only or one-time programmable. One-time programmability provides the opportunity to write once then read many times. A write once/read-multiple memory can be programmed at a point in time after the memory chip has left the factory. Once the memory is programmed, it cannot be rewritten, but it can be read many times. A read/write memory can be programmed and re-programed many times after leaving the factory. It can also be

read many times.

[00017] The memory of a contactless card can be divided into several zones, each provided with a different level of security. The contactless card processor can keep track of which memory addresses belong to which zones and the circumstances under which each zone can be accessed. A contactless card processor can also process information and store the information onto the memory. In an example embodiment, a contactless card memory can be divided into four zones: a secret zone, a confidential zone, a usage zone, and a public zone.

[00018] A secret zone can be used for storage of information which can be used only by the processor itself, e.g., passwords, cryptographic keys. The information stored in this zone is not readable outside of the contactless card. In an embodiment, the secret zone can be implemented with a separate processor that is capable of performing cryptographic functions. Cryptographic keys can be passed in to the secret zone or can be generated in the secret zone, and in either case the keys can be stored in the secret zone and used to support cryptographic services. If necessary, cryptographic keys can be exported from the secret zone.

[00019] In an example embodiment, the contactless card can be a JavaCard which can include one or more applets. The applets can be firewalled, and data can be allocated to the applet for storage. The data can be stored transactionally in an EEPROM flash memory, e.g., if the write isn't complete when the power is removed, the contents remain the same as before.

[00020] A confidential zone can be used to store a list of all transactions made with the card. The confidential zone can have password protection. In an example embodiment, the password is known only to the card issuer, who can examine the history of the card for evidence of misuse of the system. The confidential zone can have a read-only access

restriction so that the information stored in this zone could not be modified, e.g., transaction list could not be modified.

[00021] A usage zone could be used for storage of information which can be periodically updated or modified. Depending on the sensitivity of the data, a password can be implemented for this zone. The usage zone can have both read and write access protected by a password.

[00022] A public zone can be used for keeping nonsensitive information, such as the card issuer's name and address. The public zone can have read-only access, without a password.

[00023] In one example embodiment, the memory of the contactless card can store a plurality of keys. These keys can be used for various operations, e.g., encryption or signing. Additionally, the contactless card can store a plurality of encryption algorithms. The memory can also store a key selection module and an encryption selection module. Using the key selection module, an applet of the contactless card can select a key for an operation of the contactless card, e.g., encryption. Using the encryption algorithm selection module, the contactless card can select an encryption algorithm to encrypt a communication.

[00024] A contactless card can wirelessly communicate with a terminal. For example, a contactless card can be a credit card including a magnetic tape or a radio-frequency identification ("RFID") tag. Some contactless cards can include both the magnetic tape and the RFID tag.

[00025] A terminal can communicate with a contactless card if the contactless card is held in proximity to the terminal. The terminal can read the contactless card over a short distance using near-field communication ("NFC") technology, which uses radio frequency induction. A contactless card can include an inductor to capture some of the incident radio-frequency interrogation signals transmitted by the terminal, rectify it, and use it to power the card's processing circuitry. As such, contactless cards can function without an internal

power source. However, in some embodiments, contactless cards can include an internal power source.

[00026] The contactless card can be EMV-compliant. Europay, MasterCard and Visa ("EMV") is a payment method based upon a technical standard for smart payment cards. EMV cards can store their data on integrated circuits in addition to magnetic stripes.

[00027] The standard for contact cards can be based on ISO/IEC 7816, and the standard for contactless card can be based on ISO/IEC 14443.

[00028] FIG. 1 illustrates a contactless card 100 according to an example embodiment. In this embodiment, the contactless card 100 can be a payment card issued by a service provider 101, the name of which can be displayed on the front or back of the contactless card 100. The size of the contactless card 100 can be compliant with ID-1 of the ISO/IEC 7810 standard, *i.e.*, 85.60 by 53.98 millimeters. The contactless card 100 can include a contact pad 102 for establishing contact with a contact terminal. The contactless card 100 can also include processing circuitry, antenna and other components not displayed in FIG. 1 (e.g., one or more microprocessors and one or more memories). These components can be located behind the contact pad 102, however, it is understood that these components can also be located elsewhere within the contactless card 100 and do not need to be located behind the contactless card 100. The contactless card 100 can also include various identification information 103 displayed on front or back of the card. The contactless card 100 can also include a magnetic strip or tape, which can be located on the back of the card.

