

What is claimed is:

1. A method of key agreement over an air link of a wireless communication system, the method comprising:
 - at a mobile station, receiving a first message from a base station, including a random NONCE wherein said random NONCE is a number or bit string used only once in a message for a security purpose;
 - computing a permutation of a mobile station identification (MSID*);
 - sending a second message including a mobile station random NONCE, the base station random NONCE and a first integrity check value (ICV);
 - receiving at said mobile station a third message including a mobile station NONCE, the base station random NONCE and a second ICV;
 - receiving at said mobile station a third message including a mobile station NONCE, the base station random NONCE and a second ICV if the base station verified the first ICV;
 - verifying the second ICV; and
 - sending a fourth message including mobile station identification in a secure link.
2. The method of claim 1, wherein calculating said permutation of said mobile station identification comprises:
 - computing said MSID* according to
$$MSID^*=DOT16KDF(MSID|BSID|NONCE_BS,48)$$
wherein,
 - MSID is the mobile station identification (ID),
 - BSID is the base station ID,
 - NONCE_BS is the random NONCE of the base station and
 - DOT16KDF is a key derivation function to create a hashed permutation from the MSID, BSID and NONCE_BS.
3. The method of claim 2, comprising:
 - computing security keys according to:
$$Security_keys=DOT16KDF(Parentkey,MSID^*|XXX|YYY|,size),$$
wherein,
 - Parentkey is the parent key from which the keys are derived;
 - XXX is more parameters for a specific key such as, for example BSID;
 - YYY is a generic string which is defined per key;

- and size is the size of the key.
4. A method of key agreement over an air link of a wireless communication system, the method comprising:
- at a base station, sending a first message to a mobile station, including a first random NONCE wherein said random NONCE is a number or bit string used only once in a lifetime cycle of a key for a security purpose;
 - receiving a second message including a mobile station permuted identification (MSID*), a mobile station random NONCE, the base station random NONCE and a first integrity check value (ICV);
 - computing a plurality of security keys and verifying the first ICV;
 - sending a third message including said random NONCE of the base station, a random NONCE of the mobile station and a second ICV;
 - receiving a fourth message including a mobile station identification in a secure link; and
 - comparing calculated MSID** with the MSID* and establishing secure link based on the comparison.
5. The method of claim 4, wherein computing said plurality of security keys comprises: $\text{Security_keys} = \text{DOT16KDF}(\text{Parentkey}, \text{MSID}^* | \text{XXX} | \text{YYY}, \text{size})$, wherein, Parentkey is the parent key from which the keys are derived; XXX is more parameters for a specific key such as, for example BSID; YYY is a generic string which is defined per key; and size is of the key.
6. The method of claim 4, comprising:
- computing another permutation of the mobile station ID (MSID**) according to $\text{MSID}^{**} = \text{DOT16KDF}(\text{MSID} | \text{BSID} | \text{NONCE_BS}, 48)$
 - wherein,
 - MSID is the mobile station identification (ID),
 - BSID is the base station ID,
 - NONCE_BS is the NONCE of the base station and
 - DOT16KDF is a key derivation function to derive one or more security keys material from the MSID, BSID and NONCE_BS.
7. A mobile station comprising:

a receiver to receive a first message from a base station, including a random NONCE wherein said random NONCE is a number or bit string used only once in a lifetime cycle of a key for a security purpose;

a computing module to compute a permutation of a mobile station identification ($MSID^*$); and

a transmitter to send a second message including a mobile station random NONCE, the base station random NONCE and a first integrity check value (ICV) and to send a fourth message a mobile station identification in a secure link after receiving a third message including a mobile station NONCE, the base station random NONCE and a second ICV.

8. The mobile station of claim 7, wherein the computing module is to compute said $MSID^*$ according to $MSID^* = DOT16KDF(MSID|BSID|NONCE_BS, 48)$ wherein,
- $MSID$ is the mobile station identification (ID),
- $BSID$ is the base station ID,
- $NONCE_BS$ is the NONCE of the base station and
- $DOT16KDF$ is a key derivation function to derive one or more security keys from the $MSID$, $BSID$ and $NONCE_BS$.
9. The mobile station of claim 7, wherein the computing module is to compute security keys from $MSID^*$ and according to: $Security_Keys = DOT16KDF(Parentkey, MSID^*|XXX|YYY|size)$ wherein,
- $Parentkey$ is the parent key from which the keys are derived;
- XXX is more parameters for a specific key such as, for example $BSID$;
- YYY is a generic string which is defined per key;
- and $size$ is of the key.
10. The mobile station of claim 7 comprising:
- a multiple input multiple output (MIMO) transmitters receivers system operably coupled to a plurality of antennas wherein said MIMO transmitters receivers system includes at least said transmitter and at least said receiver.
11. The mobile station of claim 7 comprising:
- a modulator to modulate the first message and the third message according to an Orthogonal Frequency Division Multiple Access (OFDMA) modulation scheme; and

