# Quantum Key Distribution Without Sifting

Extended abstract for QCrypt 2017. Full version attached.

A. B. Price[1,2,*], J. G. Rarity[1] and C. Erven[1]

[1]Centre for Quantum Photonics, University of Bristol, UK.
[2]Quantum Engineering Centre for Doctoral Training, University of Bristol, UK.
[*]alasdair.price@bristol.ac.uk

April 26, 2017

## Abstract

We propose a novel quantum key distribution protocol that uses AES to expand an initial secret, allowing us to individually authenticate every qubit, with tags that are efficient to construct. In exchange for an increase in the amount of classical data to be transmitted, the tags can be handled such that they allow secure key generation from two photon states, and make BB84 exactly 100% efficient. This can be implemented as part of a software patch on pre-existing devices as no hardware modification is required. The scheme is secure so long as AES cannot be broken, therefore it is ideal for real-world implementations that use encryption schemes other than the one-time pad.

## Background and Motivation

Assuming it is implemented perfectly, BB84 [1] is an unconditionally secure way of distributing cryptographic keys. It is of particular value for schemes that themselves offer unconditional security, such as the one time pad, but which have no intrinsic method for generating a shared secret. However, for day-to-day real-world communications, BB84-with-one-time-pad is not fast enough to be useful, so the quantum key distribution is better supplying keys to practically computationally secure applications, such as AES-256 GCM instead. In this case, BB84 still surpasses modern cryptographic alternatives, as it offers eavesdropper detection, and is secure against quantum computers. Yet a number of issues remain. Half of the qubits transmitted from Alice to Bob are discarded during sifting, rendering BB84 only 50% efficient, and photon number splitting (PNS) attacks exploit the use of weak coherent pulses in place of a single photon source.

In this more realistic system, AES GCM is now the weakest link with regards to mathematical attacks (although it is still strong in absolute terms), so we ask whether a reduction in the theoretical security of BB84 can be leveraged to counter the issues above? In addition, can this new protocol be constructed in such a way that it is vulnerable only to mathematical attacks that would break the data encryption scheme, thus giving no additional benefit to attackers who target the key generation? PNS resistance and (asymptotic) efficiency improvements are already provided by the decoy state [2] and biased basis [3] protocols respectively, both by modifying the quantum hardware. Therefore, our protocol must not require any physical changes be made to the BB84 setup. SARG04 [4] helps mitigate against PNS attacks without making hardware changes, so our protocol must overall be better than this.