[00029] In one example embodiment, the contactless card 100 can include a power source and a timer. The timer can be powered by the power source. The processor of the contactless card can receive a time signal from the timer, e.g., when processing transactions or encrypting messages. The processor can encrypt a message, select a key or select an encryption algorithm based on the time signal. In one example embodiment, the contactless

card can receive a time signal from a terminal, client device or a host computer. In this embodiment, the contactless card can encrypt a message or select a key based on the time signal received.

[00030] In another example, an applet of the contactless card 100 can include a counter module. The counter module can maintain a count number which can count the number of occurrences of an event. For example, the module can count the number of times the contactless card interacts with a terminal, client device or host computer. Each time the contactless card is scanned at a terminal, the processor of the contactless card can send a signal to the counter module to increment the count number.

[00031] In an example embodiment, the contactless card is provided with a radio-frequency identification ("RFID") tag. In some embodiments, the RFID tag can include processing circuitry for storing and processing information that modulates and demodulates a radio-frequency signal (usually received from a terminal, reader/writer or scanner). An RFID tag can also include an antenna for receiving and transmitting the signal. Additionally, an RFID tag can include a power source or means for collecting DC power from the incident terminal signal. These means can include modulators, voltage regulators, resets, and connections to an antenna. The antenna can be an electric dipole antenna or a coil antenna.

[00032] In an example embodiment, the coil of a contactless card can act as the secondary of an air core transformer. The terminal can communicate with the contactless card by cutting power or amplitude modulation. The contactless card can infer the data transmitted from the terminal using the gaps in the contactless card's power connection, which is functionally maintained through capacitors. The contactless card can communicate back by switching a load on the contactless card's coil or load modulation. Load modulation can be detected in the terminal's coil through interference.

[00033] A terminal can read information from a contactless card and write information onto the contactless card. In some embodiments, the terminal can pass information from the contactless card to a host computer (or server) and write information from the host computer into the contactless card. In some embodiments, the host computer can be the terminal. The terminal can provide power to the contactless card and communicatively connect the card's hardware interface to the host computer. Since the contactless card's processor can control the actual flow of information into and out of the card's memories, the terminal can operate with only minimal processing capabilities for sending the information to the host computer. In one embedment, the terminal can be a payment terminal. In other embodiments, the terminal can be a client device such as a cellphone, smart phone, laptop, desktop, wearable device, etc.

[00034] In some embodiments, the terminal can include a processor and a transceiver. The processor of the terminal can decode any data received from the contactless card. The terminal can also update, delete or modify the information stored on the contactless card.

[00035] A terminal can write data on the contactless card by passing the data to the processor of the contactless card. The processor can process the data and store it in the contactless card's memory. A terminal can have a two-way communication with a contactless card as described in ISO 14443. The contactless card can include an RFID tag. The two-way communication can be digitally encoded. There can be several frequency ranges, and several proprietary formats for the two-way communication (e.g., HID in the 125Mhz range). The 13.56Mhz frequency range (NFC) is dominated by ISO 14443 compatible cards.

[00036] A terminal and a contactless card can exchange messages, which can include commands or data. For example, a terminal can send a command message to the contactless card, the contactless card can process the command message in its processor and the

contactless card can send back a response message to the terminal. Each of the command message and the response message can include data. A message can include TLV (Type, Length and Value) data and a command such as STORE_DATA command which prompts storage of the data included in the message in the contactless card.

[00037] FIG. 2 illustrates a terminal 200 according to an example embodiment. In this example embodiment, the terminal 200 can include a display screen 201. This display screen can be any type of display screen, e.g., an LCD display screen. The terminal 200 can also include a keypad 202. Using the keypad 202, a customer can enter information into the terminal 200. The terminal 200 can also include an opening 203 for inserting a chip card into the terminal 200. Using the opening 203, a customer can insert a chip card into the terminal 200 so that the pins of the terminal 200 can electrically connect with the contact pad of the chip card. In some embodiments, the terminal 200 can include a magnetic card opening 204. Using the magnetic card opening 204, the customer can swipe the contactless card at the terminal 200 and the terminal 200 can obtain any information stored on the magnetic tape of the contactless card.