- a demodulator to demodulate the second and the fourth message according to said OFDMA modulation scheme.
12. The mobile station of claim 7 comprising:
- a modulator to modulate the first message and the third message according to a single carrier frequency division multiple access (SC-FDMA) modulation scheme; and
 - a demodulator to demodulate the second and the fourth message according to an Orthogonal Frequency Division Multiple Access (OFDMA) modulation scheme.
13. A base station comprising:
- a transmitter to send a first message to a mobile station, including a first random NONCE wherein said random NONCE is a number or bit string used only once in a lifetime of a key for a security purpose and to send a third message including said random NONCE of the base station, a random NONCE of the mobile station and a second ICV;
 - a receiver to receive a second message including a mobile station permuted identification (MSID*), a mobile station random NONCE, the base station random NONCE and a first integrity check value (ICV) and a fourth message including a mobile station identification in a secure link;
 - a computing module to compute plurality of security keys and to verify the first ICV of the second message; and
 - a comparator to compare calculated MSID* with the MSID* and to establish said secure link based on the comparison.
14. The base station of claim 13 wherein the computing module is to compute said plurality of security keys from said MSID* according to $\text{Security_keys} = \text{DOT16KDF}(\text{Parentkey}, \text{MSID*}|\text{XXX}|\text{YYY}, \text{size})$, wherein, Parentkey is the parent key from which the keys are derived; XXX is more parameters for a specific key such as, for example BSID; YYY is a generic string which is defined per key; and size is the key size.
15. The base station of claim 13 wherein the computing module is to compute another permutation of the mobile station ID (MSID**) according to $\text{MSID**} = \text{DOT16KDF}(\text{MSID}|\text{BSID}|\text{NONCE_BS}, 48)$

wherein,

MSID is the mobile station identification (ID),

BSID is the base station ID,

NONCE_BS is the NONCE of the base station and

DOT16KDF is a key derivation function to derive one or more security keys materials from the MSID, BSID and NONCE_BS.

16. The base station of claim 13 comprising:
 - a multiple input multiple output (MIMO) transmitters receivers system operably coupled to a plurality of antennas wherein said MIMO transmitters receivers system includes at least said transmitter and at least said receiver.
17. The base station of claim 13 comprising:
 - a modulator to modulate the first message and the third message according to an Orthogonal Frequency Division Multiple Access (OFDMA) modulation scheme; and
 - a demodulator to demodulate the second and the fourth message according to said OFDMA modulation scheme.
18. The base station of claim 13 comprising:
 - a modulator to modulate the first message and the third message according to an Orthogonal Frequency Division Multiple Access (OFDMA) modulation scheme; and
 - a demodulator to demodulate the second and the fourth message according to a single carrier frequency division multiple access (SC-FDMA) modulation scheme.
19. A wireless communication system comprising:
 - a mobile station and a base station wherein the mobile station comprises:
 - a receiver to receive a first message from a base station, said first message including a random NONCE, wherein said random NONCE is a number or bit string used only once in a lifetime cycle of a key for a security purpose;
 - a computing module to compute a permutation of a mobile station identification (MSID*); and
 - a transmitter to send a second message, said second message including a mobile station random NONCE, the base station random

NONCE and a first integrity check value (ICV) and to send a fourth message, said fourth message including a mobile station identification, in a secure link after receiving a third message including a mobile station NONCE, the base station random NONCE and a second ICV; and

the base station comprises:

a transmitter to send said first message and the third message to said mobile station;

a receiver to receive said second message said fourth message;

a computing module to compute a plurality of security keys and to verify the first ICV of the second message; and

a comparator to compare calculated MSID** with the MSID* and to establish said secure link based on the comparison.

