

Quantum Key Distribution

Jákó András

jako.andras@eik.bme.hu

KIFÜ, BME

Szimmetrikus kulcsú titkosítók

- a kódoláshoz és dekódoláshoz ugyanaz a kulcs kell
- pl.: DES, AES, OTP
- előny: (viszonylag) egyszerű
 - software-ben se lassú
 - könnyen implementálható olcsó célhardware segítségével
 - pl.: Intel AES-NI
- hátrány: a kulcsot előre egyeztetni kell

Publikus kulcsú titkosítók

- kulcspár: összetartozó titkos és nyilvános kulcs
 - kódolás a nyilvánossal, dekódolás a titkossal
 - a nyilvánosból a titkost kitalálni nagyon nehéz
 - faktorizálás vagy diszkrét logaritmus adja a nehézségét
- pl.: RSA
- előny: nem kell előzetesen egyeztetni kulcsot
- hátrány: számításigényes, lassú

Ma szokásos felhasználás

- publikus kulcsú titkosítóval ad-hoc szimmetrikus kulcs kiosztása
- felhasználói adatok továbbítása szimmetrikus kulcsúval kódolva
- pl.: SSL/TLS, SSH

Fenyegetettség

- a faktorizálás és a diszkrét logaritmus csak a “hagyományos” számítógépek számára nehéz
 - Peter Shor algoritmusával (1994) egy kellően nagy kvantumszámítógép gyorsan meg tudja oldani majd
- az elterjedt szimmetrikus kulcsú algoritmusok viszont nem fenyegetettek
 - legalábbis nem annyira: elegendő a kulcs méretét növelni

Menekülési útvonalak

- PQC: Post-Quantum Cryptography
 - olyan publikus kulcsú algoritmusok kifejlesztése a cél, amit a kvantumszámítógépek sem tudnak feltörni
- QKD: Quantum Key Distribution
 - publikus kulcsú algoritmusok mellőzése
 - a szimmetrikus kulcs eljuttatása a kommunikáló feleknek teljesen más módon

Quantum Key Distribution

- miért “kvantum”?
 - mert a kvantumfizikán alapul
 - semmi köze a kvantumszámítógépekhez
- az információt olyan fizikai paraméterekbe kódolva továbbítja, ami megfigyelés esetén „elromlik”
 - a lehallgatást működési hibaként észlelik a kulcsot egyeztető felek

QKD módszerek osztályozása

- változó jellege: amilyen értékeket a kvantumfizika törvényszerűségei által védett információt hordozó fizikai paraméter felvehet
 - diszkrét (DV)
 - folytonos (CV)
- protokoll jellege
 - elkészít és megmér (prepare & measure)
 - összefonódás (entanglement) alapú
- átviteli közege
 - fényvezető szál
 - földfelszíni szabadtéri
 - műholdas

Prepare & measure

- Alice generál egy véletlen értéket
- ezt kódolja egy foton valamilyen fizikai tulajdonságába
- átküldi Bobnak
- Bob megméri

