

CLAIMS:

1. A method of sending an encrypted message by a sender having a sender identity string to a recipient over a network using Identity-Based Encryption, the method comprising:
 - identifying a Trusted Centre (TC) by a TC identity string (Id_{TC}), the Trusted Centre having a master public key of the Trusted Centre (g_{Pub}) based on the TC identity string (Id_{TC});
 - determining if the sender has a sender private key Prv_{Sender} and a plurality of public parameters (PK) for the Trusted Centre (TC), the public parameters (PK) including the master public key of the Trusted Centre (g_{Pub}) and a bilinear map (e);
 - verifying the public parameters (PK) of the Trusted Centre (TC) using the TC identity string (Id_{TC}) prior to encrypting a plaintext message (M);
 - identifying the recipient by a recipient identity string ($Id_{Recipient}$);
 - hashing the identity string of the recipient ($Id_{Recipient}$) using the hash function lying in the public parameters (PK), encrypting the plaintext message (M) as ciphertext (C) using the public parameters (PK), a random symmetric key (Σ) and the hash of the identity string of the recipient ($Id_{Recipient}$), and transmitting the ciphertext (C) to the recipient over the network.
2. The method of claim 1, wherein verifying the public parameters (PK) comprises comparing values of the bilinear map (e) calculated with variables comprising the sender private key (Prv_{Sender}) and the master public key of the Trusted Centre (g_{Pub}).
3. The method of claim 1 or claim 2, wherein the public parameters (PK) are verified if: $e(g_{Pub}, Prv_{(Sender,2)}) = e(H_1(Id_{TC}), H_2(Id_{Sender}))$.
4. The method of any one of claims 1 to 3, wherein the sender private key Prv_{Sender} and master public key of the Trusted Centre (g_{Pub}) are provided by the Trusted Centre (TC).
5. The method of any one of claims 1 to 4, wherein the Trusted Centre (TC) can decide to be separated in a plurality of Trusted Centers avoiding any key escrow (as shown in FIG. 10).

6. The method of any one of claims 1 to 5, wherein the Trusted Centre (TC) is separated in two Trusted Centre (TC_1) and ($TC_{(-1)}$) with master secret key (s_1) and ($s_{(-1)}$) and the private keys (Prv_{Id}) are computed through a protocol between the Trusted Centre ($TC_1, TC_{(-1)}$) and the user with identity (Id) as followed:

- at each Trusted Centre (TC_i):
 - computing $A_i = H_1(Id_{TC})^{s_i}$, $B_i = H_2(Id_{TC})^{s_i^{-1}}$;
 - transmitting privately A_i , B_i to TC_{-i} ;
 - publishing A_i ;
 - receiving A_{-i} , B_{-i} ;
 - verifying if $e(A_{-i}, B_{-i}) = e(H_1(Id_{TC}), H_2(Id_{TC}))$ and $A_{-i} \neq H_1(Id_{TC})$;
 - computing the master public key of (TC) as $g_{Pub} = A_{-i}^{s_i}$; and/or
- new request of private key, at a Trusted Centre (TC_i): if the request from the requestor contains an identifier (Id) identifying the requestor, verifying that this identifier has not been requested, generating a private key (Prv_{Id}) based on the identifier (Id) and the secret master key (s_i) and transmitting securely the private key (Prv_{Id}) to the requestor over the network system; whereby all next transmissions preferably does not need to be secured; and/or
- at requestor with identity string (Id):
 - receiving the private key ($Prv_{Id,1}, Prv_{Id,2}$);
 - picking a random number (a) in $\mathbb{Z}$;
 - computing $(HPK_1, HPK_2) = (Prv_{Id,1}^{a^{-1}}, Prv_{Id,2}^{a^{-1}})$ and $T = H_2(Id)^{a^{-1}}$;

- transmitting (Id, HPK_1, HPK_2, T) to the second Trusted Centre (TC_{-i}) ; and/or
 - at the second Trusted Centre (TC_{-i}) :
 - identifying the requestor with the identity string (Id) ;
 - verifying that this identifier has not been requested;
 - verifying that $e(H_1(Id), HPK_2) = e(HPK_1, H_2(Id))$ and $e(A_i, HPK_2) = e(H_1(Id_{TC}), T)$;
 - computing $(HK_1, HK_2) = (HPK_1^{s^{-1}}, HPK_2^{s^{-1}})$;
 - transmitting (HK_1, HK_2) to the requestor over the network; and/or
 - at the requestor:
 - receiving (HK_1, HK_2) ;
 - computing $Prv_{Id} = (HK_1^a, HK_2^a)$.
7. The method of any one of claims 1 to 6, wherein the public parameters (PK) further include a description of the groups (G_1, G_2, G_T) , a description of cryptographic hash functions (H_1, H_2, H_3, H_T) , a symmetric key encryption function (ϵ) , and a description of the bilinear map (also called pairing) (e) which takes as input one element from (G_1) and one element of (G_2) and output an element from (G_T) and that verifies the properties of a non-degenerated bilinear map.
8. The method of any one of claims 1 to 7, wherein the ciphertext (C) includes an authentication component (Y) for authenticating the sender once the ciphertext (C) is received by the recipient.
9. The method of claim 8, wherein the authentication component (Y) is based on the sender private key (Prv_{Sender}) and the identity string of the recipient $(Id_{Recipient})$, and wherein the recipient is operable to verify the sender using

