A note on quantum safe symmetric key growing

Alexander Ling,1,2 Christoph Wildfeuer,3 and Valerio Scarani1,2

1Centre for Quantum Technologies, National University of Singapore, Blk S15, 3 Science Drive 2, 117543 Singapore
2Department of Physics, National University of Singapore, Blk S12, 2 Science Drive 3, 117551 Singapore
3Institute of Microelectronics, University of Applied Sciences Northwestern Switzerland, CH-5210 Windisch, Switzerland

(Dated: July 11, 2017)

Quantum key distribution is a cryptographic primitive for the distribution of symmetric encryption keys between two parties that possess a pre-shared secret. Since the pre-shared secret is a requirement, quantum key distribution may be viewed as a key growing protocol. We note that the use of pre-shared secrets coupled with access to randomness beacons may enable key growing which, though not secure from an information-theoretic standpoint, remains quantum safe.

Quantum key distribution (QKD) is a family of optical techniques that enable two parties possessing a pre-shared secret to grow a private symmetric key. The only additional requirement to the pre-shared secret is access to a high quality source of entropy via a quantum channel. The entropy source is either controlled by one party or, when entanglement is used, may be operated by a third-party that is not necessarily trusted. The quantum channel, typically an optical link, is not controlled.

The protocols for performing QKD are well-established and numerous trials have been conducted to demonstrate the practicability of the concept. Much effort has gone into the development of QKD to extend the range of optical links, to improve the protocols for growing the secret key, and increasingly to identify and close side-channels in actual implementations.

The main appeal for QKD is that it provides information-theoretic security, or more simply ‘forward security’. If a secret key is grown correctly using QKD today, then it remains secure against any future improvements in computational power. Once in possession of this highly secure key, the users must make the decision of how to use it. The common assumption is that QKD users will deploy the key for information-theoretic encryption such as in a Vernam cipher. However, this will severely limit the quantity of data that can be encrypted, and is likely to be used only for the most critical applications.

There is growing acceptance that the key grown using QKD will be used in some type of fast symmetric encryption that provides a useful level of communications performance while ensuring security against the emergence of quantum computers. This is known as “quantum safe” encryption. Such an encryption technique generally cannot provide full forward security as it remains vulnerable to unlimited computational power, but may be sufficient for a wide range of communications data that need to be kept private for a limited period of time.

In particular, a block-cipher scheme called the Advanced Encryption Standard (AES) has been commonly identified to be quantum safe as long as the length of the seed key is of sufficient length. Existing recommendations are that the seed key be doubled from 128 bits to 256 bits leaving aside the question of how the keys are distributed and managed in the first place.

We note the possibility that methods like AES may be used to grow encryption keys in a ‘quantum safe’ manner, without the need for any quantum communication.

We consider the situation where Alice and Bob (our two parties) have a pre-shared secret, as in QKD, but instead of sharing an optical link, they now have access to a randomness beacon that both of them agree to use. The concept is illustrated in Figure 1. A randomness beacon is a broadcast service of high quality random numbers that are typically obtained from a quantum source. Each new number that is broadcast is known as a pulse. Randomness beacons can provide pulses via the Internet or radio and may also provide an authenticated historical record of its performance to allow users to gauge the quality of the randomness being provided.

Suppose that Alice and Bob treat their pre-shared secret random numbers as a master key (M), which they split into blocks of fixed size labelled $M_1, \ldots, M_n$. They label the pulses from the randomness beacon as $P_1, \ldots, P_n$. In a sense, Alice and Bob treat each pulse as an encrypted random number, which only they can decrypt uniquely given their pre-shared secret. These decrypted pulses can be used by Alice and Bob as session keys for normal communications. In other words, a session key $S_i$ would be given by $S_i = F(M_i, P_i)$, where the operation $F$ can be any quantum safe cryptographic block cipher or function. Such a method is similar to recommendations for key derivation using pseudorandom functions with the exception that in our example the function should be quantum safe.

As an example consider the scenario when Alice and Bob choose to use AES both for key growing and encrypting their regular communications. They need to keep in mind that while the quantum safe AES master key $M_i$ has to be at least 256 bits long, the function $F$ can only process pulses $P_i$ that are only 128 bits long (by definition). Hence Alice and Bob will need to concatenate the output of a sequence of operations to obtain a session key $S_i$ that is again quantum safe. Alternative options for key growing would be to use functions derived from

* cqtalej@nus.edu.sg
FIG. 1. Quantum safe symmetric key growing using (a) QKD or (b) a randomness beacon. In the QKD approach Alice operates a random number generator (RNG) to encode a raw key (K) into a stream of quantum particles that is transmitted to Bob’s detector (D). Bob measures the particles and communicates with Alice via a conventional channel authenticated with their pre-shared secret (M) to derive a key with unconditional security (U). A cryptographic function (F') may be used to obtain an expanded session key (S'). In QKD, the pre-shared secret is used in an auxiliary protocol to prevent man-in-the-middle attacks, and its entropy is not inherited by U or S'. The RNG must be under the control of one party unless they are performing entanglement-based QKD [14]. In the beacon approach, the RNG is operated at the beacon. Random numbers in the form of pulses (P) are publicly broadcast. Alice and Bob use the pulses and their pre-shared secret (M) as inputs to a cryptographic function (F) to generate the session key (S). No quantum channel is required in this case, and multi-party key growing is possible. In both cases, a quantum safe key is obtained; in the QKD case the amount of unconditionally secure entropy inherited by the derived key S’ is at best of the same length as U.

the Secure Hash Algorithm 3 (SHA-3) [17], or related functions.