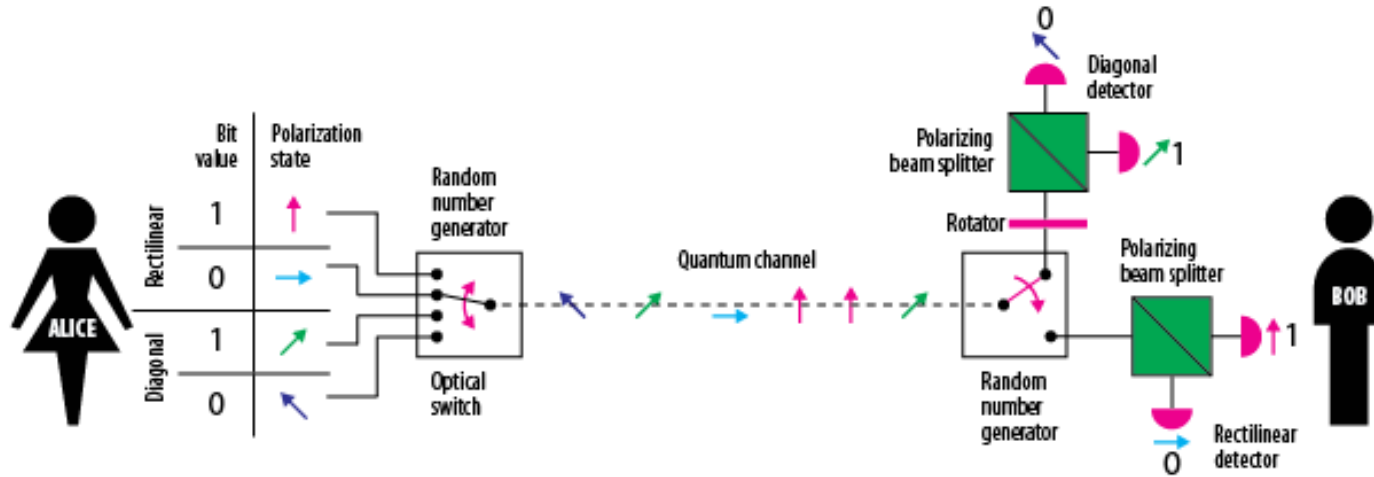
Entanglement based

- valaki generál egy összefonódott fotonpárt
 - generálhatja Alice, vagy harmadik fél is (pl. műholdon)
- az egyik foton eljuttatja Alice-nek, a másikat Bobnak
- mindketten megméri
 - a mérés eredménye véletlen, de azonos

BB84 protokoll

- C. Bennett, G. Brassard, 1984.
- DV, prepare & measure
- hozzávalók:
 - egyirányú kvantum csatorna (pl.: ITU-T G.652 fényvezető szál)
 - a lehallgatás elrontja az átvitelt
 - kétirányú szerviz csatorna (pl.: IP)
 - nem titkos

BB84 működés



Quantum transmission & detection	ALICE sends photons								
	ALICE's random bits	0	1	0	1	1	1	0	1
	BOB's detection events								
	BOB's detected bit values	1	1	0	1	1	1	0	0
Public discussion (i.e., sifting)	BOB tells ALICE the basis choices he made								
	ALICE tells BOB which bits to keep		✓		✓		✓	✓	
	ALICE and BOB's shared sifted key	-	1	-	1	-	1	0	-

BB84 működés (folyt.)

- kvantum csatornán:
 - Alice véletlenszerűen választ értéket (0/1) és polarizációs bázist (rectilinear/diagonal)
 - a választott bit és bázis szerint polarizált fotont küld Bobnak
 - Bob véletlenszerűen választ polarizációs bázist a detektáláshoz
 - ha Alice-ével azonos bázist választott, akkor a bit értékét is jól fogja dekódolni
- szervíz csatornán a fentiek után:
 - Alice és Bob egyeztetik, hogy milyen bázist választottak
 - azonos bázis esetén Bob megtartja a bitet, különben eldobja (sifting, rostálás)

