

CLAIMS:

1. A system for generating an escrow session key SK_1 and a private session key SK_2 for encoding digital communications between a device i and an another device j , comprising:

a secure server configured to:

generate a master secret key (MSK) and global system parameters (GSP) for an Identity Based Cryptography (IBC) scheme, whereby the MSK and GSP are utilized together with a requesting device's identity to generate an IBC private key IBC-K for the requesting device;

the device i , being configured to:

use an Identity Based Encryption (IBE) scheme associated with the IBC scheme to encrypt a first element g^a with an identity ID_j , associated with the another device j , where g is a generator of a cyclic multiplicative group G and a is a random number generated by the device i ;

communicate to the another device j , the encrypted first element, an identity ID_i associated with the device i and a session key request such that upon receiving the communication, the another device j is configured to:

use the IBE scheme to decrypt the encrypted first element with an IBC private key, IBC- K_j , whereby the private key, IBC- K_j , is requested and obtained from the secure server;

generate a second element g^b where g is the generator of the cyclic multiplicative group G and b is a random number generated by the another device j ;

compute the escrow session key SK_1 , using the first element;

compute the private session key SK_2 , using the first element and the random number b ; and

communicate the second element and an identity ID_j associated with the another device j to the device i ,

compute the escrow session key SK_1 , using the first element;

compute the private session key SK_2 , using the second element and the random number a ;

compute a first combined key SK_{11} by obtaining a coproduct of SK_1 and SK_2 ;

generate a key confirmation value using the first combined key SK_{11} whereby the key confirmation value is communicated to the another device j , such that upon receiving the key confirmation value, the another device j is configured to:

compute a second combined key SK_{22} by obtaining a coproduct of SK_1 and SK_2 ; and

verify the received key confirmation value using the second combined key SK_{22} and validate the escrow session key SK_1 and the private session key SK_2 if the received key confirmation value is verified

~~2. The system according to claim 1 further comprising the device i , being configured to:~~

~~compute a first combined key SK_{11} by obtaining a coproduct of SK_1 and SK_2 ;~~

~~generate a key confirmation value using the first combined key SK_{11} whereby the key confirmation value is communicated to the another device j , such that upon receiving the key confirmation value, the another device j is configured to:~~

~~compute a second combined key SK_{22} by obtaining a coproduct of SK_1 and SK_2 ; and~~

~~verify the received key confirmation value using the second combined key SK_{22} and validate the escrow session key SK_1 and the private session key SK_2 if the received key confirmation value is verified.~~

~~3.2. The system according to claims 1 or 2 wherein the another device j being configured to communicate the second element and the identity ID_j associated with the another device j to the device i further comprises the another device j being configured to:~~

~~use the IBE scheme to encrypt the second element with an identity ID_i associated with the device i ,~~

~~communicate the encrypted second element and the identity ID_j associated with the another device j to the device i such that upon receiving the communication, the device i is configured to:~~

~~use the IBE scheme to decrypt the encrypted second element with an IBC private key, $IBC-K_i$, whereby the private key, $IBC-K_i$, is requested and obtained from the secure server by the device i .~~

4.3. The system according to claim 32 wherein the computing the escrow session key SK_1 by the another device j comprises the another device j being configured to use the first element and the second element to generate the escrow session key SK_1 and the computing the escrow session key SK_1 by the device i comprises the device i being configured to use the first element and the second element to generate the escrow session key SK_1 .

5.4. The system according to claims 1 or 2 wherein the another device j being configured to communicate the second element and the identity ID_j associated with the another device j to the device i further comprises the another device j being configured to:

use a Public Key Infrastructure (PKI) scheme to encrypt the second element with a PKI Public Key PBK_i , associated with the device i ,

communicate the encrypted second element and the identity ID_j associated with the another device j to the device i such that upon receiving the communication, the device i is configured to:

use the PKI scheme to decrypt the encrypted second element with a PKI Private Key, PRK_i , associated with the device i .

6.5. The system according to claims 1 or 2 wherein the step of, communicating the encrypted first element, the identity ID_i associated with the device i and the session key request to the another device j by the device i further comprises the device i being configured to:

sign the encrypted first element using an IBC private signing key $IBC-K_i$ associated with the device i and in place of the encrypted first element, transmit the signed encrypted first element to the another device j such that upon receiving the communication, the another device j is configured to:

verify the signed encrypted first element using the identity ID_i associated with the device i and a verification function associated with the IBC scheme, whereby the first element is decrypted if the signed encrypted first element is verified.