the public parameters (PK), the sender identity string (Id_{Sender}) and a recipient private key ($Prv_{\text{Recipient}}$) obtained from the Trusted Centre (TC).

10. The method of any one of claims 1 to 9, wherein the sender can specify an expiry date for the master public key of the Trusted Centre (g_{Pub}), whereby after the expiry date, the recipient is forced to authenticate with the Trusted Centre (TC) to obtain a new recipient private key ($Prv_{\text{Recipient}}$).
11. The method of any one of claims 1 to 10, wherein the sender can specify a descriptive string to append to the TC identity string (Id_{TC}), whereby the descriptive string is used by the Trusted Centre (TC) to require additional levels of authentication from the recipient in order for the Trusted Centre (TC) to provide a recipient private key ($Prv_{\text{Recipient}}$) to the recipient.
12. The method of claim 11, wherein the descriptive string is selected from the group consisting of: a revocation number, a role of the recipient, an age of the recipient, a location of the recipient and/or an expiry date.
13. The method of any one of claims 1 to 12, wherein the plaintext message (M) is a conventional encryption key.
14. A method for using verifiable identity based encryption (VIBE) in a network system between a sender having a sender identity string (Id_{Sender}) and a recipient having a recipient identity string ($Id_{\text{Recipient}}$), the method comprising:
 - at the sender:
 - identifying a Trusted Centre (TC) by a TC identity string (Id_{TC}), the Trusted Centre having a master public key of the Trusted Centre (g_{Pub}) based on the Trusted Centre identity string (Id_{TC});
 - determining if the sender has a sender private key (Prv_{Sender}) and a plurality of public parameters (PK) for the Trusted Centre (TC), the public parameters (PK) including the master public key (g_{Pub}) of the Trusted Centre (TC) and a bilinear map (e);
 - verifying the public parameters (PK) of the Trusted Centre (TC) using the Trusted Centre identity string (Id_{TC}) prior to encrypting a plaintext message (M);
 - identifying the recipient by an identity string ($Id_{\text{Recipient}}$);

- hashing the identity string of the recipient ($Id_{\text{Recipient}}$) using the hash functions lying in the public parameters (PK);
 - encrypting the plaintext message (M) as ciphertext (C) using the public parameters (PK), a random symmetric key (Σ) and the hash of the identity string of the recipient ($Id_{\text{Recipient}}$);
 - transmitting (C) to the recipient over the network; and/or
 - at the recipient:
 - receiving the ciphertext (C) from the sender over the network system;
 - determining if the recipient has a recipient private key ($Prv_{\text{Recipient}}$) and the public parameters (PK) for the Trusted Centre (TC);
 - decrypting the first part of the ciphertext (C) (e.g. U, V) to obtain the symmetric key (Σ) using the public parameters (PK) and the recipient private key ($Prv_{\text{Recipient}}$);
 - decrypting the second part of the ciphertext (C) (e.g. W the same as in the algorithm **Auth-Decrypt**) to obtain the plaintext message (M) using the decryption algorithm (ϵ) and the symmetric key (Σ).
15. The method of claim 14, wherein the method further comprises, at the recipient, verifying the identity of the sender using the ciphertext (C), the public parameters (PK), the sender identity string (Id_{Sender}) and the recipient private key ($Prv_{\text{Recipient}}$).
16. A method of verifying a plurality of public parameters (PK) from a Trusted Centre (TC) in an identity based encryption system prior to encrypting a plaintext message (M) by a sender having a sender identity string (Id_{Sender}), the method comprising:
- identifying the Trusted Centre (TC) by a Trusted Centre identity string (Id_{TC}), the Trusted Centre having a master public key (g_{Pub}) based on the Trusted Centre identity string (Id_{TC});
 - determining if the sender has a sender private key (Prv_{Sender}) and the plurality of public parameters (PK) for the Trusted Centre (TC), the public parameters (PK) including the master public key of the Trusted Centre (g_{Pub}) and a bilinear map (e).
 - verifying the public parameters (PK) of the Trusted Centre (TC) using the Trusted Centre identity string (Id_{TC}) prior to encrypting the plaintext message (M) by comparing values of the bilinear map (e) calculated

with variables comprising the sender private key ($\text{Prv}_{\text{Sender}}$) and the master public key of the Trusted Centre (g_{Pub}).

