

CLAIMS:

1. A method for constructing a self-authenticating message to be sent from a first device to a second device comprising:
 - obtaining, by the first device, a first partial key and a second partial key for the first device, wherein the second partial key for the first device comprises a random number and the first partial key is generated based on the second partial key and a private key K_{first_device} ;
 - computing an intermediate key IK_{SR} using an identity of the second device ID_2 and the first partial key of the first device;
 - generating a shared key K_{SR} using the computed intermediate key IK_{SR} and the second partial key of the first device ;
 - generating an encryption key K using the shared key K_{SR} ;
 - encrypting a message using the generated encryption key K ;
 - forming the self-authenticating message based at least on the encrypted message;
 and
 - transmitting the formed self-authenticated message to the second device.
2. The method according to claim 1 wherein the forming the self-authenticating message based at least on the encrypted message comprises:
 - calculating, by the first device, a first Message Authentication Code (MAC) using the encryption key K and the encrypted message; and
 - forming the self-authenticating message based at least on an identity of the first device ID_1 , the encrypted message and the first MAC.
3. The method according to claim 1 or 2 wherein the method for obtaining the private key K_{first_device} comprises:
 - transmitting, by the first device, an identity of the first device ID_1 to a private key generator such that the generator generates the private key K_{first_device} based on a master secret key s and the identity of the first device ID_1 ; and
 - receiving the private key K_{first_device} from the private key generator.
4. The method according to any one of claims 1 to 3 wherein the computing the intermediate key IK_{SR} by the first device using the identity of the second device ID_2 and the first partial key of the first device comprises:
 - transmitting, by the first device, the identity of the second device ID_2 and the first partial key of the first device to a computer server such that the computer server computes

the intermediate key IK_{SR} using the identity of the second device ID_2 and the first partial key of the first device; and

receiving the computed intermediate key IK_{SR} from the computer server.

5. The method according to any one of claims 1 to 4 wherein at the step of generating, by the first device, the encryption key K using the shared key K_{SR} , this step further comprises:
 - using a generated cryptographic nonce together with the shared key K_{SR} to generate the encryption key K ,
 - wherein at the step of forming the self-authenticating message, this step further comprises adding, by the first device, the cryptographic nonce to the self-authenticating message.
6. The method for constructing a self-authenticating message to be sent from a first device to a second device comprising, comprising:
 - obtaining, by the second device, a first partial key and a second partial key for the second device, wherein the second partial key for the second device comprises a random number and the first partial key is generated based on the second partial key and a private key K_{second_device} ;
 - receiving the self-authenticated message transmitted from the first device;
 - computing an intermediate key IK_{RS} using an identity of the first device ID_1 and the first partial key of the second device;
 - generating a shared key K_{SR} using the computed intermediate key IK_{RS} and the second partial key of the second device;
 - generating an encryption key K using the shared key K_{SR} ;
 - authenticating the received self-authenticating message using the encryption key K ; and
 - decrypting an encrypted message in the received self-authenticating message using the generated encryption key K , when the received self-authenticating message is authenticated successfully.
7. The method according to claim 6 wherein before the step of authenticating the received self-authenticating message using the encryption key K , the method further comprises:
 - calculating, by the second device, a second MAC using the generated encryption key K and the encrypted message from the received self-authenticating message,
 - wherein the step of authenticating the received self-authenticating message using the encryption key K , comprises:

determining, by the second device, whether the second MAC matches with a first MAC obtained from the received self-authenticating message or not;

authenticating the self-authenticating message successfully when the second MAC matches with the obtained first MAC.

8. The method according to claim 6 or 7 wherein the method for obtaining the private key K_{second_device} comprises:

transmitting, by the second device, an identity of the second device ID_2 to a private key generator such that the private key generator generates the private key K_{second_device} based on a master secret key s and the identity of the second device ID_2 ; and

receiving the private key K_{second_device} from the private key generator.

9. The method according to any one of claims 6 to 8 wherein the computing the intermediate key IK_{RS} by the second device using the identity of the first device ID_1 and the first partial key of the second device comprises:

transmitting, by the second device, the identity of the first device ID_1 and the first partial key of the second device to a computer server such that the computer server computes the intermediate key IK_{RS} using the identity of the first device ID_1 and the first partial key of the second device; and

receiving the computed intermediate key IK_{RS} from the computer server.

10. The method according to any one of claims 6 to 9 wherein at the step of generating, by the second device, the encryption key K using the shared key K_{SR} , the method further comprises:

retrieving, by the second device, a cryptographic nonce from the received self-authenticating message; and

generating, by the second device, the encryption key K , using the retrieved cryptographic nonce and the shared key K_{SR} .