7.6. A method for generating an escrow session key SK_1 and a private session key SK_2 for encoding digital communications between a device i and an another device j , the method comprising:

generating, by a secure server, a master secret key (MSK) and global system parameters (GSP) for an Identity Based Cryptography (IBC) scheme, whereby the MSK and GSP are utilized together with a requesting device's identity to generate an IBC private key IBC-K for the requesting device;

encrypting, by the device i , a first element g^a with an identity ID_i , associated with the another device j , using an Identity Based Encryption (IBE) scheme associated with the IBC scheme, where g is a generator of a cyclic multiplicative group G and a is a random number generated by the device i ;

communicating, by the device i , to the another device j , the encrypted first element, an identity ID_i associated with the device i and a session key request such that upon receiving the communication, the another device j is configured to:

use the IBE scheme to decrypt the encrypted first element with an IBC private key, IBC- K_j , whereby the private key, IBC- K_j , is requested and obtained from the secure server;

generate a second element g^b where g is the generator of the cyclic multiplicative group G and b is a random number generated by the another device j ;

compute the escrow session key SK_1 , using the first element;

compute the private session key SK_2 , using the first element and the random number b ; and

communicate the second element and an identity ID_j associated with the another device j to the device i ,

computing, by the device i , the escrow session key SK_1 , using the first element, and computing the private session key SK_2 , using the second element and the random number a ;

computing, by the device i , a first combined key SK_{11} by obtaining a coproduct of SK_1 and SK_2 ;

generating a key confirmation value using the first combined key SK_{11} whereby the key confirmation value is communicated to the another device j , such that upon receiving the key confirmation value, the another device j is configured to:

compute a second combined key SK_{22} by obtaining a coproduct of SK_1 and SK_2 ; and

verify the received key confirmation value using the second combined key SK_{22} and validate the escrow session key SK_1 and the private session key SK_2 if the received key confirmation value is verified.

~~8. The method according to claim 7 further comprising the steps of:~~

~~computing, by the device i , a first combined key SK_{11} by obtaining a coproduct of SK_1 and SK_{21}~~

~~generating a key confirmation value using the first combined key SK_{11} whereby the key confirmation value is communicated to the another device j , such that upon receiving the key confirmation value, the another device j is configured to:~~

~~compute a second combined key SK_{22} by obtaining a coproduct of SK_1 and SK_{21} and~~

~~verify the received key confirmation value using the second combined key SK_{22} and validate the escrow session key SK_1 and the private session key SK_2 if the received key confirmation value is verified.~~

~~9.7. The method according to claims 7 or 8~~ 6 wherein the step of the another device j being configured to communicate the second element and the identity ID_j associated with the another device j to the device i further comprises the step of:

using, by the another device j , the IBE scheme to encrypt the second element with an identity ID_i associated with the device i ,

communicating the encrypted second element and the identity ID_j associated with the another device j to the device i such that upon receiving the communication, the device i is configured to:

use the IBE scheme to decrypt the encrypted second element with an IBC private key, $IBC-K_i$, whereby the IBC private key, $IBC-K_i$, is requested and obtained from the secure server by the device i .

~~10.8.~~ The method according to claim 9 7 wherein the step of computing the escrow session key SK_1 by the another device j comprises the step of the another device j being configured to use the first element and the second element to generate the escrow session key SK_1 and the computing the escrow session key SK_1 by the device i comprises the step of the device i being configured to use the first element and the second element to generate the escrow session key SK_1 .

~~11.9.~~ The method according to claims ~~7- or 86~~ wherein the step of the another device j being configured to communicate the second element and the identity ID_j associated with the another device j to the device i further comprises the step of:

using, by the another device j , a Public Key Infrastructure (PKI) scheme to encrypt the second element with a PKI Public Key PBK_i , associated with the device i ,

communicating the encrypted second element and the identity ID_j associated with the another device j to the device i such that upon receiving the communication, the device i is configured to:

use the PKI scheme to decrypt the encrypted second element with a PKI Private Key, PRK_i , associated with the device i .

~~12.10.~~ The method according to claims ~~7- or 86~~ wherein the step of, communicating the encrypted first element, the identity ID_i associated with the device i and the session key request to the another device j by the device i further comprises the step of:

signing, by the device i , the encrypted first element using an IBC private signing key $IBC-K_i$ associated with the device i and in place of the encrypted first element, transmit the signed encrypted first element to the another device j such that upon receiving the communication, the another device j is configured to:

verifying the signed encrypted first element using the identity ID_i associated with the device i and a verification function associated with the IBC scheme, whereby the first element is decrypted if the signed encrypted first element is verified.

~~13.11.~~ A device i for generating an escrow session key SK_1 and a private session key SK_2 for encoding digital communications between the device i and another device j , comprising:

a processor; and

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

use an Identity Based Encryption (IBE) scheme associated with an Identity Based Cryptography (IBC) scheme to encrypt a first element g^a with an identity ID_j , associated with the another device j , where g is a generator of a cyclic multiplicative group G and a is a random number generated by the device i ,

wherein the IBC scheme comprises a master secret key (MSK) and global system parameters (GSP), whereby the MSK and GSP are utilized together with a requesting device's identity to generate an IBC private key IBC-K for the requesting device;

communicate to the another device j , the encrypted first element, an identity ID_i associated with the device i and a session key request;

receive a second element g^b and an identity ID_j associated with the another device j ;

compute the escrow session key SK_1 , using the first element; and

compute the private session key SK_2 , using the second element g^b and the random number a , where g is the generator of the cyclic multiplicative group G and b is a random number generated by the another device j ;

compute a first combined key SK_{11} by obtaining a coproduct of SK_1 and SK_2 ;

generate a key confirmation value using the first combined key SK_{11} whereby the key confirmation value is communicated to the another device j ; and

validate the key confirmation value if a key confirmation validation value associated with the another device j is received.