[00038] In an example embodiment, the terminal 200 can be a contactless RFID terminal, which can include antennas for sending and receiving signals, a transceiver, and a processor to decode data. In a passive system, the terminal can transmit an energy field that can wake up the tag and power its chip, thereby enabling it to transmit or store data. In turn, the tag converts the radio signal into usable power, and responds to the terminal in the form of a radio signal. The signal can include the tag's identity and other information. Once the terminal receives the response, the terminal converts the response and extracts any information included in the radio signal. The information collected from the tag is then transferred through a communications interface to a host computer system, where the data can be stored in a database or analyzed by the computer system. The terminal can also

update, delete or modify the information stored on the contactless card.

[00039] In the example embodiment of FIG. 2, the terminal 200 is provided with one or more antennas (not displayed), which enable the device to read information from a contactless card and write information on the contactless card. The terminal 200 can include an indicator 205, which shows that the device can be contactless.

[00040] In this disclosure, the terms reader/writer, scanner, terminal and client device have been used interchangeably, and they all refer to a device which can scan a contactless card and/or write information on the contactless card.

[00041] In some embodiments, the terminal can be communicatively connected to a host computer, backend server or server. In other embodiments, the terminal can be integrated in the host computer (or server). The host computer can receive encrypted or signed communication from the contactless card (e.g., through a terminal) and can decrypt the communication or verify the communication's authenticity.

[00042] FIG. 3 illustrates exemplary hardware components of a host computer or backend server. A computer system 300, or other computer systems similarly configured, may include and execute one or more subsystem components to perform functions described herein, including the steps of various flow processes described above. Likewise, a mobile device, a cell phone, a smartphone, a laptop, a desktop, a notebook, a tablet, a wearable device, a server, etc., which includes some of the same components of the computer system 300, may run an application (or software) and perform the steps and functionalities described above. Computer system 300 may connect to a network 314, *e.g.*, Internet, or other network, to receive inquiries, obtain data, and transmit information and incentives as described above.

[00043] The computer system 300 typically includes a memory 302, a secondary storage device 304, and a processor 306. The computer system 300 may also include a plurality of

processors 306 and be configured as a plurality of, *e.g.*, bladed servers, or other known server configurations. The computer system 300 may also include a network connection device 308, a display device 310, and an input device 312.

[00044] The memory 302 may include RAM or similar types of memory, and it may store one or more applications for execution by processor 306. Secondary storage device 304 may include a hard disk drive, floppy disk drive, CD-ROM drive, or other types of non-volatile data storage. Processor 306 executes the application(s), such as those described herein, which are stored in memory 302 or secondary storage 304, or received from the Internet or other network 314. The processing by processor 306 may be implemented in software, such as software modules, for execution by computers or other machines. These applications preferably include instructions executable to perform the system and subsystem component functions and methods described above and illustrated in the FIGS. herein. The applications preferably provide graphical user interfaces (GUIs) through which users may view and interact with subsystem components.

[00045] The computer system 300 may store one or more database structures in the secondary storage 304, for example, for storing and maintaining the information necessary to perform the above-described functions. Alternatively, such information may be in storage devices separate from these components.

[00046] Also, as noted, processor 306 may execute one or more software applications to provide the functions described in this specification, specifically to execute and perform the steps and functions in the process flows described above. Such processes may be implemented in software, such as software modules, for execution by computers or other machines. The GUIs may be formatted, for example, as web pages in HyperText Markup Language (HTML), Extensible Markup Language (XML) or in any other suitable form for presentation on a display device depending upon applications used by users to interact with

the computer system 300.

[00047] The input device 312 may include any device for entering information into the computer system 300, such as a touch-screen, keyboard, mouse, cursor-control device, microphone, digital camera, video recorder or camcorder. The input and output device 312 may be used to enter information into GUIs during performance of the methods described above. The display device 310 may include any type of device for presenting visual information such as, for example, a computer monitor or flat-screen display (or mobile device screen). The display device 310 may display the GUIs and/or output from sub-system components (or software).

[00048] Examples of the computer system 300 include dedicated server computers, such as bladed servers, personal computers, laptop computers, notebook computers, palm top computers, network computers, mobile devices, or any processor-controlled device capable of executing a web browser or other type of application for interacting with the system.

