An approach for security evaluation and certification of a complete quantum communication system

Shihan Sajeed,[1,2] Poompong Chaiwongkhot,[2,3] Anqi Huang,[4,2,5] Hao Qin,[2,6,3,7] Vladimir Egorov,[8] Anton Kozubov,[8] Andrei Gaidash,[8] Vladimir Chistiakov,[8] Artur Vasiliev,[8] Artur Gleim,[8] and Vadim Makarov[9,3]

[1]*Department of Electrical and Computer Engineering, University of Toronto, M5S 3G4, Canada*
[2]*Institute for Quantum Computing, University of Waterloo, Waterloo, ON, N2L 3G1 Canada*
[3]*Department of Physics and Astronomy, University of Waterloo, Waterloo, ON, N2L 3G1 Canada*
[4]*Institute for Quantum Information & State Key Laboratory of High Performance Computing, College of Computer, National University of Defense Technology, Changsha 410073, People's Republic of China*
[5]*Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, N2L 3G1 Canada*
[6]*Department of Combinatorics and Optimization, University of Waterloo, Waterloo, ON, N2L 3G1 Canada*
[7]*CAS Quantum Network Co., Ltd., 99 Xiupu road, Shanghai 201315, People's Republic of China*
[8]*Faculty of Photonics and Optical Information, ITMO University, Kadetskaya line 3b, 199034 St. Petersburg, Russia*
[9]*Shanghai Branch, National Laboratory for Physical Sciences at Microscale and CAS Center for Excellence in Quantum Information, University of Science and Technology of China, Shanghai 201315, People's Republic of China*

Although quantum communication (QC) systems are currently being deployed commercially on a global scale, hardly any security certification standard and methodology exists. This is ironic since security was the main motivation behind the shift from classical to quantum cryptography. Although many studies have been performed to address individual system vulnerabilities, neither any complete system analysis has yet been reported, nor has there been any outline on how to approach the problem. This work tries to address this problem. We introduce a methodology for security evaluation and certification of a complete quantum communication system against implementation imperfections. Our proposed methodology progresses in an iterative fashion: first, security evaluation from the testing group; then patching from the manufacturer; then again security evaluation and so on. Throughout this process, the system security is gradually improved and expected to reach a level that can be trusted and widely accepted.

As an example, we present our security evaluation results performed in collaboration with the system manufacturer: ITMO University and Quantum Communication Ltd. (St. Petersburg, Russia). The manufacturer thus becomes the first commercial QKD system manufacturer to openly publish the security assessment results of their system. The project started in 2017 and has followed the proposed methodology, as described here. We also present the results of follow-up works, that consisted of joint theoretical and experimental studies, and allowed for quick improvement of implementation security of the system. We believe that our security evaluation method will pave the way for future security audits of quantum communication system and be incorporated among the future standards.

System implementation layers: To structure the security evaluation process and ensure that people with specific expertise can tackle the right problems, we subdivide the complete implementation complexity into seven layers based on a hierarchical order of information flow and control. Our layer structure – presented in Table I – is conceptually similar to the open systems interconnection (OSI) model for telecommunication systems. Just like OSI layers, a layer in our system serves the layer above it and is served by the layer below; however, unlike OSI, all our layers are inside one system, and most of them are not abstraction layers. See [1] for a detailed discussion on the functionality of these layers.

Quantifying hardness against implementation imperfections: When an imperfection is suspected to be security-critical, it is necessary to evaluate the security risks. The first step is testing. If it is found security-critical then next step is to design a countermeasure solution, and then checking the robustness of that solution. This procedure may be iterative. To standardize this process, we have categorized the implementation imperfections in terms of existing solutions as shown in Table II. See [1] for more details. Eventually, the goal of the manufacturer (and security certification) should be to update the system such that all imperfections are on level C3. Level C3 should be considered good for a commercial product, while levels C1, C0 and CX should be deemed inadequate and need to be remedied by a security update or new product development. Level C2 lies in the gray zone and while it may be considered secure for practical purposes, i.e., adequate for a commercial product, one should remember that it has no theoretical security proof based on quantum mechanics.