20. The wireless communication system of claim 19 wherein the computing module of the mobile station is to calculate said MSID* according to

$MSID^* = DOT16KDF(MSID|BSID|NONCE_BS, 48)$

wherein,

MSID is the mobile station identification (ID),

BSID is the base station ID,

NONCE_BS is the NONCE of the base station and

DOT16KDF is a key derivation function to derive one or more security keys materials from the MSID, BSID and NONCE_BS.

21. The wireless communication system of claim 19 wherein the computing module of the mobile station is to compute security keys from MSID* and according to

$Security_keys = DOT16KDF(Parentkey, MSID^*|XXX|YYY, size)$, wherein,

Parentkey is the parent key from which the keys are derived;

XXX is more parameters for a specific key such as, for example BSID;

YYY is a generic string which is defined per key;

and size is of the key.

22. The wireless communication system of claim 19, the mobile station further comprising:

- a multiple input multiple output (MIMO) transmitters receivers system operably coupled to a plurality of antennas wherein said MIMO transmitters receivers system includes at least said transmitter and at least said receiver.
23. The wireless communication system of claim 19, the mobile station further comprising:
- a modulator to modulate the first message and the third message according to an Orthogonal Frequency Division Multiple Access (OFDMA) modulation scheme; and
 - a demodulator to demodulate the second and the fourth message according to said OFDMA modulation scheme.
24. The wireless communication system of claim 19, the mobile station further comprising:
- a modulator to modulate the first message and the third message according to a single carrier frequency division multiple access (SC-FDMA) modulation scheme; and
 - a demodulator to demodulate the second and the fourth message according to an Orthogonal Frequency Division Multiple Access (OFDMA) modulation scheme.
25. The wireless communication system of claim 19 wherein the computing module of the base station is to compute said plurality of security keys from said MSID* according to $\text{Security_keys} = \text{DOT16KDF}(\text{Parentkey}, \text{MSID}^* | \text{XXX} | \text{YYY}, \text{size})$, wherein,
- Parentkey is the parent key from which the keys are derived;
 - XXX is more parameters for a specific key such as, for example BSID;
 - YYY is a generic string which is defined per key;
 - and size is of the key.
26. The wireless communication system of claim 19 wherein the computing module of the base station to compute another of the mobile station ID (MSID**) according to $\text{MSID}^{**} = \text{DOT16KDF}(\text{MSID} | \text{BSID} | \text{NONCE_BS}, 48)$ wherein,
- MSID* is the mobile station identification (ID),
 - BSID is the base station ID,
 - NONCE_BS is the NONCE of the base station and

DOT16KDF is a key derivation function to derive one or more security keys from the MSID, BSID and NONCE_BS.

27. The wireless communication system of claim 19, the base station comprising:
 - a multiple input multiple output (MIMO) transmitters receivers system operably coupled to a plurality of antennas wherein said MIMO transmitters receivers system includes at least said transmitter and at least said receiver.
28. The wireless communication system of claim 19, the base station comprising:
 - a modulator to modulate the first message and the third message according to an Orthogonal Frequency Division Multiple Access (OFDMA) modulation scheme; and
 - a demodulator to demodulate the second and the fourth message according to said OFDMA modulation scheme.
29. The wireless communication system of claim 19, the base station comprising:
 - a modulator to modulate the first message and the third message according to an Orthogonal Frequency Division Multiple Access (OFDMA) modulation scheme; and
 - a demodulator to demodulate the second and the fourth message according to a single carrier frequency division multiple access (SC-FDMA) modulation scheme.
30. A method of key agreement over an air link of a wireless communication system, the method comprising:
 - sending in an unsecure mode a permutation of a mobile station identification (MSID*);
 - establishing a secure link with a first set of keys derived from said permutation of a mobile station identification (MSID*);
 - sending over the established secured link mobile station identification (MSID).
31. The method of claim 30 comprising:
 - deriving a second set keys based on said MSID; and
 - communicating over the secure link using the second set of keys.
32. The method of claim 30, wherein calculating said permutation of said mobile station identification comprises:

computing said MSID* according to

$MSID^* = DOT16KDF(MSID|BSID|NONCE_BS, 48)$

wherein

MSID is the mobile station identification (ID),

BSID is the base station ID,

NONCE_BS is the random NONCE of the base station and

DOT16KDF is a key derivation function to create a hashed permutation from the MSID, BSID and NONCE_BS.