[00049] Although only one computer system 300 is shown in detail, system 300 may use multiple computer systems or servers as necessary or desired to support the users and may also use back-up or redundant servers to prevent network downtime in the event of a failure of a particular server. In addition, although computer system 300 is depicted with various components, one skilled in the art will appreciate that the system can contain additional or different components. In addition, although aspects of an implementation consistent with the above are described as being stored in a memory, one skilled in the art will appreciate that these aspects can also be stored on or read from other types of computer program products or computer-readable media, such as secondary storage devices, including hard disks, floppy disks, or CD-ROM; or other forms of RAM or ROM. The computer-readable media may include instructions for controlling the computer system 300, to perform a particular method, such as methods described above.

[00050] In an example embodiment, a contactless card can communicate (i.e., transmit or receive) data from the host computer, e.g., through the terminal or client device. The contactless card can communicate with the terminal, e.g., using at least one of NFC, Bluetooth, RFID, Wi-Fi, and/or the like technologies. The terminal can act as an intermediary between the contactless card and the host computer, e.g., the terminal can forward a communication received from the contactless card to the host computer and vice versa. The terminal can communicate with the host computer using a network. For example, the network can include one or more of a fiber optics network, a passive optical network, a cable network, an Internet network, a satellite network, a wireless LAN, a Global System for Mobile Communication, a Personal Communication Service, a Personal Area Network, Wireless Application Protocol, Multimedia Messaging Service, Enhanced Messaging Service, Short Message Service, Time Division Multiplexing based systems, Code Division Multiple Access based systems, D-AMPS, Wi-Fi, Fixed Wireless Data, IEEE 802.11b, 802.15.1, 802.11n and 802.11g, Bluetooth, NFC, RFID, Wi-Fi, and/or the like.

[00051] In some embodiments, a communication between the contactless card and the terminal can be encrypted, e.g., the communication can be encoded in such a way that only authorized parties or devices (e.g., the contactless card or the host computer) can decode or decrypt the communication. For example, the communication can be encrypted using a symmetric-key or a public-key scheme. For each one of these encryption schemes, there can be at least one key and an encryption algorithm stored on the contactless card. Similarly, an associated key and an associated encryption (decryption) algorithm can be stored on the host computer. The contactless card can encrypt a communication using the key and the encryption algorithm. The contactless card can transmit the communication to the host computer, e.g., through a client device such as a cell phone. The host computer

can decrypt the communication using the associated key and associated encryption algorithm.

[00052] In an example embodiment, the encryption scheme is the symmetric-key scheme. In this example, the contactless card can store a symmetric key and an encryption algorithm. Example encryption algorithms can include Twofish, Serpent, AES (Rijndael), Blowfish, CAST5, Kuznyechik, RC4, DES, 3DES, Skipjack, Safer+/++ (Bluetooth), and IDEA. The host computer can also store a copy of the symmetric key and the encryption (or decryption) algorithm. In response to a message from the terminal, the processor of the contactless card can encrypt a communication using the symmetric key and the encryption algorithm to create a cryptogram. The contactless card can transmit the cryptogram to the terminal using a transceiver of the contactless card. The terminal can in turn transmit the cryptogram to the host computer. The host computer can decrypt the cryptogram using the symmetric key and the encryption (or decryption) algorithm.

[00053] In an example embodiment, the encryption scheme is the public-key scheme. In this example, the contactless card can store a public (or private) key and an encryption algorithm. Examples of public-key encryption algorithms include Diffie–Hellman key exchange protocol, DSS, ElGamal, Paillier cryptosystem, RSA, Cramer–Shoup cryptosystem and YAK authenticated key agreement protocol. The host computer can store a private (or public) key and the encryption (or decryption) algorithm. In response to a message from the terminal, the processor of the contactless card can encrypt a communication using the public (or private) key and the encryption algorithm to create a cryptogram. The contactless card can transmit the cryptogram to the terminal using a transceiver of the contactless card. The terminal can in turn transmit the cryptogram to the host computer. The host computer can decrypt the cryptogram using the private (or public) key and the encryption (or decryption) algorithm.

