Abstract

Embodiments of the invention provide methods and apparatuses for session key generation, which use Diffie-Hellman procedure in both user equipment and network to prevent an attacker from breaking the session key by simply listening to signal exchanges passively when the attacker possesses credentials of a USIM card.

(Figure 3)