Science Bulletin 65 (2020) 2048–2049

Contents lists available at ScienceDirect

Science Bulletin

journal homepage: www.elsevier.com/locate/scib

Science Bulletin
www.scibull.com

Commentary

Improving the security of "measurement-device-independent quantum communication without encryption"

Nayana Das [a], Goutam Paul [b,*]

[a] Applied Statistics Unit, Indian Statistical Institute, Kolkata, India
[b] Cryptology and Security Research Unit, R. C. Bose Centre for Cryptology and Security, Indian Statistical Institute, Kolkata, India

In 2018, Niu et al. [1] proposed a measurement-device-independent quantum secure direct communication (MDI-QSDC) protocol and quantum dialogue (MDI-QD) protocol using Einstein-Podolsky-Rosen (EPR) pairs. In their protocols, the two legitimate parties prepare two sets of EPR pairs in their locations, and send the partner qubits of their EPR pairs to an untrusted third party (UTP). Here we analyze these protocols and show that 50% of the information about the secret message bits is leaked out in both the protocols.

MDI-QSDC protocol [1]. There are three parties in this protocol, namely, Alice – the sender, Bob – the receiver, and Charlie – an UTP, who performs all the measurements. They use the EPR pairs $|\Phi^{\pm}\rangle, |\Psi^{\pm}\rangle$ for sending the message bits, where, $|\Phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle), |\Psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$. The steps of the protocol are as follows:

1. Alice (Bob) prepares n EPR pairs randomly in $|\Psi^{\pm}\rangle$ states and creates two sequences S_{A_1} and S_{A_2} (S_{B_1} and S_{B_2}) of single photons, such that for $1 \leqslant i \leqslant n$, the i-th qubits of S_{A_1} and S_{A_2} (S_{B_1} and S_{B_2}) are partners of each other in the i-th EPR pair. Alice (Bob) also chooses m single qubit states randomly from $\{|0\rangle, |1\rangle, |+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$ and inserts these qubits in random positions of S_{A_2} (S_{B_2}), and let the new sequence be C_{A_2} (C_{B_2}) containing $(n+m)$ single qubit states. They send the sequences C_{A_2} and C_{B_2} to Charlie, who makes Bell measurement on each pair of C_{A_2} and C_{B_2} and announces the result.
2. Alice and Bob announce the positions of the single qubit states in the sequences C_{A_2} and C_{B_2} respectively. For $1 \leqslant i \leqslant n+m$, three cases may arise. (i) Both the i-th qubits are from S_{A_2} and S_{B_2}, and as a result of quantum entanglement swapping [2], the Bell measurement converts the corresponding partner qubits of S_{A_1} and S_{B_1} into an EPR pair. (ii) Both of them are single qubits, then Alice and Bob exchange the basis information of their single qubits and if the bases are different, then they discard the measurement result. Else it is used for security checking, they estimate the error in the channel and decide to continue the protocol or not. (iii) One of the i-th qubit is a single qubit and another is a partner qubit of an EPR pair, then Alice and Bob discard the i-th Bell measurement result.
3. Alice and Bob discard the qubits, which are not entangled, from their sequences S_{A_1} and S_{B_1}, and make the new sequences M_A and M_B respectively. Let each new sequence contain $(n-\delta)$ single qubits (number of discarded qubits is δ). Alice performs the unitary operation σ_z [3], on the qubits of M_A, whose initial states were $|\Psi^{+}\rangle$. Now for $1 \leqslant i \leqslant n-\delta$, only Bob knows the actual state of the i-th qubit pair (M_{Ai}, M_{Bi}) (which is a Bell state).
4. Message encoding: Alice puts some random checking bits on random positions of her message. She applies one of the four unitary operators (Pauli matrices [3]), $I, \sigma_x, i\sigma_y$ and σ_z, on the qubits of M_A, to encode the information $00, 01, 10$ and 11 respectively. To make the protocol secure against the intercept-and-resend attack, Bob randomly applies I or σ_z on the qubits of M_B. They send the sequences M_A, M_B to Charlie, who measures each pair of qubits of M_A and M_B on Bell basis and announces the result. From the measurement outcomes, Bob decodes the message of Alice. Then Alice announces the positions and values of the random checking bits, and from this information, they can check the integrity of the message. A non-negligible error implies the existence of some eavesdropper in the channel.