[00054] In an example embodiment, a communication between the contactless card and the host computer can include a message authentication code (MAC), a hashed message authentication code (HMAC) or a digital signature. The MAC, HMAC or digital signature can be a mathematical code or scheme which can establish authenticity of the information included in the communication. For example, when a contactless card is scanned at a terminal, the contactless card can transmit a communication to the host computer to seek authorization of a transaction. The communication can include various data, such as an account number, a name, a card security value, an expiration date and a MAC (or HMAC or digital signature). Using the MAC (or HMAC or digital signature) included in the communication, the host computer can establishes that the content of the communication is authentic (i.e., not altered). Specifically, the host computer can recreate the MAC (or HMAC or digital signature), and if the value of the MAC (or HMAC or digital signature) is the same as the MAC (or HMAC or digital signature) included in the communication, the host computer can ensure that the content of the communication is not altered. Also, the digital signature prevents (the owner of) the contactless card from denying that it transmitted the information because only the contactless card could create the MAC (or HMAC or digital signature) included with the message.

[00055] A MAC can include the following algorithms. In the first step, a key generation algorithm can generate a key. In the second step, a signing algorithm can return a tag created using the generated key and a message. In the third step, a verifying algorithm verifies the authenticity of the message given the key and the tag.

[00056] A digital signature scheme can include the following algorithms. In the first step, a key generation algorithm generates a private key and a corresponding public key. In the second step, a signing algorithm generates a digital signature using a message and a private key. In the third step, a signature verifying algorithm can verify the message using the

digital signature and the public key. A MAC differs from a digital signature in that a MAC scheme uses only one key but a digital signature scheme uses two keys, i.e., a public key and a private key.

[00057] In an example digital signature scheme, the authenticity of the digital signature generated from the fixed message and fixed private key can be verified by using the corresponding public key. Moreover, these algorithms are selected such that it is computationally infeasible to generate a valid signature for a party without knowing that party's private key. This digital signature scheme can ensure authenticity of the content of a communication because if the content is digitally signed, any change in the content after signature invalidates the signature. In other words, it is practically impossible to modify the content and its signature to produce new content with a valid signature.

[00058] In an example embodiment, a contactless card can be provided with a private key and a signing algorithm. The host computer can be provided with a public key and a verifying algorithm. When a contactless card is scanned at a terminal, the contactless card can transmit a communication including a digital signature to the terminal, and the terminal can forward this communication to the host computer. The digital signature can be generated using the signing algorithm and the private key of the contactless card. The digital signature can include data such as an account number, an expiration date and a code verification value. When the host computer receives the communication, the host computer can verify the authenticity of the information included in the communication using the public key, the verifying algorithm and information included in the communication. For example, the host computer can regenerate the digital signature using the information included in the communication. If the regenerated digital signature matches the digital signature included in the communication, the host computer can verify the authenticity of the information. Otherwise, the host computer can conclude that the content of the

communication is forged.

[00059] A digital signature scheme can have several advantages. For example, a hacker would be motivated to forge the content of a communication to seek authorization of a sham transaction. A digital signature can prevent this by authenticating the information included in the communication. So long as the private key associated with the contactless card is secret, the digital signature can authenticate and verify the communication.

[00060] In some example embodiments, before the content is converted into a MAC or digital signature using a signing algorithm, the message or content can be hashed. A hash function is a mathematical algorithm that maps a message of arbitrary size to a bit string of a fixed size (i.e., a hash). A hash function can be a one-way function, i.e., it is infeasible to invert the function. In an example embodiment, the MAC is built from a hash function, and thus, the product is a HMAC. In another example embodiment, the digital signature is built from a hash function.

[00061] There are several reasons to make a MAC or digital signature form hashed content as opposed to the content itself. For example, because a hash has a fixed size, the hash of the content can be shorter than the actual content, and thus, the MAC or the digital signature of the hash can be much shorter than the MAC or the digital signature of the actual content. Moreover, because it is faster to hash the content than to convert it into MAC or digital signature, it is faster to convert the hash of the content into a MAC or digital signature. In an example embodiment, the content of the contactless card is written using a HMAC.

