On pseudorandomness in quantum cryptography

D.A.Kronberg

Steklov Mathematical Institute of Russian Academy of Sciences,
Russian Quantum Center,
Moscow Institute of Physics and Technologies

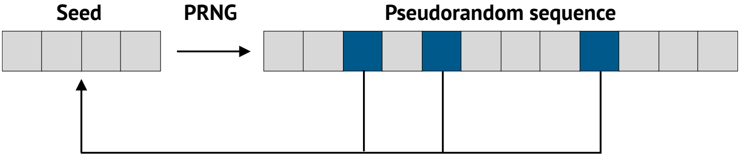
September 10, 2018

Outline

- Pseudorandomness in classical cryptography
- Quantum cryptography: B92 protocol
- Using pseudorandomness in quantum key distribution: Y00 protocol
- A generalized protocol

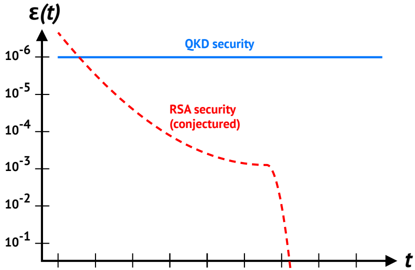
Pseudorandomness in classical cryptography

- One-time pad is the only information-theoretically secure classical cryptosystem, but it needs a long key which can be used just once. Other symmetric cryptosystems like DES or AES use shorter keys but can offer only computational security.
- A PRNG is an algorithm, which generates a sequence of bits which look like random, but are determined by an initial value (**seed**).
- For cryptographical purposes, it should take a lot of time to compute seed by the output sequence. Every key bit discovered by Eve simplifies the seed computation



Quantum cryptography and motivation

- Every classical cryptosystem beside one-time pad is only computationally secure, and its security tends to zero with time, since Eve can reduce it performing computation
- Quantum cryptography relies on impossibility of discrimination between non-orthogonal quantum states, which does not depend on time. Thus the security of quantum cryptosystems remains constant.
- The motivation of my work is to use classical pseudorandomness to increase key generation rate of quantum cryptography, keeping the security constant

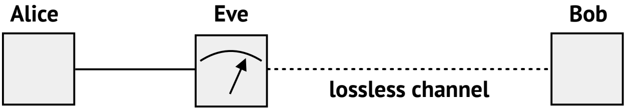


Picture from the tutorial by R.Renner at QCrypt'2018

Quantum cryptography: B92 protocol

- The main task for quantum cryptography is key distribution between two distant users (Alice and Bob) with no technological or computational assumptions about the eavesdropper (Eve)
- In B92 protocol, Alice uses two non-orthogonal states $\{|\psi_0\rangle, |\psi_1\rangle\}: \quad \langle\psi_0|\psi_1\rangle = \varepsilon$
- Bob performs "three-outcomes measurement" $\{M_0 = \frac{I-|\psi_1\rangle\langle\psi_1|}{1+\varepsilon}, M_1 = \frac{I-|\psi_0\rangle\langle\psi_0|}{1+\varepsilon}, M_? = I - M_0 - M_1\}$, which whether gives correct bit value, or yields an inconclusive result
- The closer the states are (i.e. the closer is ε to 1), the higher is inconclusive result probability
- Alice and Bob use public authentic channel to discard the positions with inconclusive results

Unambiguous state discrimination (USD) attack



- For a lossy channel between Alice and Bob, Eve can perform the same measurement as Bob, and block the signal in case of inconclusive result; otherwise she uses lossless channel to send it to Bob. For a long channel with high losses, Eve can perform this attack without being detected by extra losses
- Alice and Bob can make the states less distinguishable to resist USD attack, but they would suffer from inconclusive results as well
- Common countermeasures against USD attack include: strong reference pulse, decoy states, distributed encoding.

Symmetric coherent states

- Coherent states are widely used in quantum cryptography since they can easily be generated with attenuated lasers
- Coherent states is described by one complex parameter α, or with two real: intensity μ and phase φ, where $\alpha = \sqrt{\mu} e^{i\varphi}$:

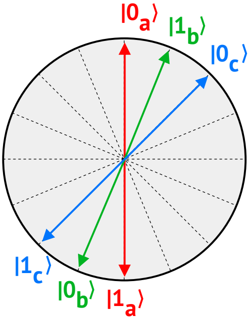
$$|\alpha\rangle = e^{-\frac{|\alpha|^2}{2}} \sum_{n=0}^{+\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle$$

- For a set of N symmetric coherent states $\{|\alpha_j\rangle, \}, \alpha_j = \alpha e^{\frac{2\pi ij}{N}}$ with equal intensities and phases from 0 to 2π, the success probability for USD has been found
- Using the set of symmetric states can be a countermeasure against USD attack since their unambiguous discrimination is hard for large N

A.Chefles and S.M.Barnett, quant-ph/9807023

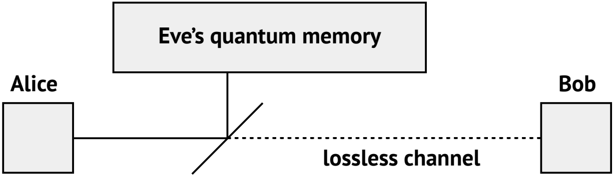
Y00 protocol: quantum stream cipher

- Y00 is probably the most common QKD protocol which uses pseudorandomness and assumptions about limited Eve's possibilities
- It uses symmetric coherent states of relatively high intensity and pseudorandom sequence which specifies the basis for Alice and Bob at each position
- Bob measures the states close to orthogonal in the known basis, therefore key generation rate is very high