Security evaluation of ITMO's subcarrier wave (SCW) QKD system: The detailed working principle of this system developed by ITMO University and Quantum Communication Ltd. can be found in [7], with the analyzed version described in [1]. We have performed a complete security analysis of the bottom four layers (Q1–Q4) and examined all suspected implementation security issues according to the current knowledge. For higher layers Q5 and up, we have not performed a complete security evaluation as they lay outside our expertise area. Nevertheless, few issues in layer Q5 have been pointed out. We would like to note that no previously unknown or unfixable SCW-specific loopholes have been found dur-

TABLE I. **Implementation layers in a quantum communication system.**

Layer	Description
Q7. Installation and maintenance	Manual management procedures from the manufacturer, network operator, and end users.
Q6. Application interface	Handles the communication between the quantum communication protocol and the (classical) application that has asked for the service. For QKD this layer may transfer the generated key to an encryption device or key distribution network.
Q5. Post-processing	Handles the post-processing of the raw data. For QKD it involves preparation and storage of raw key data, sifting, error correction, privacy amplification, authentication, and the communication over a classical public channel involved in these steps.
Q4. Operation cycle	State machine that decides when to run subsystems in different regimes, at any given time, alternating between qubit transmission, calibration and other service procedures, and possibly idling.
Q3. Driver and calibration algorithms	Firmware/software routines to control low-level operation of analog electronics and electro-optical devices in different regimes.
Q2. Analog electronics interface	Electronic signal processing and conditioning between firmware/software and electro-optical devices. This includes for example current-to-voltage conversion, signal amplification, mixing, frequency filtering, limiting, sampling, timing-to-digital and analog-to-digital conversions.
Q1. Optics	Generation, modulation, transmission and detection of optical signals, implemented with optical and electro-optical components.

TABLE II. **Hardness against implementation imperfections.**

Hardness level		Description	Examples
C3.	Solution secure	Imperfection is either not applicable or has been addressed with proven security.	The threat of a photon-number-splitting attack on multiphoton pulses is eliminated by the decoy-state protocol.
C2.	Solution robust	Status of many countermeasures and systems after their initial design. With time, it may move up to C3 after a security proof is completed, or down to C1 or C0 after working attacks on it are found.	Phase-remapping in Clavis2 (the imperfection is there, but any known attack attempting to exploit it causes too many errors).
C1.	Solution partially effective	Countermeasure is successful against certain attack(s), but known to be vulnerable against at least one other attack or modification of the original attack.	Random-efficiency countermeasure against detector control in Clavis2 [2].
C0.	Insecure	Security-critical imperfection has been confirmed to exist, but no countermeasure is implemented.	Laser damage attack on the pulse-energy-monitoring detector in Clavis2 [3]; photon emission caused by detection events in certain single-photon detectors [4].
CX.	Not tested	Imperfection is suspected to exist and be security-critical, but has not been tested.	Patch for channel-calibration in Clavis2 [5]; imperfections reported in Ref. [6] against detector-device-independent QKD.

ing the analysis. Based on the received information about the system, we identified 10 potential security issues. A sample is given in Table III, and full list in [1]. Almost all the listed issues required further detailed analysis, and in many cases, in-depth experimental testing. We assigned an initial hardness level C_{init} (see Table II) to each of them. For many issues, this level was CX, meaning the issue's applicability to the system implementation needed to be studied and tested. For each issue, we also specified the corresponding Q-layers according to the classification in Table I. The risk evaluation was based on a guessed likelihood of the vulnerability, expected fraction of the secret key leakage, and estimated feasibility of exploit technology. This risk estimate should be useful for the manufacturer with limited resources to prioritize the problems.

Follow-up effort: When this collaboration began, the SCW-QKD protocol and its security proof were in final stage of development and hence the security against general attacks, privacy amplification and finite key effects had not been fully covered by ITMOs theoreticians. However, during the follow-up period, the analysis was completed, and the protocol-related issues were discussed. To date, we continue to jointly verify the security proof to ensure its integrity. These results can be found in [8, 9]. The highest risk issues of Table III have been tested experimentally in the lab, and the vulnerabilities were experimentally confirmed. For detector control attack, both detectors – used in the system – were found to be fully controllable by bright light [10]. We remark that this vulnerability remains unsolved in most existing QKD systems [11]. For the laser damage attack, the variable

optical attenuator (VOA) was tested and it was verified that laser damage changed the attenuation [12]. The manufacturer has designed countermeasures for both attacks and implemented them in the current version of the system. The testing of their robustness – the next step of the certification methodology – will be performed as a part of future work.