33. The method of claim 2, comprising:

computing security keys according to

$Security_keys = DOT16KDF(Parentkey, MSID^*|XXX|YYY, size)$, wherein,

Parentkey is the parent key from which the keys are derived;

XXX is more parameters for a specific key such as, for example BSID;

YYY is a generic string which is defined per key;

and size is the size of the key.

What is claimed is:

1. A method of key agreement over an air link of a wireless communication system, the method comprising:

at a mobile station, receiving a first message from a base station, including a random NONCE wherein said random NONCE is a number or bit string used only once in a message for a security purpose;

computing a permutation of a mobile station identification (MSID*), wherein the permutation is computed using said random NONCE;

computing security keys according to:

Security keys=DOT16KDF(Parentkey,MSID*|XXX|YYY|,size), wherein,

Parentkey is the parent key from which the keys are derived;

XXX is more parameters for a specific key such as, for example BSID;

YYY is a generic string which is defined per key;

and size is the size of the key;

sending a second message including a mobile station random NONCE, the base station random NONCE and a first integrity check value (ICV);

receiving at said mobile station a third message including a mobile station NONCE, the base station random NONCE and a second ICV if the base station verified the first ICV;

verifying the second ICV; and

sending a fourth message including mobile station identification in a secure link.

2. The method of claim 1, wherein computing said permutation of said mobile station identification comprises:

computing said MSID* according to

MSID*=DOT16KDF(MSID|BSID|NONCE_BS,48) wherein,

MSID is the mobile station identification (ID),

BSID is the base station ID,

NONCE_BS is the random NONCE of the base station and

DOT16KDF is a key derivation function to create a hashed permutation from the MSID, BSID and NONCE_BS.

3. A method of key agreement over an air link of a wireless communication system, the method comprising:

at a base station, sending a first message to a mobile station, including a first random NONCE wherein said random NONCE is a number or bit string used only once in a lifetime cycle of a key for a security purpose;

receiving a second message including a mobile station permuted identification (MSID*), a mobile station random NONCE, the base station random NONCE and a first integrity check value (ICV) , wherein the permutation is computed using said first random NONCE;

computing a plurality of security keys and verifying the first ICV, wherein computing said plurality of security keys comprises: Security keys=DOT16KDF(Parentkey,MSID*|XXX|YYY|,size), wherein,

Parentkey is the parent key from which the keys are derived;

XXX is more parameters for a specific key such as, for example BSID;

YYY is a generic string which is defined per key;

and size is of the key;

sending a third message including said random NONCE of the base station, a random NONCE of the mobile station and a second ICV;

receiving a fourth message including a mobile station identification in a secure link;
and

comparing calculated MSID** with the MSID* and establishing secure link based on the comparison.

4. The method of claim 3, comprising:

computing another permutation of the mobile station ID (MSID**) according to $MSID^{**} = \text{DOT16KDF}(MSID|BSID|NONCE_BS, 48)$ wherein,

MSID is the mobile station identification (ID),

BSID is the base station ID,

NONCE_BS is the NONCE of the base station and

DOT16KDF is a key derivation function to derive one or more security keys material from the MSID, BSID and NONCE_BS.

5. A mobile station comprising:

a receiver to receive a first message from a base station, including a random NONCE wherein said random NONCE is a number or bit string used only once in a lifetime cycle of a key for a security purpose;

a computing module to compute a permutation of a mobile station identification (MSID*), wherein the permutation is computed using said random NONCE, and wherein the computing module is to compute security keys from MSID* and according to:

$\text{Security Keys} = \text{DOT16KDF}(\text{Parentkey}, MSID^*|XXX|YYY|size)$ wherein,

Parentkey is the parent key from which the keys are derived;

XXX is more parameters for a specific key such as, for example BSID;

YYY is a generic string which is defined per key;

and size is of the key; and

a transmitter to send a second message including a mobile station random NONCE, the base station random NONCE and a first integrity check value (ICV) and to send a fourth message a mobile station identification in a secure link after receiving a third message

including a mobile station NONCE, the base station random NONCE and a second ICV.

6. The mobile station of claim 5, wherein the computing module is to compute said MSID * according to

$MSID^* = \text{DOT16KDF}(MSID|BSID|NONCE_BS, 48)$ wherein,

MSID is the mobile station identification (ID),

BSID is the base station ID,

NONCE_BS is the NONCE of the base station and

DOT16KDF is a key derivation function to derive one or more security keys from the MSID, BSID and NONCE_BS.

