Key distribution. Episode 1: Quantum menace

Grigory Marshalko Vladimir Rudskoy

4 June, 2019

How to share keys in post-quantum world?

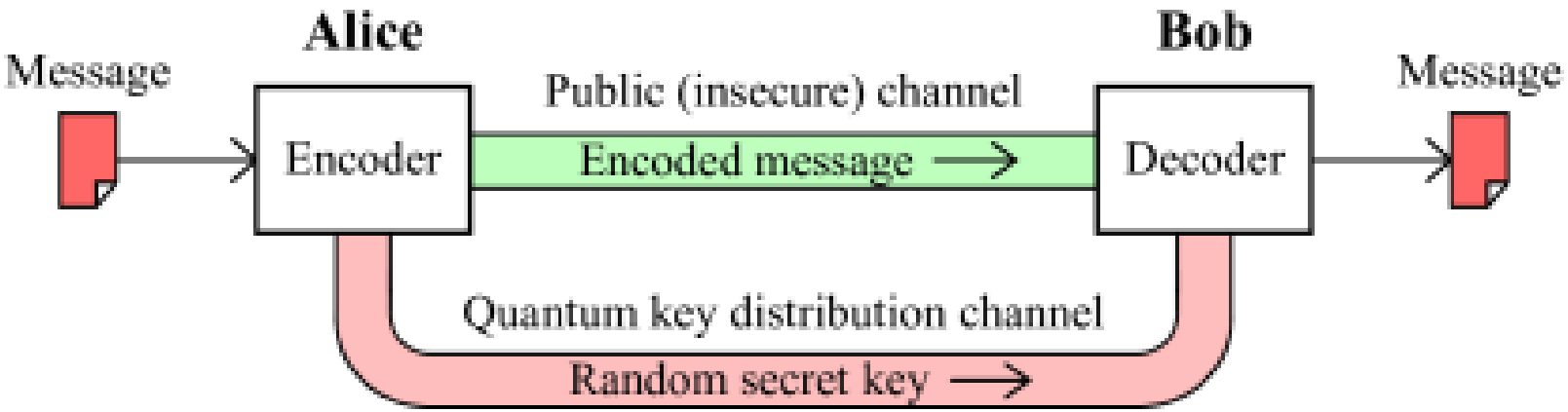
- Use post-quantum schemes
- Use Quantum Key distribution
- Send with Russian Post, FedEx and other courier services

QKD: pros & cons

- Resistant against quantum attacks
- Information-theoretic secure
- Detects eavesdropper (if properly implemented)

- Hard and expensive to implement
- Implementation attacks (if not properly implemented)
- Speed and distance limitations

How QKD works?



How to load quantum key into the cryptographic device?

How keys are usually treated in quantum protocols?

One-time pad

- easy to use (XOR is fast!)
- easy to prove (One-time pad is information-theoretically secure)

Post-processing with error correcting codes

- k_q - secret key
- G - generator matrix of an error correcting code
- k_a - Alice's quantum sequence
- k_b - Bob's quantum sequence

Alice: $k_q \rightarrow G(k) \oplus k_a$
Bob: $G(k) \oplus k_a \oplus k_b \rightarrow k_q$

How to load distributed key into the cryptographic device?

- QKDs are new! If QKD fails, how to protect information?
- Use combination of quantum distributed k_q and classical keys k_c
- Can we use a one time-pad ($k_q \oplus k_c$) and get information-theoretical security?

Related key attacks

- Introduced by Eli Biham in 1994
- Multi-key setting (attacker doesn't know the values, but can exploit relations between keys)
- Very efficient: relax data and time complexities of classical attacks (attacker has several instances - additional freedom)
- Usually have simple relations (linear, affine)

