Whatsapp Encryption

The term 'end-to-end encryption' (E2EE) has entered the common lexical use and is no more restricted to the geeks, thanks to WhatsApp which popularised it and brought it to over a billion users globally. It has become the part of our daily digital life as it is the definitive security mechanism that protects our personal data (messages etc.) such that it can only be read on by the sender, and by the recipient on the other end. No one else, including the hackers or the government, can snoop and read the encrypted data.

How does end-to-end encryption work?

WhatsApp's end-to-end encryption ensures that only you and the person you're communicating with can read what's sent. Nobody in between, not even WhatsApp, can read the messages. The messages are secured with locks, and only the recipient has the special key to unlock and read the messages. WhatsApp uses Signal Protocol developed by Open Whisper Systems. The following steps describes the working of E2EE when two people communicate on WhatsApp.

1. When the user first opens the WhatsApp, two different keys (public & private) are generated. The encryption process takes place on the phone itself.
2. The private key must remain with the user whereas the public key is transferred to the receiver via the centralised WhatsApp server.
3. The public key encrypts the senders message on the phone even before it reaches the centralised server.
4. The server is only used to transmit the encrypted message. The message can only be unlocked by the private key of the receiver. No third part, including WhatsApp can intercept and read the message.
5. If a hacker tries to hack and read the messages, they would fail because of the encryption.