Quantum Cryptography

Quantum cryptography can be seen as the first, perhaps most natural consequence of the difference between classical and quantum information. The course will base its approach on quantum information theory to present the main principles related to quantum cryptographic constructions. It will also connect and discuss the practical developments, technologies, and applications of quantum cryptography, and its positioning with respect to classical cryptography.

Lecture 1: Quantum Cryptography principles
Classical and Quantum Information, Conjugate coding, No-cloning, Quantum Money, Uncertainty relation, Monogamy of entanglement

Lecture 2: Randomness generation
Types of RNG, Randomness extraction, DD-QRNG, DI-QRNG,

Lecture 3: Quantum Key Distribution,
QKD protocol, Security Definition, BB84 Security Proof

Lecture 4: QKD versus classical key exchange, TD on QKD, QRNG

Lecture 5: QKD in practice,
Q Communications Technologies, DV-QKD, CV-QKD, Implementations, Protocols, Performance, Maturity

Lecture 6: Quantum Internet, TD on Experimental Quantum Cryptography (ideally TP in the future)

Lecture 7: Multi-Party Quantum Cryptography
Bit Commitment, Oblivious Transfer, Coin Flipping