17. A system for sending an encrypted message over a network using Identity-Based Encryption, the system comprising:
 - a Trusted Centre (TC) having a Trusted Centre identity string (Id_{TC}), a sender having a sender identity string ($\text{Id}_{\text{Sender}}$), and a recipient having a recipient identity string ($\text{Id}_{\text{Recipient}}$);
 - wherein the Trusted Centre (TC) has a first memory and one or more configured for:
 - generating a plurality of public parameters (PK) and a secret master key (s) from a security parameter (λ), the public parameters (PK) including a bilinear map (e) and a master public key of the Trusted Centre (g_{Pub}) based on the Trusted Centre identity string (Id_{TC});
 - receiving a request from a requestor;
 - if the request from the requestor contains an identifier (Id) identifying the requestor, generating a private key (Prv_{Id}) based on the identifier (Id) and the secret master key (s) and transmitting the private key (Prv_{Id}) to the requestor over the network system;
 - if the request from the requestor includes a request for the public parameters (PK), transmitting the public parameters (PK) to the requestor over the network system;
 - wherein the sender has a second memory and one or more processors configured for:
 - identifying the Trusted Centre (TC) by the Trusted Centre identity string (Id_{TC});
 - determining if the sender has a sender private key ($\text{Prv}_{\text{Sender}}$) and the public parameters (PK) for the Trusted Centre (TC);
 - verifying the public parameters (PK) of the Trusted Centre (TC) using the Trusted Centre identity string (Id_{TC}) prior to encrypting a plaintext message (M);
 - identifying the recipient by the recipient identity string ($\text{Id}_{\text{Recipient}}$);
 - hashing the identity string of the recipient ($\text{Id}_{\text{Recipient}}$) using the hash functions lying in the public parameters (PK);
 - encrypting the plaintext message (M) as ciphertext (C) using the public parameters (PK), a random symmetric key (Σ) and the hash of the identity string of the recipient ($\text{Id}_{\text{Recipient}}$);

- transmitting (C) to the recipient over the network;
 - wherein the recipient has a third memory and one or more processors configured for:
 - receiving the ciphertext (C) from the sender over the network system;
 - determining if the recipient has a recipient private key $\text{Prv}_{\text{Recipient}}$ and the public parameters (PK) for the Trusted Centre (TC);
 - decrypting the first part of the ciphertext (C) (e.g. U, V) to obtain the symmetric key (Σ) using the public parameters (PK) and the recipient private key ($\text{Prv}_{\text{Recipient}}$);
 - decrypting the second part of the ciphertext (C) (e.g. W) to obtain the plaintext message (M) using the decryption algorithm (ϵ) and the symmetric key (Σ).
18. The system of claim 17, wherein the plurality of public parameters (PK) further include a description of the groups (G_1, G_2, G_T), a description of cryptographic hash functions (H_1, H_2, H_3, H_T), a symmetric key encryption function (ϵ), and a description of the bilinear map (also called pairing) (e) which takes as input one element from (G_1) and one element of (G_2) and output an element from (G_T) and that verifies the properties of a non-degenerated bilinear map.
19. A computer program product comprising a computer readable memory storing computer executable instructions thereon that, when executed by a computer, perform the method steps of:
- identifying a Trusted Centre (TC) by a TC identity string (Id_{TC}), the Trusted Centre having a master public (g_{Pub}) based on the TC identity string (Id_{TC});
 - determining if a sender has a sender private key ($\text{Prv}_{\text{Sender}}$) and a plurality of public parameters (PK) for the Trusted Centre (TC), the public parameters (PK) including the master public key of the Trusted Centre (g_{Pub}) and a bilinear map (e);
 - verifying the public parameters (PK) of the Trusted Centre (TC) using the Trusted Centre identity string (Id_{TC}) prior to encrypting a plaintext message (M);
 - identifying a recipient by a recipient identity string ($\text{Id}_{\text{Recipient}}$);
 - hashing the identity of the recipient ($\text{Id}_{\text{Recipient}}$);

- encrypting the plaintext message (M) as ciphertext (C) using the public parameters (PK) a random symmetric key (Σ) and the hash of the identity of the recipient;
- transmitting the ciphertext (C) to the recipient over a network.