~~14. The device according to claim 13 further comprising the device i , being configured to:~~

~~compute a first combined key SK_{11} by obtaining a coproduct of SK_1 and SK_2 ;~~

~~generate a key confirmation value using the first combined key SK_{11} whereby the key confirmation value is communicated to the another device j ; and~~

~~validate the key confirmation value if a key confirmation validation value associated with the another device j is received.~~

~~15.12.~~ The device according to claims ~~13 or 14~~11 wherein the received second element g^b is encrypted using the IBE scheme and an identity ID_i associated with the device i , whereby the device uses the IBE scheme to decrypt the encrypted second element with an IBC private key, IBC- K_i , whereby the private key, IBC- K_i , is requested and generated in accordance with the IBC scheme.

~~16.13.~~ The device according to claim ~~15-12~~ wherein the computing the escrow session key SK_1 by the device i comprises the device i being configured to use the first element and the second element to generate the escrow session key SK_1 .

~~17.14.~~ The device according to claims ~~13 or 14~~11 wherein the received second element g^b is encrypted using a Public Key Infrastructure (PKI) scheme with a PKI Public Key PBK_i , associated with the device i , whereby the device uses the PKI scheme to decrypt the encrypted second element with a PKI Private Key, PRK_i , associated with the device i .

~~18.15.~~ The device according to claims ~~13 or 14~~11 wherein the step of, communicating the encrypted first element, the identity ID_i associated with the device i and the session key request to the another device j by the device further comprises the device i being configured to:

sign the encrypted first element using an IBC private signing key $IBC-K_i$ associated with the device i and in place of the encrypted first element, transmit the signed encrypted first element to the another device j .

~~19.16.~~ A method for generating an escrow session key SK_1 and a private session key SK_2 for encoding digital communications between a device i and another device j , comprising:

encrypting, by the device i , a first element g^a with an identity ID_j , associated with the another device j , using an Identity Based Encryption (IBE) scheme associated with an Identity Based Cryptography (IBC) scheme, where g is a generator of a cyclic multiplicative group G and a is a random number generated by the device i , wherein the IBC scheme comprises a master secret key (MSK) and global system parameters (GSP), whereby the MSK and GSP are utilized together with a requesting device's identity to generate an IBC private key $IBC-K$ for the requesting device;

communicating, by the device i , to the another device j , the encrypted first element, an identity ID_i associated with the device i and a session key request;

receiving ~~the a~~ second element and an identity ID_j associated with the another device j ; and

computing, by the device i , the escrow session key SK_1 , using the first element, and computing the private session key SK_2 , using the second element and the random number a_i ;

computing a first combined key SK_{11} by obtaining a coproduct of SK_1 and SK_2 ;

generating a key confirmation value using the first combined key SK_{11} whereby the key confirmation value is communicated to the another device j ; and

validating the key confirmation value if a key confirmation validation value associated with the another device j is received

~~20. The method according to claim 19 further comprising the steps of:~~

~~computing a first combined key SK_{11} by obtaining a coproduct of SK_1 and SK_{21} ;~~

~~generating a key confirmation value using the first combined key SK_{11} whereby the key confirmation value is communicated to the another device j ; and~~

~~validating the key confirmation value if a key confirmation validation value associated with the another device j is received.~~

~~21.17.~~ The method according to claims ~~19 or 20~~16 wherein the received second element g^b is encrypted using the IBE scheme and an identity ID_i associated with the device i , whereby the device uses the IBE scheme to decrypt the encrypted second element with an IBC private key, $IBC-K_i$, whereby the private key, $IBC-K_i$, is requested and generated in accordance with the IBC scheme.

~~22. The method according to claim 21 wherein the received second element g^b is encrypted using the IBE scheme and an identity ID_i associated with the device i , whereby the device uses the IBE scheme to decrypt the encrypted second element with an IBC private key, $IBC-K_i$, whereby the private key, $IBC-K_i$, is requested and generated in accordance with the IBC scheme.~~

~~23.18.~~ The method according to claims ~~19 or 20~~16 wherein the received second element g^b is encrypted using a Public Key Infrastructure (PKI) scheme with a PKI Public Key PBK_i , associated with the device i , whereby the device uses the PKI scheme to decrypt the encrypted second element with a PKI Private Key, PRK_i , associated with the device i .

~~24.19.~~ The method according to claims ~~19 or 20~~16 wherein the step of, communicating the encrypted first element, the identity ID_i associated with the device i and the session key request to the another device j by the device i further comprises the step of:

signing, by the device i , the encrypted first element using an IBC private signing key $IBC-K_i$ associated with the device i and in place of the encrypted first element, transmit the signed encrypted first element to the another device j .