Experimental covert communication over metropolitan distances

Yang Liu,[1] Juan Miguel Arrazola,[2] Wen-Zhao Liu,[1] Ignatius William Primaatmaja,[3] Qiang Zhang,[1,4,5] Valerio Scarani,[2,3] and Jian-Wei Pan[1,4]

[1] *CAS Center for Excellence and Synergetic Innovation Center in Quantum Information and Quantum Physics, Shanghai Branch, University of Science and Technology of China, Hefei, Anhui 230026, China*
[2] *Centre for Quantum Technologies, National University of Singapore, 3 Science Drive 2, Singapore 117543*
[3] *Department of Physics, National University of Singapore, 2 Science Drive 3, Singapore 117542.*
[4] *Department of Modern Physics and National Laboratory for Physical Sciences at Microscale, Shanghai Branch, University of Science and Technology of China, Hefei, Anhui 230026, China*
[5] *Jinan Institute of Quantum Technology, Jinan, Shandong, 250101, China*

Encryption is not enough when the sole fact that two people are communicating can be incriminating to them. Whether you are a spy in enemy territory, an employee looking for a job in the competition, or a friend trying to organize a surprise birthday party, you need more than just hiding the content of your messages: you must hide the fact that you are communicating at all. The goal of covert communication is to address this issue, by studying how to transmit information in such a way that it is not possible for an adversary to distinguish whether communication is happening or not.

Using tools from information theory, fundamental square-root laws for covert classical communication have been established for the scenario in which two parties, Alice and Bob, have access to a noisy channel and they wish to perform secure covert communication in the presence of a quantum adversary, Eve [1–4]. However, these results have been derived under a strong assumption on Eve's power, namely that she has no control over the channel and has access only to the photons that are lost in the transmission. In Ref. [5], covert communication has been extended to the quantum case, where it was shown that covert quantum communication protocols such as covert QKD are also possible, even in a setting where the adversary has full control over the channel.

In this work, we report the first experimental demonstration of covert communication over metropolitan distances, where no assumptions are made about the adversary's power. The noise in the channel – which permits covert communication to take place – originates from crosstalk in a multi-mode fibre due to bright classical signals in a channel at a neighbouring wavelength. Thus, in this scenario, regular classical communication between a sender and receiver opens the possibility of performing covert communication between the sender and another third party.

We perform a numerical optimization to obtain the optimal pulse-widths and signal intensities that maximize security and minimize the total running time of the protocol, given the constraints set by our equipment. We perform the transmission of three distinct messages of varying lengths and different security parameters, showcasing the interplay between security, message length, and running time. Our work demonstrates the feasibility of secure covert communication in a practical setting, opening the way for further improvements in both theory and experiment.

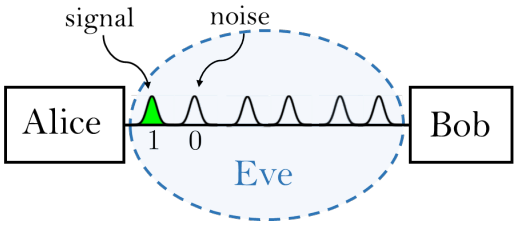

FIG. 1: Alice and Bob want to communicate covertly. They have access to $2N$ time-bin modes, which are by default in a noisy state. They randomly choose some time-bin pairs, unknown to Eve, in which they send signals. Eve has access to all outputs from Alice's lab and she can perform any attack to attempt to distinguish whether they are communicating or not.

Covert communication protocol.– Alice wants to transmit a message to Bob in such a way that Eve cannot detect that they are communicating. To quantify their ability to do so, we assume that Alice is equally likely to communicate or not, and Eve's goal is to correctly distinguish between these two scenarios. Eve's detection error probability P_e is given by $P_e = \frac{1}{2}(P_{FA} + P_{MD})$, where P_{FA} is the probability of a false alarm and P_{MD} is the probability of a missed detection. Alice and Bob's goal is to prevent Eve from performing better than a random guess, i.e. they want that $P_e \geq \frac{1}{2} - \epsilon$ for sufficiently small $\epsilon > 0$. We refer to ϵ as the *detection bias*. The setting for covert communication is illustrated in Fig. 1.

We consider the case when Alice's signals are phase-randomized weak coherent pulses with mean photon number μ at a center wavelength of 1560 nm. A single bit of information is encoded in subsequent time-bin modes, with the early time-bin encoding a "0" and the later one encoding a "1". We further assume that Alice and Bob they have access to N such time-bin pairs, each of which may be used to send a signal. The protocol for covert communication is simple: for each of the N time-bin pairs, Alice sends a qubit signal with probability $q \ll 1$, and with probability $1-q$, she does nothing. This

shared randomness that specifies the time-bins where signals are sent must be kept secret from Eve. The average number of signals sent is $d = qN$, which fixes q for a given message length.

