

CLAIMS

1. A method of establishing a direct wireless communication link between a first device and a second device, the first device being designated as a sender and the second device being designated as a receiver, the method comprising:
 - 5 a proximity authentication operation that comprises determining, based on signals received by the first and second devices over one or more RF channels from a plurality of wireless access points, that the first device is proximate the second device;
 - 10 following the proximity authentication operation, a key generation operation that comprises: generating a shared secret by performing randomness extraction on respective signals received at the first and second devices over a selected channel of the one or more RF channels; and
 - establishing the direct wireless communication link using the shared secret.
- 15 2. A method according to claim 1, wherein the direct wireless communication link is a WiFi Direct link.
3. A method according to any one of the preceding claims, further comprising introducing, prior to the key generation operation, randomness in the physical layer of the first device and/or of the second device.
- 20 4. A method according to claim 3, wherein randomness is introduced by imparting movement to an antenna of the first device and/or an antenna of the second device.
- 25 5. A method according to claim 4, wherein said movement is imparted by a first user gesturing with the first device and/or a second user gesturing with the second device.
6. A method according to any of the preceding claims, comprising a device discovery operation that comprises:
 - 30 the second device:
 - waiting in a listen state for a predetermined wait time in a current channel of said RF channels;
 - if no probe is detected from the first device during the predetermined wait time, setting the current channel to another of said RF channels;
 - 35 if a probe is detected from the first device during the predetermined wait time from the first device, sending a response to the first device over the current channel; and

the first device setting, responsive to the response from the second device, the current channel as a search state channel.

- 5 7. A method according to any of the preceding claims, wherein the proximity authentication operation comprises the second device broadcasting a secure sketch of signal data received by the second device from the plurality of wireless access points; and the first device determining, based on the secure sketch and on signal data received by the first device from the plurality of wireless access points, whether the first device is proximate the second device.
- 10 8. A method according to any of the preceding claims, wherein the proximity authentication operation comprises scanning for said plurality of wireless access points over a subset of frequently used channels.
- 15 9. A method according to any of the preceding claims, wherein the proximity authentication operation further comprises selecting, from said plurality of access points, a subset of access points that are suitable for authentication.
- 20 10. A method according to claim 9, wherein said selecting comprises discarding access points that have small angular range and/or that have large angular range with respect to the first device and the second device.
- 25 11. A device configured to establish a direct wireless communication link with another device, the device comprising at least one processor in communication with computer-readable storage that comprises instructions for causing the at least one processor to:
 - perform a proximity authentication operation that comprises receiving signal data from the another device, said signal data being indicative of signals received by the another device over one or more RF channels from a plurality of wireless access points; and determining, based on signals received by the device over the one or
 - 30 more RF channels from the plurality of wireless access points, that the device is proximate the another device;
 - following the proximity authentication operation, perform a key generation operation that comprises: generating a shared secret by performing randomness extraction on signals received at the device over a selected channel of the one or
 - 35 more RF channels; and
 - establishing the direct wireless communication link with the another device using the shared secret.
12. A device according to claim 11, wherein the direct wireless communication link is a

WiFi Direct link.

13. A device according to claim 11 or claim 12, comprising an antenna that is polarised such that movement of the device introduces randomness in the physical layer of the device.

14. A device according to any one of claims 11 to 13, configured to perform a device discovery operation that comprises:

when the device is in a send mode, successively transmitting probes over a plurality of channels until a first response is received from the another device over one of said channels, and responsive to the response from the another device, setting a search state channel to be the one of said channels; and

when the device is in a receive mode:
waiting in a listen state for a predetermined wait time in a current channel of said RF channels;

if no probe is detected from the another device during the predetermined wait time, setting the current channel to another of said RF channels;

if a probe is detected from the another device during the predetermined wait time, sending a response to the another device over the current channel.

15. A device according to any one of claims 11 to 14, wherein the proximity authentication operation comprises:

when the device is in a send mode, receiving, from the another device, a secure sketch of signal data received by the another device from the plurality of wireless access points; and determining, based on the secure sketch and on signal data received by the device from the plurality of wireless access points, whether the device is proximate the another device.

16. A device according to any one of claims 11 to 15, wherein the proximity authentication operation comprises scanning for said at least one access point over a subset of frequently used channels.

17. A device according to any one of claims 11 to 16, wherein the proximity authentication operation further comprises selecting, from said at least one access point, one or more access points that are suitable for authentication.

18. A device according to claim 17, wherein said selecting comprises discarding access points that have small angular range and/or that have large angular range with respect to the device and the another device.

19. Non-transitory computer-readable storage having stored thereon instructions for causing at least one processor to perform a method according to any one of claims 1 to 10.