CLAIMS:

1. A method of generating a common session key SK_{ij} for encoding digital communications between a first device and a second device, comprising:

generating, by a secure server, a private key sk_i for the first device wherein the private key sk_i comprises a Discrete-Logarithm type digital signature, $[R_i, s_i]$, of an identity of the first device, id_i, and generating, by the secure server, a private key sk_j for the second device wherein the private key sk_j comprises a Discrete-Logarithm type digital signature, $[R_j, s_j]$, of an identity of the second device, id_j, wherein R_i and R_j are group elements, and s_i and s_j comprise integers modulo q, whereby q is a prime number, wherein the private key sk_i is communicated to the first device and the private key sk_j is communicated to the second device;

sharing, by the first device, a cryptographic nonce N_i, the identity of the first device id_i, and R_i with the second device;

calculating, by the second device, an implicitly shared secret k_{ji} using the shared R_i, where g is a generator of a cyclic group G, and providing the implicitly shared secret k_{ji}, the cryptographic nonce N_i, and a cryptographic nonce N_j to an Authentication Data Deriving Function to generate an authentication data Ad_j;

sharing, by the second device, the cryptographic nonce N_j, the identity of the second device id_j, R_j, and the authentication data Ad_j with the first device; and

calculating, by the first device, an implicitly shared secret k_{ij} using the shared R_j and verifying the authentication data Ad_j using the implicitly shared secret k_{ij}, the cryptographic nonce N_i, and the cryptographic nonce N_j, wherein if the authentication data Ad_j is verified, generating the common session key SK_{ij} by providing the implicitly shared secret k_{ij}, the cryptographic nonce N_i, the cryptographic nonce N_j, the identity of the first device id_i and the identity of the second device id_j to a Key Deriving Function;

providing, by the first device, the implicitly shared secret k_{ij}, the cryptographic nonce N_i, and the cryptographic nonce N_j to the Authentication Data Deriving Function to generate an authentication data Ad_i, and communicating the authentication data Ad_i to the second device; and

verifying, by the second device, the authentication data Ad_i using the implicitly shared secret k_{ji}, wherein if the authentication data Ad_i is verified, providing the implicitly shared

secret k_{ji}, the cryptographic nonce N_i, the cryptographic nonce N_j, the identity of the first device id_i and the identity of the second device id_j to the Key Deriving Function to generate the common session key SK_{ij}.

2. The method according to claim 1 wherein the generation of the authentication data Ad_j further comprises providing the identity of the first device id_i and the identity of the second device id_j to the Authentication Data Deriving Function.

3. The method according to any one of claims 1 or 2 wherein the generation of the authentication data Ad_i further comprises providing the identity of the first device id_i and the identity of the second device id_j to the Authentication Data Deriving Function.

4. The method according to any one of claims 1 to 3 wherein the verifying the authentication data Ad_j comprises:

providing the implicitly shared secret k_{ij}, the cryptographic nonce N_i, and the cryptographic nonce N_j to the Authentication Data Deriving Function to obtain a result, and determining if the result matches with authentication data Ad_j, whereby if a match is found, verifying the authentication data Ad_j.

5. The method according to any one of claims 1 to 4 wherein the verifying the authentication data Ad_i comprises:

providing the implicitly shared secret k_{ji}, the cryptographic nonce N_i, and the cryptographic nonce N_j to the Authentication Data Deriving Function to obtain a result, and determining if the result matches with authentication data Ad_i, whereby if a match is found, verifying the authentication data Ad_i.

6. The method according to claim 1 wherein the cryptographic nonce N_i comprises g^a where a is a random number.

7. The method according to claim 1 or 6 wherein the cryptographic nonce N_j comprises g^b where b is a random number.

8. The method according to any one of claims 1 to 7 wherein the Authentication Data Deriving Function comprises a Message Authentication Code (MAC) function.

9. The method according to any one of claims 1 to 8 wherein the Key Deriving Function comprises a collision- resistant hash function.

