Bluetooth Secure Simple pairing

With Bluetooth becoming more widely accepted, a secure pairing method has become a hard requirement for this technology. Introduced in the Bluetooth 2.1 specification, Secure Simple Pairing (SSP) fixes the issues of the previous pairing method, where it was relatively easy to determine the PIN-code and deducing the Link Key, just by passively sniffing the pairing process. SSP also makes pairing Bluetooth devices simpler.

Pairing process:
SSP pairing is centered around a shared secret between 2 Bluetooth devices, which is the so called Link Key. This Link Key authenticates 2 Bluetooth devices to each other and encrypts the exchanged data based on the Link key. The link key is not used to directly encrypt the data, but a temporary Encryption Key is derived from the Link Key in combination with some randomized numbers that are being send just prior to the encrypted data will be send. The same temporary Encryption Key is used to encrypt and decrypt the data in both directions. Usually the Encryption key is maintained during a session, and discarded as soon as the connection is closed, but in theory it can also be changed during the session.
The bluetooth specification specifies three pairing processes;

- LMP-pairing Link Manager Protocol (aka PIN-code based)
- SSP-pairing Secure Simple Pairing
- None Standard Pairing (custom for 2 device of the same manufacturer)

Common for all 3 methods is that it results in a shared Link Key on which the encryption will be based.

LMP pairing (aka PIN-code based)
For the LMP algorithm to create a Link key the following information is

- The BDADDR of the two devices
- A 16-byte random number created by the initiating device (master)
- A PIN code (user defined or hardcoded)

These numbers are used to first create a temporary shared initialization key, which is then converted into a Link Key using LMP pairing key generation procedure.
Since the only undisclosed information is the PIN code the number of possible secret Link Keys is limited by the number of possible PIN codes That means when a 4 digit PIN code is used, an attacker would only have to try 10.000 different Link Keys at maximum before being able to decrypt the traffic. This is where the weakness of the LMP pairing resides, and on the market available Bluetooth sniffers with decryption software are capable to determine the PIN code within seconds.

Secure Simple Pairing
SSP uses a much more complex mechanism, known as elliptic curve cryptography, that strictly uses the PIN for the authentication process, but doesn't use the PIN code as part of the Link Key calculation process. For the encryption SSP uses extremely large random generated numbers for its Link Key calculation where the number of possible Link Keys is thus no longer limited to less than 2^{128} possibilities.

This elliptic curve cryptography is achieved by establishing a different kind of shared secret between the two devices, known as the Diffie-Hellman key (DHKey a 192-bit random number). As a prerequisite, for this both devices have each a SSP private key and a SSP public key where the public key is transmitted through air and can be intercepted. The private key however will never be disclosed.
The strength of the SSP protocol is that two devices will be able to pair without the need of transmitting any critical information through air, or externally share this by other means. For calculating the Link Key, it uses the DHKey as a seed and the rest of the pairing process is similar to LMP pairing.