Noise in the channel originates from cross-talk due to a coherent state signal in a neighbouring channel at 1550 nm. If there is no communication, the state of each mode is a noisy state ρ, which is a Poissonian distribution of Fock states with mean photon number $\bar{n}$. The value of $\bar{n}$ depends on the width of the signal pulses, which is an adjustable parameter of the protocol. When Alice does communicate with Bob, the state of each signal mode is given by the mixture $\sigma = (1-q)\rho + q\rho_s$, where ρ_s is the state when Alice sends a signal. The detection bias can be bounded by the expression

$$\epsilon \leq \sqrt{\frac{N}{8} D(\rho||\sigma)}, \tag{1}$$

where $D(\rho||\sigma)$ is the quantum relative entropy.

Because there are noise and losses in the channel, it is necessary to perform error-correction. We adopt the strategy of using a repetition code, where the codewords consist of k repetitions of each single bit. The repetition code allows a simple and fast encoding and decoding, as well as performing well in the presence of loss. In this case, the desired decoding error probability, the overall transmissivity of the channel, and the number of bits in the message determine the average number of signals sent. To minimize the total running time of the protocol and to maximize security, we perform a numerical optimization to deduce the optimal signal pulse widths – which determine $\bar{n}$ and the repetition rate – as well as the signal intensity μ. We find that the optimal widths correspond to 1 nanosecond, which leads to a repetition rate of 500 MHz and a noise level of $\bar{n} = 4.3 \times 10^{-4}$. The optimal signal intensity in this case is $\mu = 0.016$.

Operating the protocol at high repetition rates of 500 MHz requires precise synchronization between sender and receiver, which is usually carried out using a sync pulse. To prevent Eve from using this to detect communication, it is necessary that this pulse is also sent even when no communication takes place. Such a scheme is suitable for situations where it is not incriminating for it to be known that Alice and Bob have the potential to communicate covertly, such as would happen between employees in one company or branches of the same government. In other cases, it may be desirable to remove the need for the sync pulse. To demonstrate this, we also consider a protocol where the synchronization is performed using GPS clocks. In this case we run the experiment at 10 MHz and the optimal parameters are $\bar{n} = 0.04$ and $\mu = 0.2$.

Experiment.– In the experimental implementation of the protocol, we employ a laser set at a center frequency of 1560 nm to send the signals in the covert channel, and a transceiver centred at 1550 nm to induce noise in the covert channel via crosstalk. An NI-FPGA module is used to control the timing and pulse-width of the sent signals, and an attenuator is required to set their amplitude to the optimal value. The signal pulse width is 1 ns, which allows us to run the protocol at a repetition rate of 500 MHz. A Dense Wavelength Division Multiplexing (DWDM) system combines both channels in a single multi-mode fibre connecting Alice's and Bob's labs. The total distance between the labs is 10 kms, which is suitable for metropolitan distances. For the high-rate protocol, a sync pulse is required, which must be sent when the 1550 nm channel is used, whether or not covert communication is occurring in the 1560 nm channel. We also run the protocol without the use of a sync pulse, in this case using GPS clocks to synchronize the signals, leading to a repetition rate of 10 MHz in this case. The experimental setup is illustrated in Fig. 2.

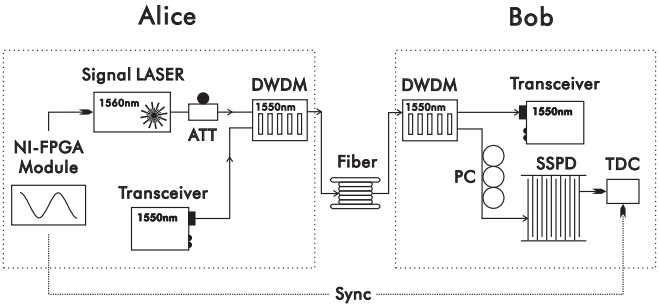

FIG. 2: Experimental setup for covert communication. A strong signal from a transceiver centred at a wavelength of 1550 nm induces noise via crosstalk on a channel with center wavelength of 1560 nm. This noise is used by Alice and Bob to perform covert communication by sending weak coherent pulses randomly spread out in time. An NI-FPGA module is used to select the pulse widths and timing of the signals, and a Dense Wavelength Division Multiplexing system combines both channels in a 10 km fibre, reaching Bob. To operate the system at high rates, a sync pulse is sent between both labs to sychronize the timing of the signals.