MDI-QD protocol [1]. This is a simple generalization of the previous MDI-QSDC protocol. The first two steps are the same as above. To encode their messages, Alice and Bob divide the pair of the sequences (M_A, M_B) into two disjoint parts (M_A^1, M_B^1) and (M_A^2, M_B^2). One part is used for sending the message from Alice to Bob and another part is used for sending a message from Bob to Alice.

Security loophole of the two protocols. Here, we explicitly analyze the MDI-QSDC protocol discussed in the previous section. After Charlie has done the first set of Bell measurements of the qubit pairs of S_{A_2} and S_{B_2} in Step 1, the qubit pairs of S_{A_1} and S_{B_1} become entangled due to entanglement swapping. If the Bell measurement result of a qubit pair of S_{A_2} and S_{B_2} is in the set $\Phi = \{|\Phi^{+}\rangle, |\Phi^{-}\rangle\}$ ($\Psi = \{|\Psi^{+}\rangle, |\Psi^{-}\rangle\}$), then also the joint state of the corresponding qubit pair of S_{A_1} and S_{B_1} is in the set Φ (Ψ). So Charlie exactly knows that the qubit pair (M_{Ai}, M_{Bi}) is in the set Φ or Ψ $(1 \leqslant i \leqslant n-\delta)$.

* Corresponding author.
E-mail address: goutam.paul@isical.ac.in (G. Paul).

https://doi.org/10.1016/j.scib.2020.09.015

Alice applies σ_z on the qubits of M_A, whose corresponding initial states were $|\Psi^+\rangle$, but Charlie's knowledge about the state of (M_{Ai}, M_{Bi}) remains same.

We now show that Charlie (or any eavesdropper) can get partial information about the secret without any active attack. Let for some i, after Alice and Bob apply their unitary operators, the states M_{A_i} and M_{B_i} become N_{A_i} and N_{B_i} respectively. If the joint state $(M_{A_i}, M_{B_i}) \in \Phi$ or Ψ, then after applying I or σ_z on M_{A_i} (M_{B_i}), the joint state (N_{A_i}, M_{B_i}) ((M_{A_i}, N_{B_i})) remains in the same set Φ or Ψ respectively. In other words, both I and σ_z are applied on M_{A_i} or M_{B_i} or both M_{A_i} and M_{B_i}, map the set Φ to Φ, and Ψ to Ψ. That is, for both the mappings, the domain and the range sets are same, and if both the joint states (M_{A_i}, M_{B_i}) and (N_{A_i}, N_{B_i}) belong to the same subset of the Bell states Φ or Ψ, then Charlie concludes that the message bits are bb. Otherwise, when (M_{A_i}, M_{B_i}) and (N_{A_i}, N_{B_i}) belong to two different subsets Φ or Ψ, then Charlie concludes that the message bits are $b\bar{b}$, where $b \in \{0, 1\}$ and $\bar{b}$ = bit complement of b. Thus Charlie can get the i-th bit of the secret information with probability $1/2$, then the Shannon entropy is equal to $-\sum_{j=1}^{2} \frac{1}{2} \log \frac{1}{2} = 1$ bit. That means, only one bit among two bits of secret information is unknown to Charlie. From the viewpoint of information theory, this is equivalent to the event that, among two bits of secret information, Charlie knows the exact value of one bit and does not have any knowledge about the other bit. Thus we can say that, here in this MDI-QSDC protocol, only fifty percent of the secret message communicated securely. By the same argument, we can say that the MDI-QD protocol proposed in Ref. [1] is also not secure against information leakage. So, the main problem in this encoding rule is, Bob's random unitary operations can not lower down the information of Charlie about the secret message. In the next section, we propose a remedy to overcome this security flaw.

Proposed modifications to improve security. We modify the MDI-QSDC protocol, to make it secure against information leakage. To resolve the problem discussed above, Bob needs to apply some random unitary operators on M_{B_i} such that the union of the range sets, of his unitary operators, becomes the whole set of Bell states.