11. A method for constructing a self-authenticating message to be sent from a first device to a second device comprising:

obtaining, by the first device, a first partial key and a second partial key for the first device, wherein the second partial key for the first device comprises a random number and the first partial key is generated based on the second partial key and a private key K_{first_device} ;

computing an intermediate key IK_{SR} using an identity of the second device ID_2 and the first partial key of the first device;

generating a shared key K_{SR} based on the computed intermediate key IK_{SR} and the second partial key of the first device ;

generating an encryption key K using the shared key K_{SR} together with a first constant and encrypting a message by the generated encryption key K , and generating an authentication key K_A using the shared key K_{SR} and a second constant, wherein the first and the second constants are obtained from the first device;

calculating a first Message Authentication Code (MAC) using the authentication key K_A and the encrypted message;

forming the self-authenticating message based at least on an identity of the first device ID_1 , the encrypted message and the first MAC; and

transmitting the formed self-authenticated message to the second device.

12. The method according to claim 11 wherein prior to the step of generating the encryption key K and the authentication key K_A , the method comprises the step of:

generating, by the first device, a cryptographic nonce, wherein the encryption key K is derived as: $K = \text{HMAC}(K_{SR}, \text{cryptographic nonce} \parallel \text{first constant})$, and the authentication key K_A is derived as: $K_A = \text{HMAC}(K_{SR}, \text{cryptographic nonce} \parallel \text{second constant})$, where $\text{HMAC}()$ is a key-hash message authentication code function.

13. A method for constructing a self-authenticating message to be sent from a first device to a second device comprising:

obtaining, by the second device, a first partial key and a second partial key for the second device, wherein the second partial key for the second device comprises a random number and the first partial key is generated based on the second partial key and a private key $K_{\text{second_device}}$;

receiving the self-authenticating message transmitted from the first device;

computing an intermediate key IK_{RS} using an identity of the first device ID_1 and the first partial key of the second device, and using the computed intermediate key IK_{RS} and the second partial key of the second device to generate a shared key K_{SR} ;

computing an encryption key K using the shared key K_{SR} and a first constant and an authentication key K_A using the shared key K_{SR} and a second constant, wherein the first and second constants are obtained from the second device,

calculating a second MAC using the computed authentication key K_A and an encrypted message from the received self-authenticating message,

determining if the second MAC matches with a first MAC obtained from the received self-authenticating message; and

decrypting the encrypted message in the received self-authenticating message using the generated encryption key K , when the second MAC matches with the obtained first MAC.

14. The method according to claim 13, wherein at the step of computing, by the second device, the encryption key K and the authentication key K_A , the encryption key K is derived as: $K = \text{HMAC}(K_{\text{SR}}, \text{cryptographic nonce} \parallel \text{first constant})$, and the authentication key K_A is derived as: $K_A = \text{HMAC}(K_{\text{SR}}, \text{cryptographic nonce} \parallel \text{second constant})$ whereby the first and second constants are obtained from the received self-authenticating message.
15. A method for constructing a self-authenticating message to be sent from a first device to a second device comprising:
 - obtaining, by the first device, a first partial key and a second partial key for the first device, wherein the second partial key for the first device comprises a random number and the first partial key is generated based on the second partial key and a private key $K_{\text{first_device}}$;
 - computing an intermediate key IK_{SR} using an identity of the second device ID_2 and the first partial key of the first device;
 - generating a shared key K_{SR} using the computed intermediate key IK_{SR} and the second partial key of the first device;
 - generating an encryption key K using the shared key K_{SR} ;
 - calculating a first Message Authentication Code (MAC) using the encryption key K and a message; and
 - forming the self-authenticating message based at least on an identity of the first device ID_1 , the message and the first MAC; and
 - transmitting the formed self-authenticated message to the second device.
16. A method for constructing a self-authenticating message to be sent from a first device to a second device comprising:
 - obtaining, by the second device, a first partial key and a second partial key for the second device, wherein the second partial key for the second device comprises a random number and the first partial key is generated based on the second partial key and a private key $K_{\text{second_device}}$;
 - receiving the self-authenticated message transmitted from the first device;
 - computing an intermediate key IK_{RS} using an identity of a first device ID_1 and the first partial key of the second device;

generating a shared key K_{SR} using the computed intermediate key IK_{RS} and the second partial key of the second device;

computing an encryption key K , and calculating a second MAC using the generated encryption key K and a message from the received self-authenticating message;

determining if the second MAC matches with a first MAC obtained from the received self-authenticating message; and

authenticating the self-authenticating message when the second MAC matches with the obtained first MAC.

17. A system for constructing a self-authenticating message to be sent from a first device to a second device, the system comprising:

a processor provided within the first device; and

a non-transitory media readable by the processor provided within the first device, the media storing instructions that when executed by the processor, cause the processor to:

obtain a first partial key and a second partial key for the first device, wherein the second partial key for the first device comprises a random number and the first partial key is generated based on the second partial key and a private key K_{first_device} ;

compute an intermediate key IK_{SR} using an identity of the second device ID_2 and the first partial key of the first device;

generate a shared key K_{SR} using the computed intermediate key IK_{SR} and the second partial key of the first device ;

generate an encryption key K using the shared key K_{SR} ;

encrypt a message using the generated encryption key K ;

form the self-authenticating message based at least on the encrypted message;

and

transmit the formed self-authenticated message to the second device.