10. The method according to any one of claims 1 to 9 wherein the private key sk_i is a Schnorr signature of the identity of the first device, id_i, where $R_i = g^{r_i}$, and $s_i = r_i + xH(R_i, id_i)$ *(modulo q)*, and wherein the private key sk_j is a Schnorr signature of the identity of the second device, id_j, where $R_j = g^{r_j}$ and $s_j = r_j + xH(R_j, id_j)$ *(modulo q)*, where r_i and r_j are random numbers, x is a master secret key, and $H()$ is a collision-resistant hash function, and

wherein the implicitly shared secret $k_{ji}=g^{si \cdot sj}$, and the implicitly shared secret $k_{ij}=g^{sj \cdot si}$, where g is a generator of a cyclic group G .

11. The method according to any one of claims 1 to 9 wherein the private key sk_i is a first variant of an ElGamal signature of the identity of the first device, id_i, where $R_i = g^{r_i}$, and $s_i = x^{-1} \cdot (H(id_i) - r_i \cdot R_i)$ *(modulo q)*, and wherein the private key sk_j is a first variant of an ElGamal signature of the identity of the second device, id_j, where $R_j = g^{r_j}$ and $s_j = x^{-1} \cdot (H(id_j) - r_j \cdot R_j)$ *(modulo q)*, where r_i and r_j are random numbers, x is a master secret key, $H()$ is a collision-resistant hash function and,

wherein the implicitly shared secret $k_{ji} = y^{si \cdot sj}$, and the implicitly shared secret $k_{ij} = y^{sj \cdot si}$, where $y = g^x$ is master public key, and where g is a generator of a cyclic group G.

12. The method according to any one of claims 1 to 9 wherein the private key sk_i is a second variant of an ElGamal signature of the identity of the first device, id_i, where $R_i = g^{r_i}$, and $s_i = xR_i + r_i \cdot H(id_i)$ *(modulo q)*, and wherein the private key sk_j is a second variant of an ElGamal signature of the identity of the second device, id_j, where $R_j = g^{r_j}$ and $s_j = xR_j +$

$r_j \cdot H(id_j)$ *(modulo q)*, where r_i and r_j are random numbers, *x* is a master secret key, and *H*() is a collision-resistant hash function and,

wherein the implicitly shared secret $k_{ji}=g^{si \cdot sj}$, and the implicitly shared secret $k_{ij}=g^{sj \cdot si}$, where g is a generator of a cyclic group G .

13. The method according to any one of claims 1-9 wherein the private key sk_i is a third variant of an ElGamal signature of the identity of the first device, id_i, where $R_i = g^{r_i}$, and $s_i = x \cdot H(id_i) + r_i \cdot R_i$ *(modulo q)*, and wherein the private key sk_j is a third variant of an ElGamal signature of the identity of the second device, id_j, where $R_j = g^{r_j}$ and $s_j = x \cdot H(id_j) + r_j \cdot R_j$ *(modulo q)*, where r_i and r_j are random numbers, *x* is a master secret key, and *H*() is a collision-resistant hash function and,

wherein the implicitly shared secret $k_{ji}=g^{si \cdot sj}$, and the implicitly shared secret $k_{ij}=g^{sj \cdot si}$, where g is a generator of a cyclic group G .

14. The method according to any one of claims 1 to 9 wherein the private key sk_i is a fourth variant of an ElGamal signature of the identity of the first device, id_i, where $R_i = g^{r_i}$, and $s_i = x^{-1} \cdot (R_i - r_i \cdot H(id_i))$ *(modulo q)*, and wherein the private key sk_j is a fourth variant of an ElGamal signature of the identity of the second device, id_j, where $R_j = g^{r_j}$ and $s_j = x^{-1} \cdot (R_j - r_j \cdot H(id_j))$ *(modulo q)*, where r_i and r_j are random numbers, *x* is a master secret key, and *H*() is a collision-resistant hash function and,

wherein the implicitly shared secret $k_{ji} = y^{si \cdot sj}$, and the implicitly shared secret $k_{ij} = y^{sj \cdot si}$, where $y = g^x$ is master public key, and where g is a generator of a cyclic group G .

