[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 may enhance the security of a contactless card against such attacks by implementing multiple security keys.

[0005a] According to one aspect, there is provided a server comprising a processor and a memory, the memory storing a first plurality of keys, a first input value, and a first encrypted communication from a contactless card, wherein the processor is configured to: update the first input value to derive a second input value, select a first selected key using a key selection algorithm and the second input value, the first selected key being one of the first plurality of keys, and decrypt the first encrypted communication using the first selected key to obtain a first unencrypted communication.

[0005b] According to another aspect, there is provided a method, the method comprising: updating, by a server, a first input value to derive a second input value; selecting, by the server, a first selected key using a key selection algorithm and the second input value, the first selected key being one of a first plurality of keys; and decrypting, by the server, a first encrypted communication using the second selected key to obtain a first unencrypted communication.

[0005c] According to another aspect, there is provided a contactless card comprising a memory containing a plurality of keys; a transceiver; and a processor in communication with the memory and the transceiver, wherein the processor is configured to: select a first selected key using a key selection algorithm and the counter, generate a communication, encrypt the communication using the first selected key to obtained an encrypted communication, and transmit, via the transceiver, the encrypted communication.

[0005d] 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

CLAIMS

1. A server, comprising:

a processor; and

a memory, the memory storing a first plurality of keys, a first input value, and a first encrypted communication from a contactless card,

wherein the processor is configured to:

update the first input value to derive a second input value,

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

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

2. The server of claim 1, wherein the first input value is updated to derive the second input value with a first number is derived from a first transaction associated with the contactless card.

3. The server of claim 2, wherein the first number derived from the transaction is a last digit of a total for a purchase transaction by a credit card.

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

5. The server of claim 1, wherein the server is further configured to:

receive a second encrypted communication from the contactless card,

update the second input value to derive a third input value using a second number associated with the contactless card,

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

decrypt the third encrypted communication using the third selected key to obtain a third unencrypted communication.

6. The server of claim 5, wherein:

the memory stores a second plurality of security keys, a fourth input value, a verification algorithm, and a fifth input value, and

the processor is further configured to:

receive a third encrypted communication from the contactless card through the client device,

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

decrypt the third encrypted communication using the third selected security key to obtain a third unencrypted communication,

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

verify the third communication using the fifth selected security key.

7. The server of claim 6, wherein the key selection algorithm is selecting the third selected key based on a counter.

8. The server of claim 5, wherein the key selection algorithm is selecting the third selected key based a time of the transaction.

9. The server of claim 5, wherein the key selection algorithm is selecting the third selected key based on a modular index.

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

11. A method, the method comprising:

updating, by a server, a first input value to derive a second input value;

selecting, by the server, a first selected key using a key selection algorithm and the second input value, the first selected key being one of a first plurality of keys; and

decrypting, by the server, a first encrypted communication using the second selected key to obtain a first unencrypted communication.

12. The method of claim 11, wherein:

the first input value is updated to derive the second input value with a last digit of a total for a purchase transaction by a credit card.

13. The method of claim 11, wherein the memory stores a second encrypted communication from the contactless card, the method further comprising:

updating the second input value to derive the third input value using a second number derived from a second transaction associated with the contactless card;

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

decrypting the second encrypted communication using the second selected key to obtain a second unencrypted communication.

14. The method of claim 11, wherein the first input value is a counter and each time the contactless card is scanned at a client device, the counter is incremented at the server.

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

16. A contactless card, comprising:

a memory containing a plurality of keys;

a transceiver; and

a processor in communication with the memory and the transceiver,

wherein the processor is configured to:

select a first selected key using a key selection algorithm and the counter,

generate a communication,

encrypt the communication using the first selected key to obtained an encrypted communication, and

transmit, via the transceiver, the encrypted communication.

17. The contactless card of claim 16, wherein the key selection algorithm is selecting the first selected key based on an assigned order.

18. The contactless card of claim 16, wherein the key selection algorithm is selecting the first selected key randomly.

19. The contactless card of claim 16, wherein the key selection algorithm is selecting the first selected key based on a transaction value for the last transaction conducted by the contactless card.

20. The contactless card of claim 16, wherein:

the memory further contains a counter,

the processor is further configured to increment the counter when the transceiver is within a range of a communication field of a client device, and

the key selection algorithm is selecting the first selected key based on the incremented counter.