18. The system according to claim 17 wherein the instructions to form the self-authenticating message based at least on the encrypted message comprises:

instructions for directing the processor to:

calculate a first Message Authentication Code (MAC) using the encryption key K and the encrypted message; and

form the self-authenticating message based at least on an identity of the first device ID_1 , the encrypted message and the first MAC.

19. The system according to claim 17 or 18 wherein the instructions to obtain the private key K_{first_device} comprises:

instructions for directing the processor to:

transmit an identity of the first device ID_1 to a private key generator such that the generator generates a private key K_{first_device} based on a master secret key s and the identity of the first device ID_1 ; and

receive the private key K_{first_device} from the private key generator.

20. The system according to any one of claims 17 to 19 wherein the instructions for directing the processor to compute the intermediate key IK_{SR} by the first device using the identity of the second device ID_2 and the first partial key of the first device comprises:

instructions for directing the processor to:

transmit the identity of the second device ID_2 and the first partial key of the first device to a computer server such that the computer server computes the intermediate key IK_{SR} using the identity of the second device ID_2 and the first partial key of the first device; and

receive the computed intermediate key IK_{SR} from the computer server.

21. The system according to any one of claims 17 to 20 wherein the instructions for directing the processor to generate the encryption key K using the shared key K_{SR} , further comprises: instructions for directing the processor to:

use a generated cryptographic nonce together with the shared key K_{SR} to generate the encryption key K ,

wherein the instructions for directing the processor to form the self-authenticating message further comprises instructions for directing the processor to add the cryptographic nonce to the self-authenticating message.

22. The system for constructing a self-authenticating message to be sent from a first device to a second device comprising, comprising:

a processor provided within the second device; and

a non-transitory media readable by the processor provided within the second device, the media storing instructions that when executed by the processor, cause the processor to:

obtain a first partial key and a second partial key for the second device, wherein the second partial key for the second device comprises a random number and the first partial key is generated based on the second partial key and a private key K_{second_device} ;

receive the self-authenticated message transmitted from the first device;

compute an intermediate key IK_{RS} using an identity of the first device ID_1 and the first partial key of the second device;

generate a shared key K_{SR} using the computed intermediate key IK_{RS} and the second partial key of the second device;

generate an encryption key K using the shared key K_{SR} ;

authenticate the received self-authenticating message using the encryption key K ;

and

decrypt an encrypted message in the received self-authenticating message using the generated encryption key K , when the received self-authenticating message is authenticated successfully.

23. The system according to claim 22 wherein before the instructions for directing the processor to authenticate the received self-authenticating message using the encryption key K , the system further comprises:

instructions for directing the processor to

calculate a second MAC using the generated encryption key K and the encrypted message from the received self-authenticating message,

wherein the instructions for directing the processor to authenticate the received self-authenticating message using the encryption key K , comprises:

instructions for directing the processor to:

determine whether the second MAC matches with a first MAC obtained from the received self-authenticating message or not; and

authenticate the self-authenticating message successfully when the second MAC matches with the obtained first MAC.

24. The system according to claim 22 or 23 wherein the instructions for directing the processor to obtain the private key $K_{fsecond_device}$ comprises:

instructions for directing the processor to:

transmit an identity of the second device ID_2 to a private key generator such that the private key generator generates a private key K_{second_device} based on a master secret key s and the identity of the second device ID_2 ; and

receive the private key K_{second_device} from the private key generator.

25. The system according to any one of claims 22 to 24 wherein the instructions for directing the processor to compute the intermediate key IK_{RS} by the second device using the identity of the first device ID_1 and the first partial key of the second device comprises:

instructions for directing the processor to:

transmit the identity of the first device ID_1 and the first partial key of the second device to a computer server such that the computer server computes the intermediate key IK_{RS} using the identity of the first device ID_1 and the first partial key of the second device;
and

receive the computed intermediate key IK_{RS} from the computer server.

26. The system according to any one of claims 22 to 25 wherein the instructions for directing the processor to generate the encryption key K further comprises:

instructions for directing the processor to:

retrieve a cryptographic nonce from the received self-authenticating message;

and

generate the encryption key K , using the retrieved cryptographic nonce and the shared key K_{SR} .