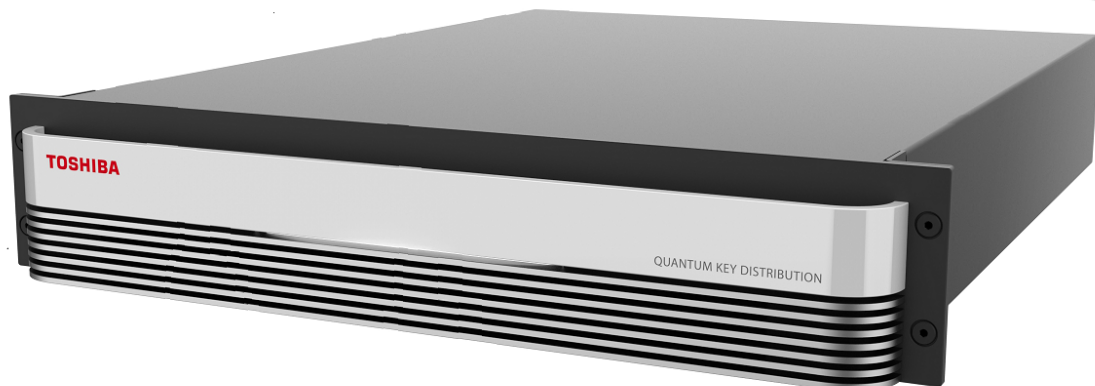
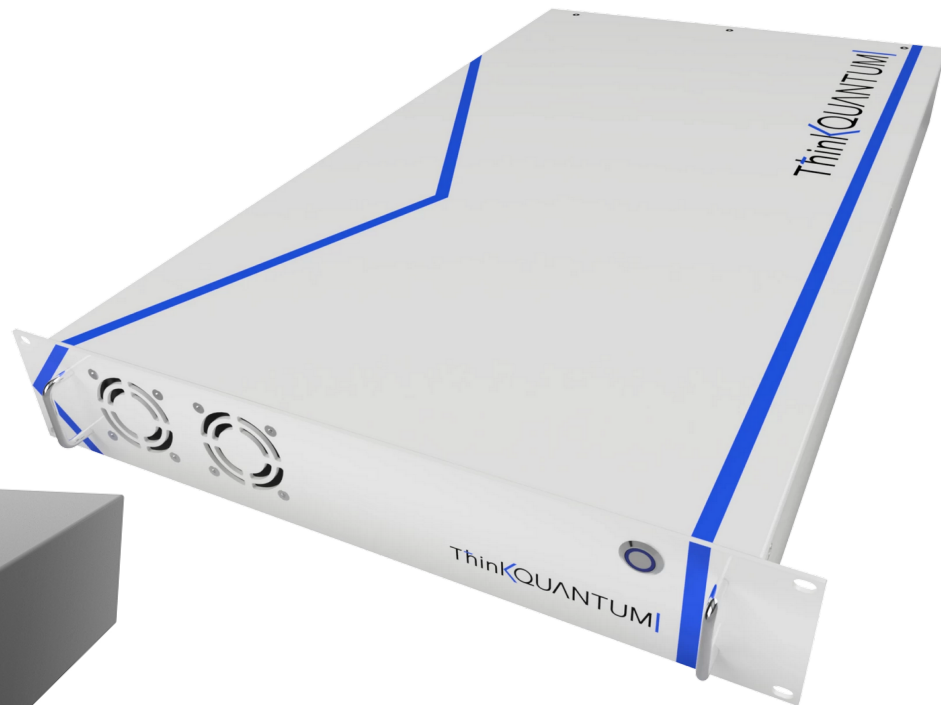
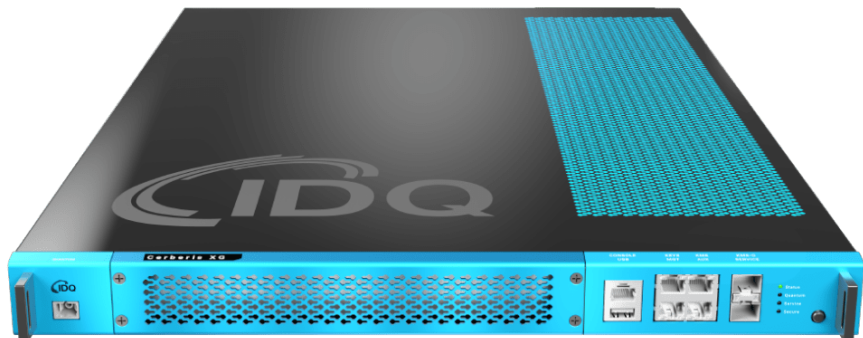
BB84 lehallgatás detektálása

- a sifted key egy részét (10-25%) publikusan összehasonlítják
 - ebből következtetnek a hibaaarányra (QBER)
 - ezeket a biteket eldobják, a maradékot használják fel kulcsbitekként
- lehallgatás → magas QBER
 - ha a QBER túl magas, akkor minden bitet eldobnak