15. A method of generating a common session key SK_{ij} for encoding digital communications between a first device and a second device, comprising:

generating, by a secure server, a private key sk_i for the first device wherein the private key sk_i comprises a Discrete-Logarithm type digital signature, $[R_i, s_i]$, of an identity of the first device, id_i, and generating, by the secure server, a private key sk_j for the second device wherein the private key sk_j comprises a Discrete-Logarithm type digital signature, $[R_j, s_j]$, of an identity of the second device, id_j, wherein R_i and R_j are group elements, and s_i and s_j comprise integers modulo q, whereby q is a prime number, wherein the private key sk_i is

communicated to the first device and the private key sk_j is communicated to the second device;

sharing, by the first device, a cryptographic nonce N_i, the identity of the first device id_i, and R_i with the second device;

calculating, by the second device, an implicitly shared secret $k_{ji}=g^{si \cdot sj}$, using the shared R_i, where g is a generator of a cyclic group G, and calculating a common session key SK_{ji} by providing the implicitly shared secret k_{ji}, the cryptographic nonce N_i, the cryptographic nonce N_j, the identity of the first device id_i and the identity of the second device id_j to the Key Deriving Function, and providing the common session key SK_{ji}, the cryptographic nonce N_i, and a cryptographic nonce N_j to an Authentication Data Deriving Function to generate an authentication data Ad_j;

sharing, by the second device, the cryptographic nonce N_j, the identity of the second device id_j, R_j, and the authentication data Ad_j with the first device; and

calculating, by the first device, an implicitly shared secret $k_{ij}=g^{sj \cdot si}$, using the shared R_j, and calculating a common session key SK_{ij} by providing the implicitly shared secret k_{ij}, the cryptographic nonce N_i, the cryptographic nonce N_j, the identity of the first device id_i and the identity of the second device id_j to the Key Deriving Function and verifying the authentication data Ad_j using the common session key SK_{ij}, the cryptographic nonce N_i, and the cryptographic nonce N_j, wherein if the authentication data Ad_j is verified, using the common session key SK_{ij} or SK_{ji} as the common session key for encoding digital communications between a first device and a second device.

16. A system for generating a common session key SK_{ij} for encoding digital communications between a first device and a second device, comprising:

a secure server configured to share a private key sk_i for the first device wherein the private key sk_i comprises a Discrete-Logarithm type digital signature, $[R_i, s_i]$, of an identity of the first device, id_i, and generating, by the secure server, a private key sk_j for the second device wherein the private key sk_j comprises a Discrete-Logarithm type digital signature, $[R_j, s_j]$, of an identity of the second device, id_j, wherein R_i and R_j are group elements, and s_i and s_j comprise integers modulo q, whereby q is a prime number, wherein the private key sk_i is communicated to the first device and the private key sk_j is communicated to the second device;

the first device configured to share a cryptographic nonce N_i, the identity of the first device id_i, and R_i with the second device;

the second device configured to calculate an implicitly shared secret k_{ji} using the shared R_i, and providing the implicitly shared secret k_{ji}, the cryptographic nonce N_i, and a cryptographic nonce N_j to an Authentication Data Deriving Function to generate an authentication data Ad_j;

the second device configured to share the cryptographic nonce N_j, the identity of the second device id_j, R_j, and the authentication data Ad_j with the first device; and

the first device configured to calculate the implicitly shared secret $k_{ij}=g^{sj \cdot si}$, using the shared R_j and verifying the authentication data Ad_j using the implicitly shared secret k_{ij}, the cryptographic nonce N_i, and the cryptographic nonce N_j, wherein if the authentication data Ad_j is verified, generating the common session key SK_{ij} by providing the implicitly shared secret k_{ij}, the cryptographic nonce N_i, the cryptographic nonce N_j, the identity of the first device id_i and the identity of the second device id_j to a Key Deriving Function,

wherein the first device is configured to provide the implicitly shared secret k_{ij}, the cryptographic nonce N_i, and the cryptographic nonce N_j to the Authentication Data Deriving Function to generate an authentication data Ad_i, and communicating the authentication data Ad_i to the second device; and wherein the second device is configured to verify the authentication data Ad_i using the implicitly shared secret k_{ji}, wherein if the authentication data Ad_i is verified, providing the implicitly shared secret k_{ji}, the cryptographic nonce N_i, the cryptographic nonce N_j, the identity of the first device id_i and the identity of the second device id_j to the Key Deriving Function to generate the common session key SK_{ij}.