In such a scheme, the security is entirely dependent on the choice of function F and as in any conventional encryption system, the decryption key M must be changed periodically. This is not different from the case in QKD where the pre-shared secret must also be replaced periodically. Furthermore, if the output of QKD is used as session keys in a block cipher such as AES those keys must also be replaced periodically.

Another area where the decryption algorithm is important is in the possibility of collisions. There may exist scenarios where an attacker has gained control of the beacon and also knows when Alice and Bob wish to update their session key. By transmitting a pulse with a specific sequence, in the instance that Alice and Bob are updating their session key, the attacker may be able to get the decryption algorithm to produce a guessable outcome. However, this can be overcome if the public beacon maintains an authenticated database of all pulses broadcast previously, allowing Alice and Bob to choose randomly from the historical record. In this sense, the ‘freshness’ of the pulses is irrelevant. In any case the quality of the quantum random number generator in QKD should also be subjected to scrutiny and investigated for possible device interference.

The ability of symmetric key block ciphers to resist quantum attacks is being investigated actively [18–20]. A recent paper estimated the resources needed to implement the Grover search algorithm to break AES blocks [20] that use key sizes of 128, 192 and 256 bits respectively. The paper provided estimates on qubit number and gate interactions needed to break AES using Grover once pre-identified ciphertext-plaintext pairs had been provided. The need for pre-identified pairs is a challenge for cryptanalysts [18–20], but it should be noted that a general weakness for encryption systems occur when pairs of plaintext-ciphertext are made available (and is generally called the ‘known plaintext attack’).

The use of a randomness beacon for quantum safe symmetric key growing has two major similarities to QKD (see Table 1). These are the use of pre-shared secrets between Alice and Bob, and a common source of random numbers. The difference is that a quantum channel is not required. Without the quantum channel one loses the possibility to achieve information-theoretic security. However, this key agreement method is extremely robust against environmental effects since the users can obtain the pulses via radio-frequency or internet services; high-speed data encryption can be carried out without having to rely on specialist technology; and key management techniques may enable multiple parties to derive a common session key, overcoming an existing bottleneck in QKD.

It is interesting to consider the use of pre-shared secrets with authenticated shared entropy sources such as randomness beacons in the context of quantum safe key growing and other related cryptographic applications. Randomness beacons that act as shared entropy sources may play a role analogous to that of the certificate authority in present day public key encryption infrastructure, and it may be worthwhile to explore the use of these beacons as part of a future quantum safe communications system.

ACKNOWLEDGEMENTS

AL would like to thank Artur Ekert, Rene Peralta and John M. Kelsey for helpful discussions. CW would like to thank Willi Meier for valuable discussions.
TABLE I. Beacon Key Distribution (BKD) vs. QKD.

|                          | BKD | QKD |
|--------------------------|-----|-----|
| Multi-party Keys         | Y   | N   |
| Quantum Channel Requirement | N  | Y   |
| Pre-shared Secret        | Y   | Y   |
| Shared Entropy Source    | Y   | Y   |
| Information-Theoretic Security | N | Y   |

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Reviews of Modern Physics 74, 145 (2002).
[2] E. Diamanti and A. Leverrier, Entropy 17, 6072 (2015).
[3] T. Schmitt-Manderbach, H. Weier, M. Fürst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kurtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter, Phys. Rev. Lett. 98, 010504 (2007).
[4] T. Scheidl, R. Ursin, A. Fedrizzi, S. Ramelow, X.-S. Ma, T. Herbst, R. Prevedel, L. Ratschbacher, J. Kofler, T. Jennewein, and A. Zeilinger, New Journal of Physics 11, 085002 (2009).
[5] S. Nauerth, F. Moll, M. Rau, C. Fuchs, J. Horwath, S. Frick, and H. Weinfurter, Nature Photonics 7, 382 (2013).
[6] C. J. Pugh, S. Kaiser, J.-P. Bourgoin, J. Jin, N. Sultana, S. Agne, E. Anisimova, V. Makarov, E. Choi, B. L. Higgins, and T. Jennewein, arXiv (2017).
[7] A. Lamas-Linares and C. Kurtsiefer, Optics Express 15, 9388 (2007).
[8] S. Nauerth, M. Frst, T. Schmitt-Manderbach, H. Weier, and H. Weinfurter, New Journal of Physics 11, 065001 (2009).
[9] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar, C. Kurtsiefer, and V. Makarov, Nature Communications (2011).
[10] ETSI, QKD Use Cases v1.1.1, Tech. Rep. (ETSI, 2010).
[11] ETSI, Quantum Safe Whitepaper ISBN No. 979-10-92620-03-0, Tech. Rep. (ETSI, 2015).