Eve has complete control over the channel and can use any output from Alice's lab to attempt to determine whether they are communicating or not. We require no assumptions about Eve's power other than the fact that she doesn't have access to Alice's lab and ignores the secret shared randomness used by Alice and Bob to select when they send signals. In particular, Eve has access to the outputs from Alice's lab right after they leave it, whereas Bob has to deal with the losses in the channel and the limited efficiency of his detectors in order to reliably retrieve the messages. The total transmissivity of the channel, including detector efficiency, is $\eta = 0.1$. Our protocol works appropriately even in this case.

Results.— We perform the covert transmission of three distinct messages, each varying in length, security, and repetition rate. We use an encoding in which each character is specified by a 5-bit string, leading to 32 possi-

Message	PRTYSAT@NINE	USTCCQT	LO
Detection bias	0.1	0.02	0.1
Average # signals	2,790,179	1,334,636	8,448
Time-bins	1.9×10^{12}	1.1×10^{13}	5.7×10^{8}
Repetition rate	500 MHz	500 MHz	10 MHz
Running time (s)	3,783	22,534	57
μ	3.4×10^{-3}	3.4×10^{-4}	0.16
$\bar{n}$	4.2×10^{-4}	4.2×10^{-4}	0.04

TABLE I: Summary of experimental parameters for different covert messages.

ble characters: the 26 letters of the alphabet and 6 special characters. The first message we transmit covertly is "PRTYSAT@NINE" – which conveys the information that a surprise party is happening next Saturday at 9 pm. With our encoding, this corresponds to a 60-bit message. We transmit the message with a detection bias of $\epsilon = 0.1$.

We also send the shorter message "CQTUSTC" – the acronyms of our affiliations – with a higher level of security of $\epsilon = 0.02$. For both of these messages, we operate at 500 MHz and use a decoding error probability of $\delta = 0.01$. Finally, using GPS clocks for synchronization and running at 10 MHz repetition rate, we send the message "LO" – in honour of the first ever Internet transmission – with a detection bias of $\epsilon = 0.1$ and a decoding error of $\delta = 0.01$. For each of the messages, the signal intensities, losses in the channel, and codeword size determine the average number of signals that need to be sent. Similarly, the desired level of security determines the total number of time-bins over which the signals are randomly spread, which in turn fixes the running time of the protocol. These values are summarized in Table I.

Significance of our work.— Quantum cryptography has been frequently associated exclusively with quantum key distribution. However, the landscape of cryptography is of course much larger and covert communication is a promising new research direction in the field: it is a natural problem that arises in many relevant scenarios while providing a form of security beyond encryption. Several theoretical insights have already been developed and our work presents the first demonstration of the practical feasibility of secure covert communication.

Contrary to the work of Ref. [4], where they reported a table-top experiment under the unrealistic restrictions that Eve had detectors with a large dark count rate (in fact even larger than Bob's) and where she only had access to photons lost in transmission (which were only 3% of all transmitted photons), our experiment addresses the much more challenging scenario where (i) no restrictions are made on Eve's power, (ii) the source of noise arises from a realistic effect in telecommunications and (iii) Bob has to face significant losses in transmission.

We hope that these results will be of great interest to the QCrypt community, not only because of their novelty, but because they open up a new field of research that is perfectly suited for researchers in quantum cryptography. Indeed, several advances in both the theoretical and experimental sides are possible, notably in terms of improving the performance of the protocols, tightening the security bounds, and addressing the range of applicability of covert communication techniques.

A full manuscript reporting our results is currently in preparation.

[1] B. A. Bash, S. Guha, D. Goeckel, and D. Towsley, Information Theory Proceedings (ISIT), 2013 IEEE International Symposium on pp. 1715–1719 (2013).

[2] P. H. Che, M. Bakshi, and S. Jaggi, Information Theory Proceedings (ISIT), 2013 IEEE International Symposium on pp. 2945–2949 (2013).

[3] L. Wang, in *Information Theory Workshop (ITW), 2016 IEEE* (IEEE, 2016), pp. 364–368.

[4] B. A. Bash, A. H. Gheorghe, M. Patel, J. L. Habif, D. Goeckel, D. Towsley, and S. Guha, Nature Communications **6** (2015).

[5] J. M. Arrazola and V. Scarani, Physical Review Letters **117**, 250503 (2016).