17. The system according to claim 16 wherein the generation of the authentication data Ad_j further comprises providing the identity of the first device id_i and the identity of the second device id_j to the Authentication Data Deriving Function.

18. The system according to any one of claims 16 or 17 wherein the generation of the authentication data Ad_i further comprises providing the identity of the first device id_i and the identity of the second device id_j to the Authentication Data Deriving Function.

19. The system according to any one of claims 16 to 18 wherein the verifying the authentication data Ad_j comprises:

providing the implicitly shared secret k_{ij}, the cryptographic nonce N_i, and the cryptographic nonce N_j to the Authentication Data Deriving Function to obtain a result, and determining if the result matches with authentication data Ad_j, whereby if a match is found, verifying the authentication data Ad_j.

20. The system according to any one of claims 16 to 19 wherein the verifying the authentication data Ad_i comprises:

providing the implicitly shared secret k_{ji}, the cryptographic nonce N_i, and the cryptographic nonce N_j to the Authentication Data Deriving Function to obtain a result, and determining if the result matches with authentication data Ad_i, whereby if a match is found, verifying the authentication data Ad_i.

21. The system according to claim 16 wherein the cryptographic nonce N_i comprises g^a where a is a random number.

22. The system according to claim 16 or 21 wherein the cryptographic nonce N_j comprises g^b where b is a random number.

23. The system according to any one of claims 16 to 22 wherein the Authentication Data Deriving Function comprises a Message Authentication Code (MAC) function.

24. The system according to any one of claims 16 to 23 wherein the Key Deriving Function comprises a collision- resistant hash function.

25. The system according to any one of claims 16 to 24 wherein the private key sk_i is a Schnorr signature of the identity of the first device, id_i, where $R_i = g^{r_i}$, and $s_i = r_i + xH(R_i, id_i)$ *(modulo q)*, and wherein the private key sk_j is a Schnorr signature of the identity of the

second device, id_j, where $R_j = g^{r_j}$ and $s_j = r_j + xH(R_j, id_j)$ *(modulo q)*, where r_i and r_j are random numbers, x is a master secret key, and $H()$ is a collision-resistant hash function and,

wherein the implicitly shared secret $k_{ji}=g^{si \cdot sj}$, and the implicitly shared secret $k_{ij}=g^{sj \cdot si}$, where g is a generator of a cyclic group G.

26. The system according to any one of claims 16 to 24 wherein the private key sk_i is a first variant of an ElGamal signature of the identity of the first device, id_i, where $R_i = g^{r_i}$, and $s_i = x^{-1} \cdot (H(id_i) - r_i \cdot R_i)$ *(modulo q)*, and wherein the private key sk_j is a first variant of an ElGamal signature of the identity of the second device, id_j, where $R_j = g^{r_j}$ and $s_j = x^{-1} \cdot (H(id_j) - r_j \cdot R_j)$ *(modulo q)*, where r_i and r_j are random numbers, x is a master secret key, $H()$ is a collision-resistant hash function and,

wherein the implicitly shared secret $k_{ji} = y^{si \cdot sj}$, and the implicitly shared secret $k_{ij} = y^{sj \cdot si}$, where $y = g^x$ is master public key, and where g is a generator of a cyclic group G.

27. The system according to any one of claims 16 to 24 wherein the private key sk_i is a second variant of an ElGamal signature of the identity of the first device, id_i, where $R_i = g^{r_i}$, and $s_i = xR_i + r_i \cdot H(id_i)$ *(modulo q)*, and wherein the private key sk_j is a second variant of an ElGamal signature of the identity of the second device, id_j, where $R_j = g^{r_j}$ and $s_j = xR_j + r_j \cdot H(id_j)$ *(modulo q)*, where r_i and r_j are random numbers, x is a master secret key, and $H()$ is a collision-resistant hash function and,

wherein the implicitly shared secret $k_{ji}=g^{si \cdot sj}$, and the implicitly shared secret $k_{ij}=g^{sj \cdot si}$, where g is a generator of a cyclic group G.