27. A system for constructing a self-authenticating message to be sent from a first device to a second device comprising:

a processor provided within the first device; and

a non-transitory media readable by the processor provided within the first device, the media storing instructions that when executed by the processor, cause the processor to:

obtain a first partial key and a second partial key for the first device, wherein the second partial key for the first device comprises a random number and the first partial key is generated based on the second partial key and a private key K_{first_device} ;

compute an intermediate key IK_{SR} using an identity of the second device ID_2 and the first partial key of the first device;

generate a shared key K_{SR} based on the computed intermediate key IK_{SR} and the second partial key of the first device ;

generate an encryption key K using the shared key K_{SR} together with a first constant and encrypting a message by the generated encryption key K , and generating an authentication key K_A using the shared key K_{SR} and a second constant, wherein the first and the second constants are obtained from the first device;

calculate a first Message Authentication Code (MAC) using the authentication key K_A and the encrypted message;

form the self-authenticating message based at least on an identity of the first device ID_1 , the encrypted message and the first MAC; and

transmit the formed self-authenticated message to the second device.

28. The system according to claim 27 wherein prior to the instructions for directing the processor to generate the encryption key K and the authentication key K_A , the system comprises:

instructions for directing the processor to:

generate a cryptographic nonce, wherein the encryption key K is derived as: $K = \text{HMAC}(K_{SR}, \text{cryptographic nonce} \parallel \text{first constant})$, and the authentication key K_A is derived as: $K_A = \text{HMAC}(K_{SR}, \text{cryptographic nonce} \parallel \text{second constant})$, where $\text{HMAC}()$ is a key-hash message authentication code function.

29. A system for constructing a self-authenticating message to be sent from a first device to a second device comprising:

a processor provided within the second device; and

a non-transitory media readable by the processor provided within the second device, the media storing instructions that when executed by the processor, cause the processor to:

obtain a first partial key and a second partial key for the second device, wherein the second partial key for the second device comprises a random number and the first partial key is generated based on the second partial key and a private key $K_{\text{first_device}}$;

receive the self-authenticating message transmitted from the first device;

compute an intermediate key IK_{RS} using an identity of the first device ID_1 and the first partial key of the second device, and using the computed intermediate key IK_{RS} and the second partial key of the second device to generate a shared key K_{SR} ;

compute an encryption key K using the shared key K_{SR} and a first constant and an authentication key K_A using the shared key K_{SR} and a second constant, wherein the first and second constants are obtained from the second device,

calculate a second MAC using the computed authentication key K_A and an encrypted message from the received self-authenticating message,

determine if the second MAC matches with a first MAC obtained from the received self-authenticating message; and

decrypt the encrypted message in the received self-authenticating message using the generated encryption key K , when the second MAC matches with the obtained first MAC.

30. The system according to claim 29, wherein the instructions for directing the processor to compute the encryption key K and the authentication key K_A , comprises:

instructions for directing the processor to:

derive the encryption key K as: $K = \text{HMAC}(K_{\text{SR}}, \text{cryptographic nonce} \parallel \text{first constant})$, and the authentication key K_A as: $K_A = \text{HMAC}(K_{\text{SR}}, \text{cryptographic nonce} \parallel \text{second constant})$ whereby the first and second constants are obtained from the received self-authenticating message.

31. A system for constructing a self-authenticating message to be sent from a first device to a second device comprising:

a processor provided within the first device; and

a non-transitory media readable by the processor provided within the first device, the media storing instructions that when executed by the processor, cause the processor to:

obtain a first partial key and a second partial key for the first device, wherein the second partial key for the first device comprises a random number and the first partial key is generated based on the second partial key and a private key $K_{\text{first_device}}$;

compute an intermediate key IK_{SR} using an identity of the second device ID_2 and the first partial key of the first device;

generate a shared key K_{SR} using the computed intermediate key IK_{SR} and the second partial key of the first device;

generate an encryption key K using the shared key K_{SR} ;

calculate a first Message Authentication Code (MAC) using the encryption key K and a message; and

form the self-authenticating message based at least on an identity of the first device ID_1 , the message and the first MAC; and

transmit the formed self-authenticated message to the second device.

32. A system for constructing a self-authenticating message to be sent from a first device to a second device comprising:

a processor provided within the second device; and

a non-transitory media readable by the processor provided within the second device, the media storing instructions that when executed by the processor, cause the processor to:

obtain a first partial key and a second partial key for the second device, wherein the second partial key for the second device comprises a random number and the first partial key is generated based on the second partial key and a private key $K_{\text{first_device}}$;

receive the self-authenticated message transmitted from the first device;

compute an intermediate key IK_{RS} using an identity of a first device ID_1 and the first partial key of the second device;

generate a shared key K_{SR} using the computed intermediate key IK_{RS} and the second partial key of the second device;

compute an encryption key K , and calculating a second MAC using the generated encryption key K and a message from the received self-authenticating message;

determine if the second MAC matches with a first MAC obtained from the received self-authenticating message; and

authenticate the self-authenticating message when the second MAC matches with the obtained first MAC.