
5G - Physical Layer Security

Dec. 7, 2021

Glossary

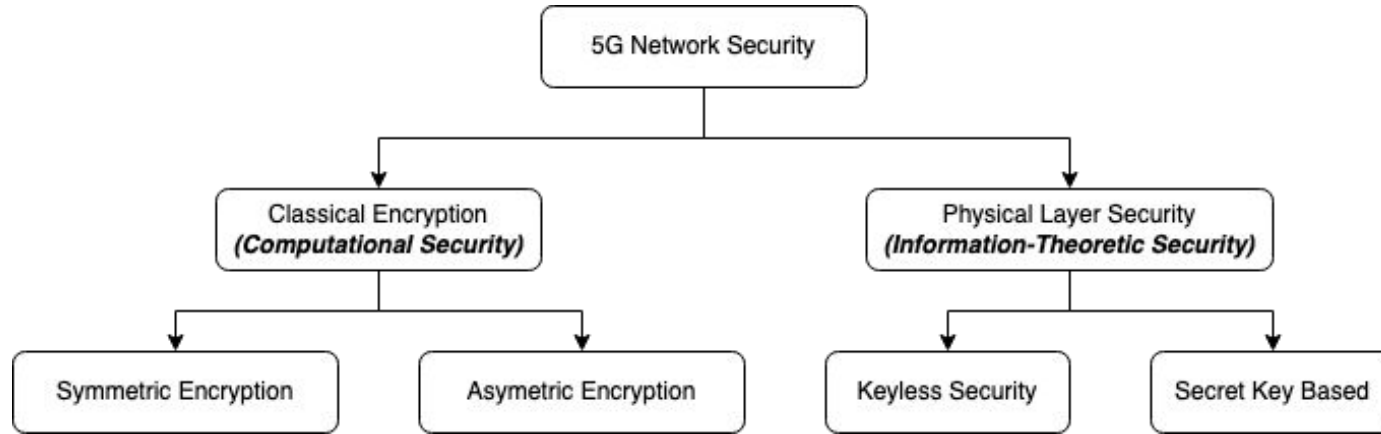
CIR - Channel Impulse response

RSS - Received Signal Strength

TDD - Time Division Duplex

PLS - Physical Layer Security

Wireless Security Architecture



Source: Key Generation From Wireless Channels: A Review [2]

Classical encryption

Pro

- No known feasible attacks
- Widely deployed and tested
- Trustworthy authentication

Cons

- Build on unproven assumptions
- Computational intensive
- Require significant infrastructure

Physical Layer Security

Pro

- Quantum secure
- On-the-fly secret key generation
- Fast and lightweight implementation

Cons

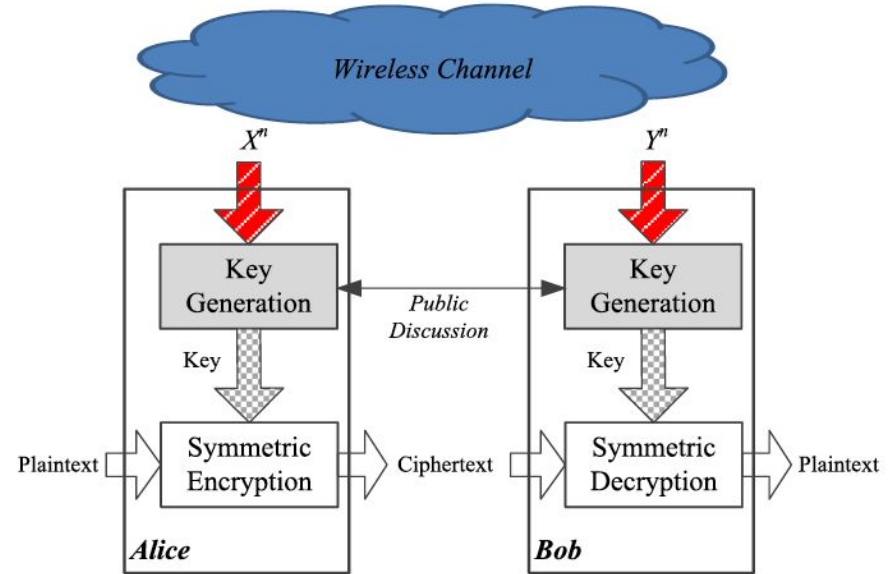
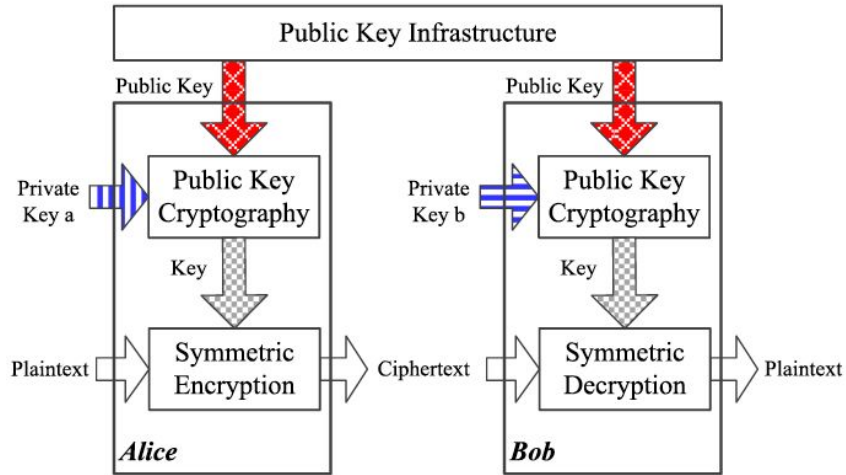
- Assumptions on main and eavesdropper channel
- Not enough testing