7. The mobile station of claim 5 comprising:

a multiple input multiple output (MIMO) transmitters receivers system operably coupled to a plurality of antennas wherein said MIMO transmitters receivers system includes at least said transmitter and at least said receiver.

8. The mobile station of claim 5 comprising:

a modulator to modulate the first message and the third message according to an Orthogonal Frequency Division Multiple Access (OFDMA) modulation scheme; and

a demodulator to demodulate the second and the fourth message according to said OFDMA modulation scheme.

9. The mobile station of claim 5 comprising:

a modulator to modulate the first message and the third message according to a single carrier frequency division multiple access (SC-FDMA) modulation scheme; and

a demodulator to demodulate the second and the fourth message according to an Orthogonal Frequency Division Multiple Access (OFDMA) modulation scheme.

10. A base station comprising:

a transmitter to send a first message to a mobile station, including a first random NONCE wherein said random NONCE is a number or bit string used only once in a lifetime of a key for a security purpose and to send a third message including said random NONCE of the base station, a random NONCE of the mobile station and a second ICV;

a receiver to receive a second message including a mobile station permuted identification (MSID*), wherein the mobile station permuted identification is computed using said first random NONCE, a mobile station random NONCE, the base station random NONCE and a first integrity check value (ICV) and a fourth message including a mobile station identification in a secure link;

a computing module to compute plurality of security keys and to verify the first ICV of the second message, wherein the computing module is to compute said plurality of security keys from said MSID* according to:

Security_keys=DOT16KDF(Parentkey,MSID*|XXX|YYY|size), wherein,

Parentkey is the parent key from which the keys are derived;

XXX is more parameters for a specific key such as, for example BSID;

YYY is a generic string which is defined per key;

and size is the key size; and

a comparator to compare calculated MSID** with the MSID* and to establish said secure link based on the comparison.

11. The base station of claim 10 wherein the computing module is to compute another permutation of the mobile station ID (MSID**) according to

MSID**=DOT16KDF(MSID|BSID|NONCE_BS,48) wherein,

MSID is the mobile station identification (ID),

BSID is the base station ID,

NONCE_BS is the NONCE of the base station and

DOT16KDF is a key derivation function to derive one or more security keys materials from the MSID, BSID and NONCE_BS.

12. The base station of claim 10 comprising:

a multiple input multiple output (MIMO) transmitters receivers system operably coupled to a plurality of antennas wherein said MIMO transmitters receivers system includes at least said transmitter and at least said receiver.

13. The base station of claim 10 comprising:

a modulator to modulate the first message and the third message according to an Orthogonal Frequency Division Multiple Access (OFDMA) modulation scheme; and

a demodulator to demodulate the second and the fourth message according to said OFDMA modulation scheme.

14. The base station of claim 10 comprising:

a modulator to modulate the first message and the third message according to an Orthogonal Frequency Division Multiple Access (OFDMA) modulation scheme; and

a demodulator to demodulate the second and the fourth message according to a single carrier frequency division multiple access (SC-FDMA) modulation scheme.

15. A wireless communication system comprising:

a mobile station and a base station wherein the mobile station comprises:

a receiver to receive a first message from a base station, said first message including a random NONCE, wherein said random NONCE is a number or bit string used only once in a lifetime cycle of a key for a security purpose;

a computing module to compute a permutation of a mobile station identification (MSID*), wherein the permutation is computed using said random NONCE, and wherein the computing module of the mobile station is to compute security keys from MSID* and according to

Security_keys=DOT16KDF(Parentkey,MSID*|XXX|YYY|,size), wherein,

Parentkey is the parent key from which the keys are derived;

XXX is more parameters for a specific key such as, for example BSID;

YYY is a generic string which is defined per key;

and size is of the key; and

a transmitter to send a second message, said second message including a mobile station random NONCE, the base station random NONCE and a first integrity check value (ICV) and to send a fourth message, said fourth message including a mobile station identification, in a secure link after receiving a third message including a mobile station NONCE, the base station random NONCE and a second ICV; and

the base station comprises:

a transmitter to send said first message and the third message to said mobile station;

a receiver to receive said second message said fourth message;

a computing module to compute a plurality of security keys and to verify the first ICV of the second message; and

a comparator to compare calculated MSID** with the MSID* and to establish said secure link based on the comparison.