BB84 alapú QKD készülékek

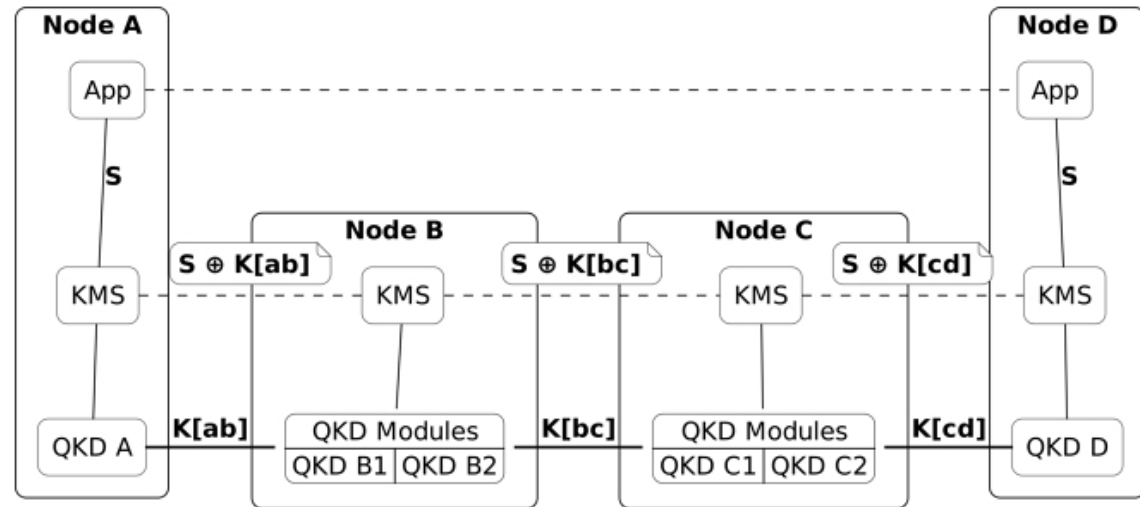
- páronként ~200k EUR
- generált kulcsbitfolyam intenzitása a kvantum csatorna minőségével arányos
 - távolság ill. beiktatásos csillapítás
 - zavarjelek (pl. WDM adat a kvantum csatornával egy szálon)
- tipikus hatótáv: ~100 km, ~20 dB
- tipikus kulcsbitfolyam ráta: kbit/s

QKD készülékek



QKD nagyobb távolságra

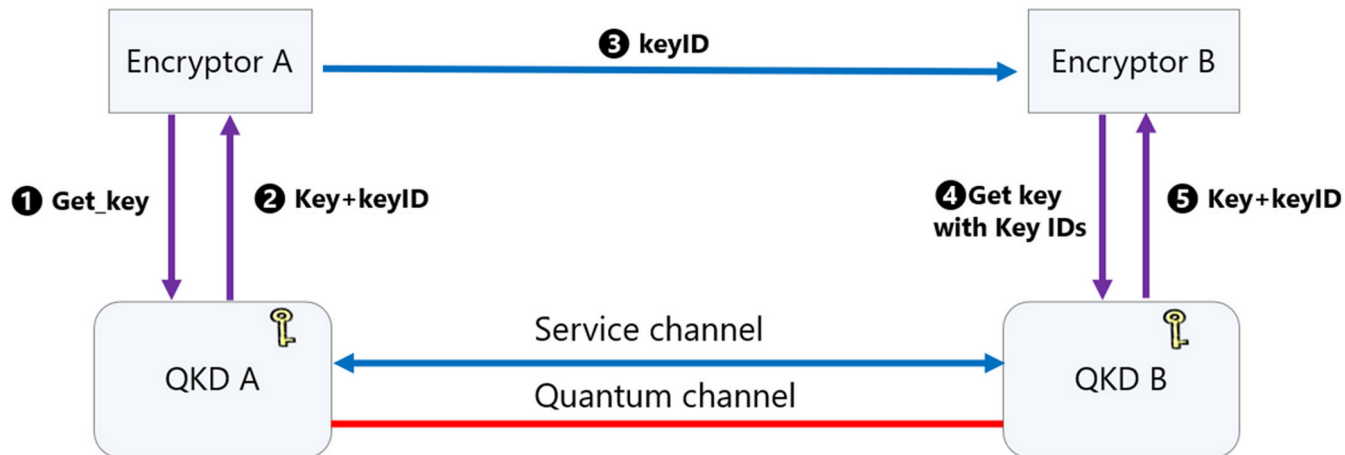
- daisy chain
 - általában QKD készülékpárok sorba kötve
- köztes trusted node-ok
 - védettnek kell lenniük, mert itt hozzáférhető a kulcs
- Key Management System (KMS)
 - azonos kulcsokat biztosít a két távoli végpontokon az egyes szakaszok kulcsai segítségével



Itt pl. az S véletlen generált kulcs szakaszonként a QKD által szolgáltatott kulccsal OTP kódolással jut el a lánc túlsó végére. ("App" a szimmetrikus kulcsú titkosító.)

Interface a titkosító felé

- ETSI GS QKD 014
 - REST API



- és persze van proprietary is (pl.: Cisco SKIP)

Kulcs felhasználása

- OTP: közvetlenül
- IPsec: RFC 8784
- MACsec: pl. a SAK származtatható a QKD kulcsából és egy hagyományosból (pl. Diffie-Hellmann)
 - MACsec Key Agreement helyett QKD
- ízlés szerint

Köszönöm a figyelmet!