Several other issues from Table III have also been patched by the manufacturer. Overall, our joint work has allowed for a quick patch of most of the loopholes, thus raising current implementation hardness levels C_{curr} from CX and C0 to C2 or even C3. Countermeasures marked C2 are likely to eventually become C3, after additional experimental testing and improvement. We hope our security certification approach – the first of its kind – will pave the way for a better security certification methodology for existing and future quantum communication systems.

TABLE III: **Selected potential security issues in ITMO's subcarrier wave QKD system.** C_{init}, hardness of initial (analyzed) implementation against this security issue (see Table II), C_{curr} , hardness of the current (patched) implementation against this security issue; Q, system implementation layers involved (see Table I). Full table is available in [1].

Potential security issue	C_{init}	Q	Target component	Brief description	Needs lab testing?	Initial risk evaluation	C_{curr}	Current status
Incomplete protocol description	C0	Q1,5	Receiver	Attacks more general than collective beam splitting need to be considered in the security proofs.	No	High	C3	Was a known issue. Covered by the manufacturer after receiving the report, see [9]. The two groups continue to jointly verify the security proof.
Detector control attack	C0	Q1–5,7	SPDs	See Ref. 13.	Yes	High	C2	Loophole was experimentally confirmed and the suggested countermeasures 10 have been implemented in the current version.
Laser damage	C0	Q1,3	Alice's & Bob's optics	See Ref. 3.	Yes	High	C2	Loophole was experimentally confirmed and the suggested countermeasures 12 have been implemented in the current version.
Trojan horse	C2, C0	Q1	Alice's & Bob's optics	See Ref. 14.	Yes	Low (Alice), High (Bob)	C2 C2	Manufacturer has developed countermeasures (patent pending) to be implemented in the next system modification, and then analyzed again by the testing group.

[1] Please refer to the submitted supplementary material for more details.

[2] A. Huang, S. Sajeed, P. Chaiwongkhot, M. Soucarros, M. Legré, and V. Makarov, IEEE J. Quantum Electron. **52**, 8000211 (2016).

[3] V. Makarov, J.-P. Bourgoin, P. Chaiwongkhot, M. Gagné, T. Jennewein, S. Kaiser, R. Kashyap, M. Legré, C. Minshull, and S. Sajeed, Phys. Rev. A **94**, 030302 (2016).

[4] P. V. P. Pinheiro, P. Chaiwongkhot, S. Sajeed, R. T. Horn, J.-P. Bourgoin, T. Jennewein, N. Lütkenhaus, and V. Makarov, Opt. Express **26**, 21020 (2018).

[5] N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov, and G. Leuchs, Phys. Rev. Lett. **107**, 110501 (2011).

[6] S. Sajeed, A. Huang, S. Sun, F. Xu, V. Makarov, and M. Curty, Phys. Rev. Lett. **117**, 250505 (2016).

[7] A. V. Gleim, V. I. Egorov, Y. V. Nazarov, S. V. Smirnov, V. V. Chistyakov, O. I. Bannik, A. A. Anisimov, S. M. Kynev, A. E. Ivanova, R. J. Collins, S. A. Kozlov, and G. S. Buller, Opt. Express **24**, 2619 (2016).

[8] G. P. Miroshnichenko, A. V. Kozubov, A. A. Gaidash, A. V. Gleim, and D. B. Horoshko, Opt. Express **26**, 11292 (2018).

[9] A. Kozubov, A. Gaidash, and G. Miroshnichenko, arXiv:1903.04371 [quant-ph].

[10] V. Chistiakov, A. Huang, V. Egorov, and V. Makarov, manuscript in preparation.

[11] A. Fedorov, I. Gerhardt, A. Huang, J. Jogenfors, Y. Kurochkin, A. Lamas-Linares, J.-Å. Larsson, G. Leuchs, L. Lydersen, V. Makarov, and J. Skaar, Laser Phys. Lett. **16**, 019401 (2019).

[12] A. Huang, Á. Navarrete, R. Li, V. Egorov, S.-H. Sun, P. Chaiwongkhot, M. Curty, and V. Makarov, "Laser damage attack against optical attenuators in quantum key distribution," QCrypt 2018 conference abstract (2018), `http://www.vad1.com/publications/huang2018.QCrypt2018-subm51.pdf`.

[13] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Nat. Photonics **4**, 686 (2010).

[14] M. Lucamarini, I. Choi, M. B. Ward, J. F. Dynes, Z. L. Yuan, and A. J. Shields, Phys. Rev. X **5**, 031030 (2015).