16. The wireless communication system of claim 15 wherein the computing module of the mobile station is to calculate said MSID* according to

MSID*=DOT16KDF(MSID|BSID|NONCE_BS,48) wherein,

MSID is the mobile station identification (ID),

BSID is the base station ID,

NONCE_BS is the NONCE of the base station and

DOT16KDF is a key derivation function to derive one or more security keys materials from the MSID, BSID and NONCE_BS.

17. The wireless communication system of claim 15, the mobile station further comprising:

a multiple input multiple output (MIMO) transmitters receivers system operably coupled to a plurality of antennas wherein said MIMO transmitters receivers system includes at least said transmitter and at least said receiver.

18. The wireless communication system of claim 15, the mobile station further comprising:

a modulator to modulate the first message and the third message according to an Orthogonal Frequency Division Multiple Access (OFDMA) modulation scheme; and

a demodulator to demodulate the second and the fourth message according to said OFDMA modulation scheme.

19. The wireless communication system of claim 15, the mobile station further comprising:

a modulator to modulate the first message and the third message according to a single carrier frequency division multiple access (SC-FDMA) modulation scheme; and

a demodulator to demodulate the second and the fourth message according to an Orthogonal Frequency Division Multiple Access (OFDMA) modulation scheme.

20. The wireless communication system of claim 15 wherein the computing module of the base station is to compute said plurality of security keys from said MSID* according to $\text{Security_keys} = \text{DOT16KDF}(\text{Parentkey}, \text{MSID*}|\text{XXX}|\text{YYY}|, \text{size})$, wherein,

Parentkey is the parent key from which the keys are derived;

XXX is more parameters for a specific key such as, for example BSID;

YYY is a generic string which is defined per key;

and size is of the key.

21. The wireless communication system of claim 15 wherein the computing module of the base station to compute another of the mobile station ID (MSID**) according to

$\text{MSID**} = \text{DOT16KDF}(\text{MSID}|\text{BSID}|\text{NONCE_BS}, 48)$ wherein,

MSID* is the mobile station identification (ID),

BSID is the base station ID,

NONCE_BS is the NONCE of the base station and

DOT16KDF is a key derivation function to derive one or more security keys from the MSID, BSID and NONCE_BS.

22. The wireless communication system of claim 15, the base station comprising:

a multiple input multiple output (MIMO) transmitters receivers system operably coupled to a plurality of antennas wherein said MIMO transmitters receivers system includes at least said transmitter and at least said receiver.

23. The wireless communication system of claim 15, the base station comprising:

a modulator to modulate the first message and the third message according to an Orthogonal Frequency Division Multiple Access (OFDMA) modulation scheme; and

a demodulator to demodulate the second and the fourth message according to said OFDMA modulation scheme.

24. The wireless communication system of claim 15, the base station comprising:

a modulator to modulate the first message and the third message according to an Orthogonal Frequency Division Multiple Access (OFDMA) modulation scheme; and

a demodulator to demodulate the second and the fourth message according to a single carrier frequency division multiple access (SC-FDMA) modulation scheme.

25. A method of key agreement over an air link of a wireless communication system, the method comprising:

sending from a mobile station to a remote station in an unsecure mode a permutation of a mobile station identification (MSID*), wherein the permutation is computed using a random NONCE;

establishing a secure link between the mobile station and the remote station with a first set of keys derived from said permutation of a mobile station identification (MSID*), wherein the security keys are computed according to $\text{Security_keys} = \text{DOT16KDF}(\text{Parentkey}, \text{MSID}^* | \text{XXX} | \text{YYY}, \text{size})$, wherein, Parentkey is the parent key from which the keys are derived; XXX is more parameters for a specific key such as, for example BSID; YYY is a generic string which is defined per key; and size is the size of the key;

sending from the mobile station to the remote station over the established secured link mobile station identification (MSID).

26. The method of claim 25 comprising:

deriving a second set keys based on said MSID; and

communicating over the secure link using the second set of keys.

27. The method of claim 25, wherein calculating said permutation of said mobile station identification comprises:

computing said MSID* according to $\text{MSID}^* = \text{DOT16KDF}(\text{MSID} | \text{BSID} | \text{NONCE_BS}, 48)$ wherein,

MSID is the mobile station identification (ID),

BSID is the base station ID,

NONCE_BS is the random NONCE of the base station and

DOT16KDF is a key derivation function to create a hashed permutation from the MSID, BSID and NONCE_BS.