We consider two sets of linear transformations $\mathcal{F}_1 = \{I, \sigma_z\}$ and $\mathcal{F}_2 = \{\sigma_x, i\sigma_y\}$, where both the domains and ranges of these linear transformations are Φ and Ψ. Then, $f \in \mathcal{F}_1$ implies that f maps the set Φ to Φ and the set Ψ to Ψ (ignoring the global phases of the Bell states). Again, $f \in \mathcal{F}_2$ implies that f maps the set Φ to Ψ and the set Ψ to Φ. Let for any mapping f, $\mathcal{D}(f)$ and $\mathcal{R}(f)$ be the domain and range of f respectively. If Bob uses both his unitary operators from the same set $\mathcal{F}_1$ or $\mathcal{F}_2$ (i.e., Bob's unitary operator $f_1, f_2 \Rightarrow \mathcal{D}(f_1) = \mathcal{D}(f_2) = \mathcal{D}$ (say) and $\mathcal{R}(f_1) = \mathcal{R}(f_2) = \mathcal{R}$ (say), where both $\mathcal{D}$ and $\mathcal{R}$ are either Φ or Ψ), then $(N_{A_i}, N_{B_i}) \in \mathcal{R} \Rightarrow (N_{A_i}, M_{B_i}) \in \mathcal{D}$. As Charlie knows exactly the set Φ or Ψ in which the state (M_{A_i}, M_{B_i}) belongs, thus from the knowledge that $(N_{A_i}, M_{B_i}) \in \mathcal{D}$, Charlie gets the information that "both the bits of Alice's two bits message are equal or not".

Now let the two unitary operators of Bob be f_1 and f_2, where $f_1 \in \mathcal{F}_1$ and $f_2 \in \mathcal{F}_2$. Then $\mathcal{D}(f_1) = \mathcal{D}(f_2) = \mathcal{D}$ (say) implies $\mathcal{R}(f_1)$ and $\mathcal{R}(f_2)$ are disjoint, thus $\mathcal{R}(f_1) \cup \mathcal{R}(f_2)$ contains all the Bell states. As Bob randomly chooses between f_1 and f_2, therefore from the exact state of (N_{A_i}, N_{B_i}), Charlie does not know the exact set of the state (N_{A_i}, M_{B_i}).

Hence the collection of all possible choices of Bob's random unitary operator pairs, from the set of Pauli matrices, is $\{(f_1, f_2) : f_1 \in \mathcal{F}_1 \text{ and } f_2 \in \mathcal{F}_2\}$, i.e., there are four options for Bob to choose his pair of unitary operators and they are: I and σ_x; I and $i\sigma_y$; σ_z and σ_x; σ_z and $i\sigma_y$. One can easily check that, if Bob (for MDI-QD, the receiver) uses any one pair from the above set as his random unitary operators, then both the protocols prevent the information leakage problem.

In summary, we have analyzed Niu et al.'s MDI quantum communication protocols and observed that both of them insecure against information leakage, and one bit among two bits of information is always leaked without any active attack. Then we have proposed modification of these protocols, which are secure against such information leakage problem. We also characterize the set of Pauli operators, which can alternatively be used to bypass the security flaws.

Note: After submitting our current work to arXiv.org (arXiv:2006.05263), the authors of Ref. [1] corrected their flaw independently in Ref. [4] by replacing the cover operation from $\{I, \sigma_z\}$ to $\{I, \sigma_x, \sigma_y, \sigma_z\}$. They also simplified the protocol by preparing the EPR pairs all in state $|\psi^-\rangle$. However, in addition to the correction, we also discussed and analyzed the information leakage problem.

Conflict of interest

The authors declare that they have no conflict of interest.

References

[1] Niu PH, Zhou ZR, Lin ZS, et al. Measurement-device-independent quantum communication without encryption. Sci Bull 2018;63:1345–50.
[2] Zukowski M, Zeilinger A, Horne MA, et al. Event-ready-detectors Bell experiment via entanglement swapping. Phys Rev Lett 1993;71:4287–90.
[3] Nielsen MA, Chuang I. Book review: quantum computation and quantum information. Cambridge UK: Cambridge University Press; 2002.
[4] Niu PH, Wu JW, Yin LG, et al. Security analysis of measurement-device-independent quantum secure direct communication. arXiv:2006.07184, 2020.

Nayana Das is a Ph.D. student at Applied Statistics Unit in Indian Statistical Institute, Kolkata. She received her B.Sc. degree in Mathematics and M.Sc. degree in Pure Mathematics from the University of Calcutta. Her research interest is Quantum Cryptography, Quantum Information Theory and Security.

Goutam Paul is an Associate Professor at Cryptology and Security Research Unit of Indian Statistical Institute, Kolkata. He did his Bachelors of Engineering, Masters and Ph.D. degrees all in Computer Science. His doctoral research was in Classical Cryptanalysis and he is known for his attacks on RC4 that eventually paved the way for its removal from TLS protocol. His current research interest includes Classical Cryptanalysis as well as Quantum Cryptography and Quantum Information.