

CLAIMS

~~What is claimed is:~~

1. A contactless card, comprising:
a processor; and
a memory, the memory containing a counter,
wherein the processor is configured to:
generate a one-time password,
transmit the one-time password for authentication, and
adjust the counter at one or more intervals in a non-monotonic sequence.
2. The contactless card of claim 1, wherein the non-monotonic sequence is created by a cryptographic algorithm.
3. The contactless card of claim 2, wherein the cryptographic algorithm is selected to avoid wrapping of the counter.
4. The contactless card of claim 2, wherein the cryptographic algorithm encrypts a starting value to obtain one or more additional counters.
5. The contactless card of claim 4, wherein the processor is further configured to derive the counter by truncating an output of the ~~encryption~~ cryptographic algorithm.

6. The contactless card of claim 5, wherein the processor is further configured to obtain the one or more additional counters by incrementing and encrypting the truncated output.
7. The contactless card of claim 1, wherein the processor is further configured to adjust the counter each time ~~a~~the one-time password is generated.
8. The contactless card of claim 1, wherein adjusting the counter comprises:
incrementing the counter by a first value for a first account, and
decrementing the counter by a second value for a second account.
9. The contactless card of claim 1, wherein the counter determines a number of cryptographic operations performed to generate the one-time password.
10. The contactless card of claim 1, wherein adjusting the counter comprises at least one selected from the group of incrementing the counter at the one or more intervals in the non-monotonic sequence and decrementing the counter at the one or more intervals in the non-monotonic sequence.
11. The contactless card of claim 1, wherein the processor is further configured to perform one or more cryptographic hashes to generate the counter.
12. A method for authentication, comprising:
generating, by a processor, a one-time password;
transmitting, by the processor, the one-time password for authentication; and

adjusting, by the processor, a counter at one or more intervals in a non-monotonic sequence.

13. The method of claim 12, wherein the non-monotonic sequence is created by a cryptographic algorithm.

14. The method of claim 13, wherein the cryptographic algorithm encrypts a starting value to obtain one or more additional counters.

15. The method of claim 12, wherein adjusting the counter comprises:

incrementing the counter by a first value for a first account, and
decrementing the counter by a second value for a second account.

16. ~~The method of claim 15, wherein:~~

~~the counter is incremented at the one or more intervals in the non-monotonic sequence,
and~~

~~the counter is decremented at the one or more intervals in the non-monotonic sequence.~~
The method of claim 13, wherein the encryption algorithm is selected to avoid collisions of counter values.

17. The method of claim 12, wherein the counter determines a number of cryptographic operations performed to generate the one-time password.

18. The method of claim 12, further comprising generating, by the processor, the counter by performing one or more cryptographic hashes.

19. The method of claim 18, further comprising:

deriving the counter by truncating an output of the ~~encryption~~ cryptographic algorithm,
and

incrementing and encrypting the truncated output to obtain one or more additional counters.

20. A non-transitory computer readable medium comprising computer executable instructions that, when executed on a processor, configure the processor to perform procedures comprising the steps of:

generating a one-time password;
transmitting the one-time password for authentication; and
adjusting a counter at one or more intervals in a non-monotonic sequence, wherein the non-monotonic sequence is created by one or more cryptographic algorithms.