CLAIMS

What is claimed is:

1. A computer-implemented method using a chameleon hash function, wherein the chameleon hash function comprises one or more modular exponentiations and one or more modular multiplications, the method comprising, at a signature-verification phase:

precomputing, at an offline phase of the signature-verification phase, at least partially each of the one or more modular exponentiations of the chameleon hash function; and

evaluating, at an online phase of the signature-verification phase, the chameleon hash function based on the precomputed one or more modular exponentiations and one or more modular multiplications,

wherein precomputing, at the offline phase of the signature-verification phase, at least partially each of the one or more modular exponentiations of the chameleon hash function comprising precomputing successive squares of a base of the respective modular exponentiation to obtain an array associated with the base of the respective modular exponentiation.

2. The computer-implemented method according to claim 1, wherein an i-th element of the array associated with the base of the respective modular exponentiation is a 2^i-th powers of the base of the respective modular exponentiation.

3. The computer-implemented method according to claim 2, wherein evaluating, at an online phase of the signature-verification phase, the chameleon hash function comprises

multiplying the *i*-th element of the array associated with the base of the respective modular exponentiation with a corresponding intermediate result iteratively obtained.

4. The computer-implemented method according to any one of claims 1 to 3, further comprising, at a signature-generation phase:

precomputing, at an offline phase of the signature-generation phase, a standard signature on a value of the chameleon hash function when applied on a random message and a randomness chosen randomly;

signing, at an online phase of the signature-generation phase, for a received message using a secret key associated with the chameleon hash function to find a collision with the value of the chameleon hash function precomputed at the offline phase of the signature-generation phase.

5. The computer-implemented method according to claim 4, wherein the signature-generation phase comprises a signature-generation phase of a threshold signature scheme wherein up to a threshold number of secret keys in the threshold signature scheme are corrupted.

6. The computer-implemented method according to claim 1, wherein the chameleon hash function is based on the discrete-logarithm problem, and is defined by a first modular exponentiation having a first base, a second modular exponentiation having a second base and a modular multiplication of the first and second modular exponentiations.

7. The computer-implemented method according to claim 6, wherein a public key of the chameleon hash function is defined by the first base associated with the first modular

exponentiation, the second base associated with the second modular exponentiation and a prime used for the first and second modular exponentiations and the modular multiplication.

8. The computer-implemented method according to any one of claims 1 to 7, wherein the precomputed one or more modular exponentiations is stored overhead at a verifier side.

9. The computer-implemented method according to any one of claims 1 to 8, wherein the chameleon hash function comprises discrete logarithm-based chameleon hash function comprising three modular exponentiations.

10. The computer-implemented method according to any one of claims 1 to 9, wherein precomputing, at an offline phase of the signature-verification phase, at least partially each of the one or more modular exponentiations of the chameleon hash function is performed one time by a single verifier.

11. The computer-implemented method according to claim 10, wherein evaluating, at an online phase of the signature-verification phase, the chameleon hash function based on the precomputed one or more modular exponentiations is performed multiple times by the single verifier.

12. The computer-implemented method according to claim 11, further comprising:
receiving a plurality of messages,

evaluating, at an online phase of the signature-verification phase, the chameleon hash function based on the precomputed one or more modular exponentiations for each of the plurality of messages.

13. A computer program comprising instructions to execute the steps of the computer-implemented method of any one of claims 1 to 12.

14. A non-transitory computer-readable medium having stored thereon the computer program of claim 13.

15. A system using a chameleon hash function, wherein the chameleon hash function comprises one or more modular exponentiations and one or more modular multiplications, the system comprising:

a processor configured to, at a signature-verification phase:

precompute, at an offline phase of the signature-verification phase, at least partially each of the one or more modular exponentiations of the chameleon hash function; and

evaluate, at an online phase of the signature-verification phase, the chameleon hash function based on the precomputed one or more modular exponentiations,

wherein precomputing, at the offline phase of the signature-verification phase, at least partially each of the one or more modular exponentiations of the chameleon hash function comprising precomputing successive squares of a base of the respective modular exponentiation to obtain an array associated with the base of the respective modular exponentiation.

16. The system according to claim 15, further comprises at least one terminal device registered with the processor, the at least one terminal device configured to send the at least one message to an input module.

17. The system according to claim 16, wherein the registration includes generating a unique identifier for each terminal device.

18. The system of claim 16, further comprises whitelisting specific IP addresses associated with the at least one terminal device.

19. The system of claim 17, wherein the at least one terminal device is a mobile computer device.