28. The system according to any one of claims 16 to 24 wherein the private key sk_i is a third variant of an ElGamal signature of the identity of the first device, id_i, where $R_i = g^{r_i}$, and $s_i = x \cdot H(id_i) + r_i \cdot R_i$ *(modulo q)*, and wherein the private key sk_j is a third variant of an ElGamal signature of the identity of the second device, id_j, where $R_j = g^{r_j}$ and $s_j = x \cdot H(id_j) + r_j \cdot R_j$ *(modulo q)*, where r_i and r_j are random numbers, x is a master secret key, and $H()$ is a collision-resistant hash function and,

wherein the implicitly shared secret $k_{ji}=g^{si \cdot sj}$, and the implicitly shared secret $k_{ij}=g^{sj \cdot si}$, where g is a generator of a cyclic group G.

29. The system according to any one of claims 16 to 24 wherein the private key sk_i is a fourth variant of an ElGamal signature of the identity of the first device, id_i, where $R_i = g^{r_i}$, and $s_i = x^{-1} \cdot (R_i - r_i \cdot H(id_i)) \ (modulo\ q)$, and wherein the private key sk_j is a fourth variant of an ElGamal signature of the identity of the second device, id_j, where $R_j = g^{r_j}$ and $s_j = x^{-1} \cdot (R_j - r_j \cdot H(id_j)) \ (modulo\ q)$, where r_i and r_j are random numbers, x is a master secret key, and $H()$ is a collision-resistant hash function and,

wherein the implicitly shared secret $k_{ji} = y^{si \cdot sj}$, and the implicitly shared secret $k_{ij} = y^{sj \cdot si}$, where $y = g^x$ is master public key, and where g is a generator of a cyclic group G.

30. A system for generating a common session key SK_{ij} for encoding digital communications between a first device and a second device, comprising:

a secure server configured to generate a private key sk_i for the first device wherein the private key sk_i comprises a Discrete-Logarithm type digital signature, $[R_i, s_i]$, of an identity of the first device, id_i, and generating, by the secure server, a private key sk_j for the second device wherein the private key sk_j comprises a Discrete-Logarithm type digital signature, $[R_j, s_j]$, of an identity of the second device, id_j, wherein R_i and R_j are group elements, and s_i and s_j comprise integers modulo q, whereby q is a prime number, wherein the private key sk_i is communicated to the first device and the private key sk_j is communicated to the second device;

the first device configured to share a cryptographic nonce N_i, the identity of the first device id_i, and R_i with the second device;

the second device configured to calculate an implicitly shared secret $k_{ji}=g^{si \cdot sj}$, using the shared R_i, where g is a generator of a cyclic group G, and calculating a common session key SK_{ji} by providing the implicitly shared secret k_{ji}, the cryptographic nonce N_i, the cryptographic nonce N_j, the identity of the first device id_i and the identity of the second device id_j to the Key Deriving Function, and providing the common session key SK_{ji}, the cryptographic nonce N_i, and a cryptographic nonce N_j to an Authentication Data Deriving Function to generate an authentication data Ad_j;

the second device configured to share the cryptographic nonce N_j, the identity of the second device id_j, R_j, and the authentication data Ad_j with the first device; and

the first device configured to calculate an implicitly shared secret $k_{ij}=g^{sj \cdot si}$, using the shared R_j, and calculating a common session key SK_{ij} by providing the implicitly shared secret k_{ij}, the cryptographic nonce N_i, the cryptographic nonce N_j, the identity of the first device id_i and the identity of the second device id_j to the Key Deriving Function and verifying the authentication data Ad_j using the common session key SK_{ij}, the cryptographic nonce N_i, and the cryptographic nonce N_j, wherein if the authentication data Ad_j is verified, using the common session key SK_{ij} or SK_{ji} as the common session key for encoding digital communications between a first device and a second device.