H.P.Yuen, quant-ph/0311061

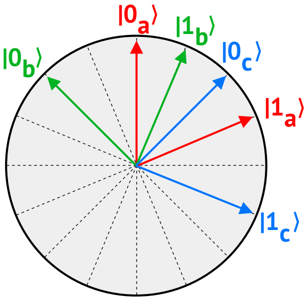
Beam splitting attack



- Y00 is good for Eve which is not beyond today's technologies, but if Eve has a long-lived quantum memory, or can perform certain computations fast, it is not secure
- In beam splitting attack, Eve simulates the channel losses by her beam splitter
- In Y00, states within each basis are almost orthogonal, and once Eve computes the seed of pseudorandom sequence, she can get a lot of information from the states

Pseudorandom protocol with non-orthogonal states

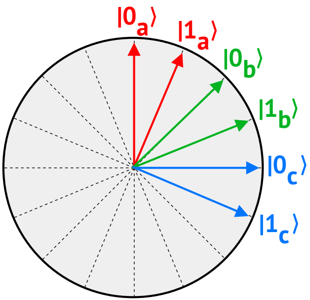
- I propose a simple Y00 modification: non-orthogonal states within each basis. Even after getting information about the basis, Eve cannot extract full information on bit value from the two non-orthogonal states
- The main assumption is that Eve cannot compute the seed of PRNG *during the communication session* between Alice and Bob and perform USD attack, knowing the basis
- If Eve knows all the pseudorandom sequence right after the communication session, her information is still below the information of Bob, like in B92 protocol



Fully random protocol version

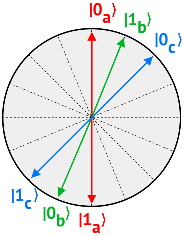
- A protocol with fully random symmetric coherent states was proposed earlier
- Large number of bases can be a problem for the fully random case, because the probability that Bob choses the correct basis is low
- For our version of the protocol, large number of bases is not a problem because Bob always knows the correct basis

S.N.Molotkov, JETP Letters 95, 6 332-337

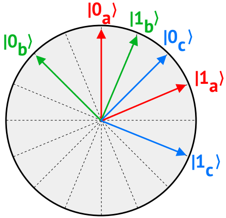


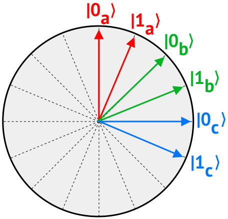
Switching between different versions

One can switch between different states configurations with the same hardware for different security criteria: from fully random version for critical applications to Y00 for high-speed key generation.



top speed





most secure

Security analysis for beam splitting attack

We can easily find the secret key rate if Eve performs beam splitting attack

For the given channel length l, the Alice intensity μ_A becomes $\mu_B = \mu_A 10^{-\frac{\delta l}{10}}$, where attenuation parameter $\delta \approx 0.2$ dB/km for fiber lines; Eve can get the states of intensity $\mu_E = \mu_A - \mu_B$

If phase difference between $|\alpha_0\rangle$ and $|\alpha_1\rangle$ in the same basis is ψ, then

$$\langle \alpha_0 | \alpha_1 \rangle = e^{|\alpha|^2 (e^{i\psi} - 1)}$$

Thus, Eve's information is given by Holevo value

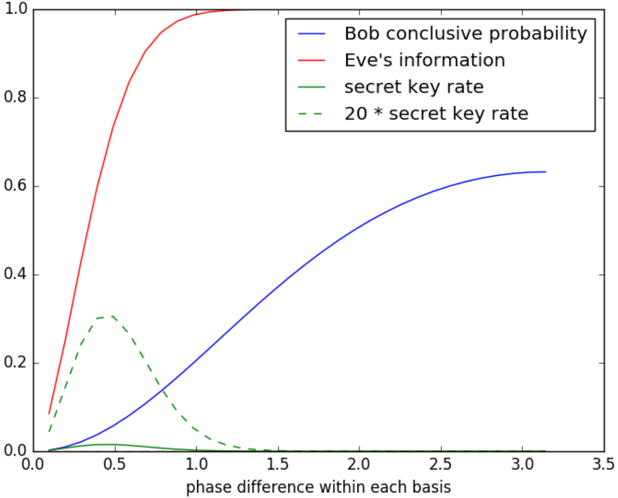
$$I_{AE} = h_2\left(\frac{1 - |e^{\mu_E (e^{i\psi} - 1)}|}{2}\right)$$

And secret key rate is given by

$$I_{sec} = p^B_{conc}(1 - I_{AE}), \quad p^B_{conc} = 1 - |e^{\mu_B (e^{i\psi} - 1)}|$$

Security analysis for beam splitting attack

Results for $\mu_A = 5$ photons/pulse, $l = 50$ km, $\delta = 0.2$ dB/km; 32 bases



Conclusion

- If classical systems with pseudorandomness are considered as satisfactory, then in certain circumstances we can use it in quantum cryptosystems as well
- Our main assumption is weak: Eve cannot compute the seed of PRNG by the end of communication session (which usually takes several minutes)
- We can use the same hardware for different states configuration, depending on the security requirements

Thank you for your attention!