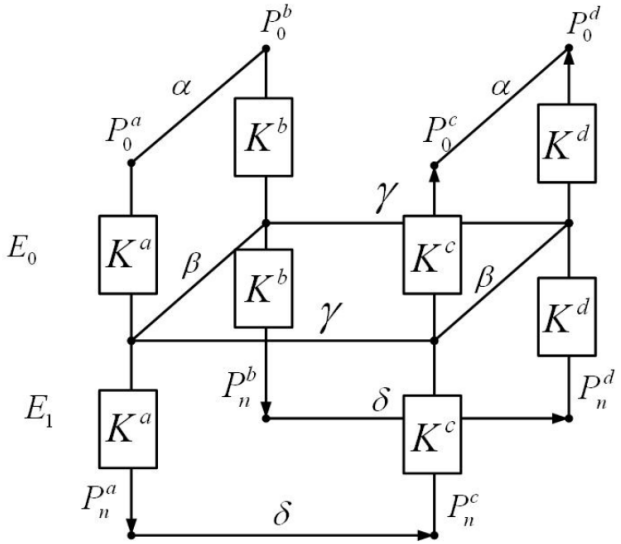


Figure 2: The related-key boomerang attack

Related key attacks and QKD

- We do not know exact values. How to find related keys?
- Vladimir Rudskoy in 2011 showed that if we count the complexity of search for related keys, the complexity of overall attack exceeds the complexity of total key search attack (On zero practical significance of key recovery attack on full GOST block cipher with zero time and memory)
- So they are considered generally impractical in classical setting
- For the considered one-time pad in case of QKD compromise we have $k_c \oplus k_{q,i}, i = 1, 2...$, where $k_{q,i}$ are known to the attacker - exactly what we need for related key attack

Related key attacks ...

in classical setting

in QKD setting

We do not have to consider the complexity of testing relations on keys. Just wait...

A small example

- Let's consider the simplest case, when an attack requires two keys: K_1 and $K_2 = K_1 \oplus \Delta$.
- Now the key set can be divided into two disjoint classes, such that if one of the keys of the pair lies in the first class, the other one lies in the second one.
- Then the estimation of the probability of finding a key pair K_1 and $K_2 = K_1 \oplus \Delta$ among K_j^H is essentially the problem of estimating the probability of a collision in two samples.
- It is known from D. Wagner «A generalised birthday problem» that the probability of collision in two subsets of N elements, where the subset sizes are equal to $\tau_1\sqrt{N}$ and $\tau_2\sqrt{N}$ can be estimated as $1 - e^{-\tau_1\tau_2}$ when $N \to \infty$.

Related key attack for Magma

Rudskoy

- $K_1, K_2 = K_1 \oplus \Delta_1, K_3 = K_1 \oplus \Delta_2, K_4 = K_1 \oplus \Delta_1 \oplus \Delta_2$.
- Related key boomerang attack with complexity is about 2^{71} encryptions, and the data complexity is 2^{28} pairs of chosen plaintexts.
- Requires a set of 14 related keys.

Pudovkina, Khoruzhenko

- A combination of differential attack and the previous boomerang attack
- The complexity of the attack is 2^{62} encryptions, and the data complexity does not exceed 2^{43} chosen text pairs.
- The attack requires 12 related keys to be mounted.

Related key attack for Kuznyechik

Not applicable

- Alekseev E., Goncharenko K., Marshalko G., Provably secure counter mode with related key-based internal rekeying
- Ishchukova E.A., Krasovsckiy A.V., Polovko I.Yu. Analysis of the cipher Kuznyechik by the related keys method
- and tomorrow ... Kiryukhin V. Related key-attack on 5-round Kuznyechik

Attacks on QKD

Photon-number splitting attack

- Non-ideal photon source - multiple photon in pulse
- Attacker can split the photon beam and measure the state
- The success probability depends on the parameters but could be very close to 1

Attacks on QKD

Detector laser damage

- Attacker can destroy Bob's photo detectors with high voltage laser pulse from the fiber channel
- Bob's photo detectors under full control of the attacker

Attacks on QKD

Trojan horse attack

- Attacker illuminates the laser on Alice side and gets the state by the analysis of the reflected signal
- The success probability is higher than 0.99

Attacks on QKD

Bright illumination attacks

- Power pulse of light illuminates moves detectors into the linear mode
- Attacker performs meet-in the middle attack: measure the photon from Alice and sends it to Bob
- Bob would have the same measurement as the attacker

So...

- The bad news - the attacker could have the whole key with probability close to 1.
- The good news - he doesn't have access to Alice RBG, so he can't force relation on keys

To be on the safe side

Use KDFs

- R 50.1.113–2016 Cryptographic algorithms to accompany the usage of digital signature and hash function
- R 1323565.1.022-2018. Key derivation functions
- Set classical key k_c as key input to KDF, and k_q as additional input
- In case of k_q - the output will be still secure