Comparison of security schemes

TABLE 1. Comparison of security schemes.

Scheme	Description	Implementation	Complexity	Pros	Cons
Symmetric encryption	Legitimate users use the same key to encrypt data.	Yes	Low	Efficiency in data encryption	Computationally secure; A secure key required prior.
Asymmetric encryption	Legitimate users use the same public key but different private keys to distribute a session key.	Yes	High	Key distribution with different private keys	Computationally secure; Public key infrastructure required; Not applicable to low computational capacity devices.
Keyless security	Legitimate users securely communicate by leveraging code design and channel properties.	Not reported	High	Information-theoretically secure; Secret transmission without keys.	Eavesdroppers' CSI usually required.
Key generation	Legitimate users generate key from the randomness of the common channel.	Yes	Low	Information-theoretically secure; Lightweight; No aid from other users required.	Limited by the channel dynamicity.

PLS - Key generation

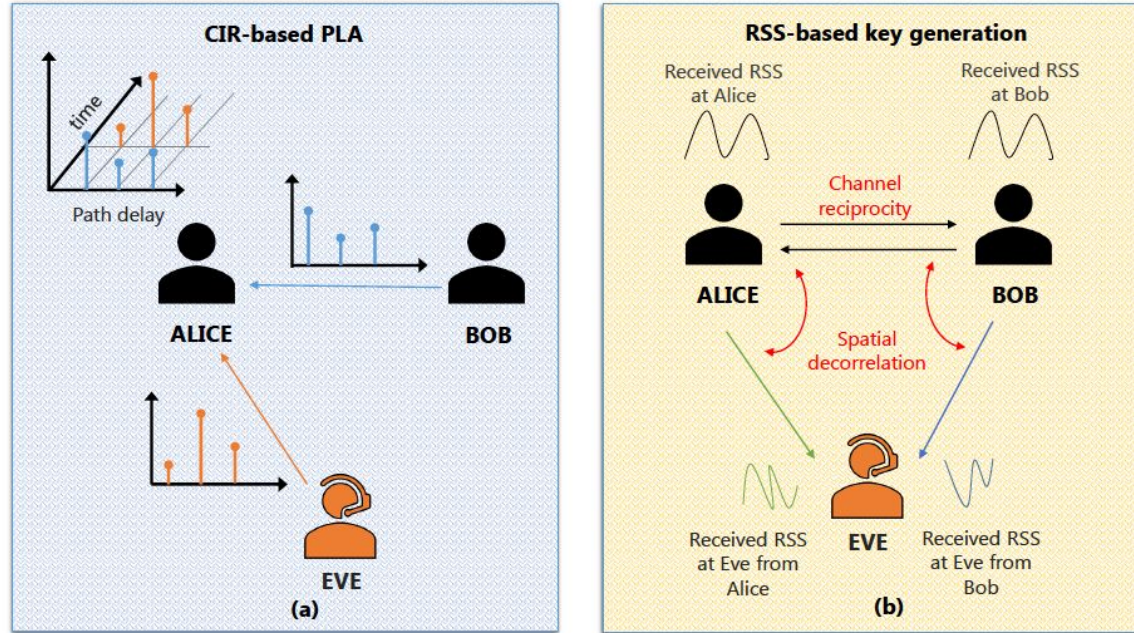


Source: Key Generation From Wireless Channels: A Review [2]

Key generation principles

- **temporal variation**: introduced by the movement of transmitter, receiver or any object in the environment which will change the channel paths;
- **channel reciprocity**: implies the uplink and downlink can be reversed
- **spatial decorrelation**

Schematic representation of **Channel Impulse Response (CIR)** and **Received Signal Strength (RSS)**



Source: **Physical-Layer Security for 5G and Beyond [1]**

References:

1. **Physical-Layer Security for 5G and Beyond:** <https://onlinelibrary.wiley.com/doi/10.1002/9781119471509.w5GRef152>
2. **Key Generation From WirelessChannels: A Review** - <https://ieeexplore.ieee.org/document/7393435>