[00062] In an example embodiment, a contactless card can include a plurality of security keys (or "keys"). For example, a contactless card can include five keys for a first operation, e.g., encryption. As another example, the contactless card can include six keys for a second operation, e.g., signing a digital signature. When the contactless card is manufactured, the

manufacturer can store these keys on the contactless card. For each key stored on the contactless card, the manufacturer can also store an associated key on the host computer. In the symmetric-key scheme, each associated key can be the same as one of the keys stored on the contactless card. In the public-key scheme, a private (or public) key can be associated with one of the public (or private) keys stored on the contactless card. In one example, the card manufacturer can generate the key pairs. In another example, the key pairs can be generated by the contactless card or the host computer.

[00063] An applet of the contactless card can include a key selection module, which can select the key to be used for an operation. For example, each time the contactless card encrypts (or signs) a communication, the key selection module selects one of the keys for the encryption (or signing) operation. The key selection module can use a variety of techniques for selecting the key.

[00064] For example, the key selection module can choose the keys sequentially. In this example, for each operation requiring a key, an order can be assigned to the keys stored on the contactless card for that operation. The key selection module can select the keys in the assigned order. Once every key is used to perform the operation (e.g., encrypt or sign a communication), the key selection module can select the keys in the same order again. The order or sequence of the keys can be known to the host computer. For example, the manufacturer of the card assigned the order of the keys when the manufacturer placed the keys on the card. In this example, the manufacturer can provide the order to the host computer. As another example, the applet of the contactless card assigns the order of the keys, and the applet can communicate this order to the host computer (e.g., through a client device). As yet another example, a terminal or client device can determine the order and the terminal or client device can send the order to the contactless card and the host computer.

[00065] In an example embodiment, the key selection module can include a mathematical function or algorithm which receives an input and selects a key based on the input (e.g., the function defines a many-to-many relationship between the inputs and keys). For example, the key selection module can receive a counter number or time signal and based on the counter number or time signal can select a key among the plurality of keys available. In this example embodiment, the host computer can also store the same key selection module (or the algorithm embedded therein) to select the keys. The host computer can also obtain the same counter number or time signal. For example, every time the contactless card is used to conduct a transaction, the counter of the contactless card increments the counter number at the contactless card and the counter of the host computer increments the count number at the host computer. This way, both the contactless card and the host computer can include the same count number when selecting the key. As another example, each of the contactless card and the host computer can include a timer. The timer can provide a time signal to the contactless card and the host computer. When both the contactless card and the host computer include the same counter number or time signal, using the key selection module, each of the contactless card and the host computer can select the same key for the operation.

[00066] As yet another example, the key selection module can select a key based on an input provided by a source outside of the contactless card. For example, the contactless card and the host computer can receive an input or signal from a terminal or client device, e.g., the input or signal can include information such as date, location coordinates of the terminal, location of the Hubble telescope, a photo of the user taken at the terminal, a number provided by the user on the terminal, etc. Based on this input, the key selection algorithm of each of the contactless card and the host computer can select a key and process a transaction.

[00067] As yet another example, the key selection module can randomly select the keys. In this example, the host computer does not know which key is selected by the contactless card. However, when the host computer receives a communication, the host computer can try all of its keys to decrypt the communication.

[00068] As yet another example, the key selection module can select the keys based on the last transaction value conducted by the card. The contactless card can store the transaction value for the last transaction. Similarly, the host computer can store the transaction value for the last transaction. Using the transaction value, the key selection module can derive a value, which can select the key. For example, if the last transaction value for the card is $9.95, the key selection module can select a key for encryption based on the last digit of the transaction value, which here is 5. The key selection module can select the key that, e.g., is ranked as 5

[00069] As yet another example embodiment, there can be a plurality of key selection algorithms, and each algorithm can receive an input and produce an output which determines the key to be selected for an operation. In this embodiment, there can be an algorithm selection module which selects the key selection algorithm based on an input. For example, the contactless card can include two key selection algorithms, and each algorithm can use the count number to designate a key for an encryption operation. In this example, a user can provide a PIN to the client device. The client device can transmit the PIN to both the contactless card and the host computer and each device can use the PIN as an input for the algorithm selection module. Using the PIN and the algorithm selection module, each of the contactless card and the host computer can select one of the two key selection algorithms. Using the count number and the chosen key selection algorithm, each of the contactless card and the host computer can select the same key for the operation.

