

generating (103) a list of temporary node identifiers on the basis of said list of node identifiers such that each of the plurality of nodes becomes identifiable by its respective temporary node identifier; and subsequently sending (105A) a first key generating file to the first node and also communicating (105B) a second key generating file to the virtual and temporary second node;

executing the virtual and temporary second node on the server and the virtual and temporary second node (22) thereby:

starting to process (106B) the second key generating file; and in response

generating (107B) a second intermediate data set;
receiving (108) a first intermediate data set from the first node;
comparing (109) bits of the first intermediate data set with corresponding bits of the second intermediate data set;

generating (110) a third intermediate data set based on the bit-by-bit comparison between the first intermediate data set and the second intermediate data set by setting a first value if the compared bits are equal and setting a second value if the compared bits are unequal;

sending (111) the third intermediate data set to the first node;

generating (113B) a second cryptographic key based on the bit by bit comparison between the first and the second intermediate data set by keeping the value of the bit of the second data set if the corresponding bit of the first intermediate data set is equal and ignoring the bit of the second intermediate data set if the compared bits are unequal;

setting up (114) communication channels between the first node and each of the plurality of other nodes, the virtual and temporary second node using the list of temporary node identifiers for identifying the respective nodes of the plurality of nodes to which communication channels are to be set up; in response to the respective communication channels having been set up

sending (115) the second cryptographic key to each of the plurality of other nodes for subsequent application by each of the plurality of other nodes during the communication sessions between the first node and each of the plurality of other nodes.

8. A computer program comprising instructions which, when executed on at least one processor of the server, cause the processor to carry out the method according to claim 7.

9. A carrier comprising the computer program according to claim 8, wherein the carrier is one of an electronic signal, an optical signal, a radio signal, or a computer readable storage medium.
- 5 10. A server (20) for establishing communication sessions between a first node and a plurality of other nodes, the server (20) comprising:
- a *transmitter* (1410);
 - a *receiver* (1410);
 - a *processor* (1420); and
 - 10 a *memory* (1430) storing computer program with instructions which, when executed on the *processor* (1420), cause the server (20) to:
 - receive, by means of the *receiver* (1410), a request message from the first node for requesting the establishment of secure communication sessions between the first node and a plurality of other nodes, the request message including a list
 - 15 of node identifiers wherein each of the node identifiers identifies a respective node of the plurality of other nodes;
 - in response to receiving said request message create a virtual and temporary second node, which is executable within said server;
 - generate a list of temporary node identifiers on the basis of said list of node identifiers such that each of the plurality of nodes becomes identifiable by
 - 20 its respective temporary node identifier; and subsequently
 - send, by means of the *transmitter* (1410), a first key generating file to the first node; and
 - communicate a second key generating file to the virtual and temporary
 - 25 second node;
 - execute the virtual and temporary second node on the server and the virtual and temporary second node thereby:
 - process the second key generating file; and in response
 - generate a second intermediate data set;
 - 30 receive, by means of the *receiver* (1410), a first intermediate data set from the first node;
 - compare bits of the first intermediate data set with the corresponding bits of the second intermediate data set;
 - generate a third intermediate data set based on the bit-by-bit
 - 35 comparison between the first intermediate data set and the second intermediate data set by setting a first value if the compared bits are equal and setting a second value if the compared bits are unequal;
 - send, by means of the *transmitter* (1410), the third intermediate data set to the first node;

receiving a second cryptographic key from the virtual and
 temporary second node, the second cryptographic key generated at the
 virtual and temporary second node based on a bit by bit comparison
 between a first intermediate data set and a second intermediate data set by
 5 keeping a value of a bit of the second data set if the corresponding bit of
 the first intermediate data set is equal and ignoring the bit of the second
 intermediate data set if the compared bits are unequal,
 the first intermediate data set received at the virtual and
 temporary second node from the first node and generated at the first node
 10 in response to processing of a first key generating file sent to the first node
 by the server, and
 the second intermediate data set generated at the virtual and
 temporary second node in response to processing of a second key
 generating file communicated to the virtual and temporary second node by
 15 the server; and
 applying the second cryptographic key during a communication
 session with the first node, wherein the first node applies a first
 cryptographic key during the communication session, said first and second
 cryptographic keys being the same,
 20 the first cryptographic key generated at the first node based
 on a bit by bit comparison between a third intermediate data set and the
 first intermediate data set by keeping a value of a bit of the first
 intermediate data set if the corresponding bit of the third intermediate data
 set is set to a first value and ignoring the bit of the first intermediate data
 25 set if the corresponding bit of the third intermediate data set is set to a
 second value, and
 the third intermediate data set sent to the first node by the virtual
 and temporary second node and generated at the virtual and temporary second
 node based on a bit-by-bit comparison between the first intermediate data set and
 30 the second intermediate data set by setting the first value if the compared bits are
 equal and setting the second value if the compared bits are unequal.

12. A computer program comprising instructions which, when executed on at least one
 processor of said node being comprised in said plurality of nodes for establishing a
 35 communication session between said node and the first node, cause the processor to
 carry out the method according to claim 11.

13. A carrier comprising the computer program according to claim 12, wherein the
 carrier is one of an electronic signal, an optical signal, a radio signal, or a
 40 computer readable storage medium.