[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, a key selection algorithm configured to select one of the first plurality of keys based on the first input value, and a first encrypted communication from a contactless card, wherein the processor is configured to: select a first selected key using the key selection algorithm and the first input value, the first selected key being selected from the first plurality of keys, and decrypt the first encrypted communication using a diversified key generated from the first selected key to obtain a first unencrypted communication.

[0005b] According to another aspect, there is provided a method, the method comprising: receiving, by a server, a first encrypted communication generated by a contactless card; selecting, by the server, a first selected key using a key selection algorithm and a first input value,

wherein the first selected key is selected from a first plurality of keys based on the first input value and the key selection algorithm; and decrypting, by the server, the first encrypted communication using a diversified key generated from the first selected key, wherein the first encrypted message is generated using a key selected by the key selection algorithm stored on the contactless card.

[0005c] According to another aspect, there is provided a contactless card comprising a memory containing a plurality of keys and a key selection algorithm; 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 the key selection algorithm and a first input value stored on the memory, generate a diversified key using the first selected key, generate a cryptogram using the diversified key, and transmit, via the transceiver, cryptogram to a client device.

[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, a key selection algorithm configured to select one of the first plurality of keys based on the first input value, and a first encrypted communication from a contactless card,

wherein the processor is configured to:

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

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

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

3. The server of claim 2, wherein the first number corresponds to a last digit of a total purchase amount associated with the first transaction.

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 first input value to a second input value associated with a second transaction conducted with the contactless card,

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

decrypt the second encrypted communication using a diversified key generated from the second selected key to obtain a second unencrypted communication.

6. The server of claim 5, wherein the first input value is based on a transaction time associated with the first encrypted communication and the second input value is associated with the second encrypted communication.

7. The server of claim 1, wherein the key selection algorithm is selecting the first selected key based on a modular index.

8. The server of claim 1, wherein:

the contactless card generated the first encrypted communication using a selected contactless card key, and

the selected contactless card key is selected, by the key selection algorithm from a plurality of keys stored on the contactless card, based on the first input value stored on the contactless card.

9. A method, the method comprising:

receiving, by a server, a first encrypted communication generated by a contactless card;

selecting, by the server, a first selected key using a key selection algorithm and a first input value, wherein the first selected key is selected from a first plurality of keys based on the first input value and the key selection algorithm; and

decrypting, by the server, the first encrypted communication using a diversified key generated from the first selected key,

wherein the first encrypted message is generated using a key selected by the key selection algorithm stored on the contactless card.

10. The method of claim 9, wherein:

the first input value corresponds to a last digit of a total for a purchase transaction by the contactless card.

11. The method of claim 9, wherein the memory stores a second encrypted communication from the contactless card, the method further comprising:

updating the first input value to a second input value associated with a second transaction conducted with the contactless card;

selecting a second selected key using the key selection algorithm and the second input value, the second selected key being selected from the first plurality of keys based on the second input value; and

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

12. The method of claim 9, 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.

13. The method of claim 9, wherein the key selection algorithm is selecting the first selected key based on a replaceable random selection algorithm.

14. A contactless card, comprising:

a memory containing a plurality of keys and a key selection algorithm;

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 the key selection algorithm and a first input value stored on the memory,

generate a diversified key using the first selected key,

generate a cryptogram using the diversified key, and

transmit, via the transceiver, the cryptogram to a client device.

15. The contactless card of claim 14, wherein the key selection algorithm is selecting the first selected key based on an assigned order.

16. The contactless card of claim 14, wherein the key selection algorithm is selecting the first selected key randomly.

17. The contactless card of claim 14, wherein the key selection algorithm is selecting the first selected key based on a transaction value for a last transaction conducted by the contactless card.

18. The contactless card of claim 14, wherein:

the first input value corresponds to a counter stored on the memory, and wherein,

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

19. The method of claim 9, wherein the key selection algorithm is selecting the first selected key based on a modular index.

20. The contactless card of claim 14, wherein the key selection algorithm is selecting the first selected key based on a modular index.