[00070] FIG. 4 shows an example flowchart for transmission of information from a

contactless card to a host computer. In this example embodiment, a public-key scheme is implemented as the encryption technique. In step 401, a plurality of pairs of private and public keys are generated. These keys can be generated using a key generation algorithm. In step 402, the private keys are stored on a contactless card and the public keys are stored on a host computer. In step 403, a customer scans the contactless card at a terminal to request a transaction. The terminal can power up the contactless card and an applet of the contactless card can generate a communication. The communication can include an account number of the user.

[00071] In step 404, a key selection module of the applet can select one of the private keys stored on the contactless card. For example, the applet can transmit a request to the terminal to prompt the user to enter a number. In response, the user can enter the number and the terminal can transmit the number to the contactless card. The terminal can also transmit the number to the host computer. Using the number, the key selection module can select one of the private keys stored on the contactless card. In another example, the contactless card can request the terminal to transmit the terminal's location, e.g., zip code, to the contactless card. The terminal can transmit the location to the contactless card and the host computer. Based on the location, the key selection module can select one of the private keys.

[00072] In step 405, the applet can encrypt the communication using the selected private key. In step 406, the contactless card can transmit the encrypted communication to the terminal and the terminal can transmit the encrypted communication to the host computer. In step 407, the host computer can select a public key for decrypting the communication. For example, the host computer can use the number that the terminal transmitted to the host computer to select the public key. The public key can be selected using the key selection module stored on the host computer. In step 408, the host computer decrypts the

communication using the public key that was selected in step 407.

[00073] In one example embodiment, the contactless card can include a plurality of encryption algorithms. The contactless card can encrypt communications or create cryptograms using each of the encryption algorithms. The contactless card can also include an encryption algorithm selection module. The encryption algorithm selection module can select one of the plurality of encryption algorithms, and the contactless card can encrypt the communication using the selected encryption algorithm. Similarly, the host computer can include the plurality of encryption algorithms and the encryption algorithm selection module. When the host computer receives an encrypted communication, using the encryption algorithm selection module, the host computer can decide which encryption algorithm use to decrypt the communication.

[00074] In one embodiment, the encryption algorithm selection module can operate similar to the algorithm selection module or key selection module discussed above, e.g., receive an input and, based on the input, select one of the plurality of encryption algorithms.

[00075] In an example embodiment, for an encryption operation, a contactless card can include ten keys and two encryption algorithms, e.g., AES and 3DES. When processing a transaction, the contactless card can receive a number input from the terminal, e.g., the user provides the number input on a keypad of the terminal. The contactless card can also store a counter number in the memory of the contactless card. The counter number can represent the number of transactions the contactless card has requested.

[00076] The contactless card can include a key selection module and an encryption algorithm selection module. The key selection module can receive the number input and, for example, based on the last digit of the number input, select one of the ten keys stored on the contactless card for the encryption operation. The encryption algorithm selection module can receive the counter number and select the AES algorithm if the counter number

is even, or select the 3DES algorithm if the counter number is odd. The contactless card can create a cryptogram using a selected key and selected encryption algorithm and transmit the cryptogram to the terminal.

[00077] In one example embodiment, the contactless card can switch between a secret key OTP (or one-time password) for some transactions, and if possible, (e.g., two-way communication is possible) Public key for other transactions. As described above for various selection modules, the encryption algorithm selection module can select or switch between the two encryption schemes.

[00078] In one example embodiment, the contactless card can include a plurality of keys for a specific operation, and each time the contactless card needs to perform the operation, the key selection module can select one of the keys for the operation.

[00079] In another example embodiment, the contactless card can include a master key and a key diversification algorithm. The key diversification algorithm can generate a plurality of distinct keys using an input. In this example embodiment, for at least one of the operations on the contactless card, the contactless card can store a master key. The key selection module can provide an output to the key diversification algorithm, and, using the output, the key diversification algorithm can generate a diversified key for the master key. The contactless card can perform the operation using the diversified key, e.g., encrypt a communication. Similarly, as described above, the host computer can generate the same output using the key selection module. The host computer can also store the same key diversification algorithm and master key. Using the output, the key diversification algorithm and master key, the host computer can generate the same diversified key as the contactless card and perform an associated operation on the host computer, e.g., decrypt the communication.

[00080] The present disclosure is not to be limited in terms of the particular embodiments

described in this application, which are intended as illustrations of various aspects. Many modifications and variations can be made without departing from its spirit and scope, as may be apparent. Functionally equivalent methods and apparatuses within the scope of the disclosure, in addition to those enumerated herein, may be apparent from the foregoing representative descriptions. Such modifications and variations are intended to fall within the scope of the appended representative claims. The present disclosure is to be limited only by the terms of the appended representative claims, along with the full scope of equivalents to which such representative claims are entitled. It is also to be understood that the terminology used herein is for the purpose of describing particular embodiments only, and is not intended to be limiting.

CLAIMS

1. A server comprising:

a processor and a memory, the memory storing a first plurality of security keys, a key selection algorithm, and a first input value;

wherein the server is configured to:

receive a first encrypted communication from a contactless card through a client device, the contactless card having a card processor and a card memory, the card memory storing the first plurality of security keys, the key selection algorithm and the first input value;

select a first selected security key using the key selection algorithm and the first input value the first selected security key being one of the first plurality of security keys; and

decrypt the encrypted communication using the first selected security key to obtain an unencrypted communication.

2. The server of claim 1, wherein:

the memory of the server stores a second plurality of security keys, a second input value, a verification algorithm and a third input value;

the card memory stores the second plurality of security keys, the second input value, the verification algorithm and the third input value;

the server is further configured to:

receive a second encrypted communication from the contactless card through the client device;

select a second selected security key using the key selection algorithm and the second input value, the second selected security key being one of the first plurality of security keys;

decrypt the second encrypted communication using the second selected security key to obtain a second unencrypted communication;

receive a third communication from the contactless card through the client device;

select a third selected security key using the verification algorithm and the third input value, the third selected security key being one of the second plurality of security keys; and

verify the third communication using the third selected security key.

3. The server of claim 1, wherein the first input value is a counter number and each time the contactless card is scanned at the client device, the counter number is incremented at the contactless card and the server.

4. The server of claim 1, wherein the first input value is a time signal.

5. The server of claim 1, wherein the contactless card generated the first encrypted communication using a contactless card selected security key.

6. The server of claim 5, wherein the contactless card selected security key was selected based on the first input value using the key selection algorithm.

7. The server of claim 5, wherein the contactless card selected security key is the same as the first selected security key.

8. The server of claim 1, wherein the key selection algorithm is selecting the first selected security key based on the counter value.

9. The server of claim 1, wherein the key selection algorithm is selecting the first selected security key based a time of the transaction.

10. The server of claim 1, wherein the key selection algorithm is selecting the first selected security key based on a modular index or a replaceable random selection algorithm.

11. A contactless card comprising:

a substrate, including:

a memory containing one or more applets, a counter value, and a plurality of master keys and a key selection algorithm;

a communication interface; and

a processor in communication with the memory and communication interface;

wherein the processor is configured to:

increment the counter value when the communication interface is within a range of a communication field of a client device;

select a selected master key using a key selection algorithm stored on the memory;

create a diversified key using the selected master key and the counter value;

create a cryptogram using the diversified key; and

transmit, via the communication interface, the cryptogram to the client device.

12. The server of claim 11, wherein the key selection algorithm is selecting the selected key based on the counter value.

13. The server of claim 11, wherein the key selection algorithm is selecting the selected key based a time of the transaction.

14. The server of claim 11, wherein the key selection algorithm is selecting the selected key based on a modular index.

15. The server of claim 11, wherein the key selection algorithm is selecting the selected key based on a replaceable random selection algorithm.

16. A method comprising:

receiving an encrypted communication from a contactless card;

transmitting the encrypted communication a server;

receive a signal from the server authorizing a transaction.

wherein:

the encrypted communication was created using a diversified key;

the diversified key was generated using a selected master key, a counter value and a cryptographic algorithm;

the selected master key was selected using a key selection algorithm; and

the contactless card is configured to increment the counter value when a communication interface of the contactless card is within a range of a communication field of a client device.

17. The server of claim 16, wherein the key selection algorithm is selecting the selected key based on the counter value.

18. The server of claim 16, wherein the key selection algorithm is selecting the selected key based a time of the transaction.

19. The server of claim 16, wherein the key selection algorithm is selecting the selected key based on a modular index.

20. The server of claim 16, wherein the key selection algorithm is selecting the selected key based on a replaceable random selection algorithm.