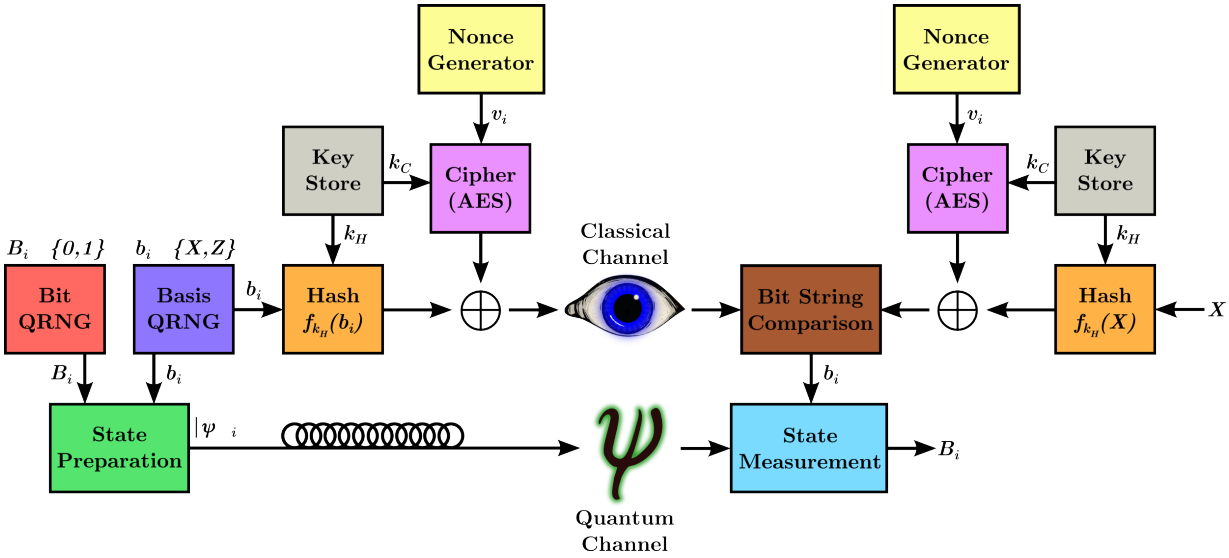


Figure 1: Block diagram showing the steps taken by Alice and Bob in order to implement quantum key distribution without sifting.

## The Protocol

Our protocol is outlined in figure 1 and can be summarised as follows:

1. As in BB84, Alice prepares her first qubit by encoding a random bit $B_i$ (0 or 1) in a random basis $b_i$ ($X$ or $Z$).

2. The qubit is delayed for a short period of time while an "authentication" tag $f_{k_H}(b_i) \oplus \mathrm{AES}_{k_C}(v_i)$ is sent to Bob. This takes the form of a computationally secure version of the authentication tag used in BB84, although it is no longer being used to authenticate a public message. $f_{k_H}(b_i)$ is a universal hash function, keyed with $k_H$, that takes the chosen basis as its input. $\mathrm{AES}_{k_C}(v_i)$ is the Advanced Encryption Standard cipher, that "expands" a key $k_C$ by operating on a nonce (arbitrary one-time number) $v_i$. Both can be computed in parallel and in advance, meaning that XORing the two together is the only operation that must happen in real time.

3. Bob compares the tag he receives with $f_{k_H}(X) \oplus \mathrm{AES}_{k_C}(v_i)$. If they are the same then, when he receives Alice's qubit, he will measure in the $X$ basis. Otherwise, he measures in the $Z$ basis. This removes the need for Alice and Bob to publicly compare their bases after the qubits have been exchanged.

4. Steps 1 to 3 are repeated for the remaining $N - 1$ qubits sent from Alice to Bob. Error correction and privacy amplification are carried out as in standard BB84.

## Security and Impact

If AES is indistinguishable from a random permutation, our protocol is secure (the 128-bit tags provide confidentiality and are difficult to forge) for up to $2^{64}$ qubits, given a single $k_H$, $k_C$ pair [5]. Our protocol is designed to distribute keys for use in AES-based encryption schemes, so if AES can be broken, there is no advantage to an attacker targeting the authentication tags, or indeed any aspect of the key exchange. Therefore, we claim not to have weakened the security in comparison to conventional QKD paired with data encryption that incorporates AES. A full analysis of the security and attack vectors can be found in [5].

With regards to fulfilling the design criteria, we observe first that Alice and Bob do not publicly announce their bases, so a traditional PNS attack will not work. A specialised form of the attack [5] will have limited success when applied to three-photon pulses, but is still no better than guesswork for two-photon terms. Secondly, as Bob always knows in advance which basis to measure in, the efficiency of the scheme is 100%. Therefore, our protocol offers higher key rates and increased resilience against photon number splitting, without modifying the standard BB84 hardware. These improvements are independent of characteristics that affect the quantum channel, such as transmission distance.

As our protocol offers advantages over BB84 and SARG04 [5], it could be implemented by means of a software update on commercial systems already in the field, which are capable of running either or both of these protocols. Although the classical channel must be able to transmit 128x the number of bits transferred over the quantum channel (as a 128-bit tag arrives before every qubit), this requirement is not unrealistic. For example, ID Quantique's Clavis$^2$ emits laser pulses clocked at 5 MHz [6], so will require a 640 Mbit/s classical channel. The Bristol and UK quantum networks, on which the Clavis$^2$ systems are being deployed, have SFP+ and QSFP channels with capacities of 10 Gbit/s and above, which is more than adequate for our needs. In the case of newer, pre-commercial devices running at super-GHz clock speeds [7], some minor modifications can be made to avoid having to multiplex two transceivers together. Reducing the tag length to 64 bits, as is possible with a UMAC [8], brings the classical data rate down by enough to be handled with QSFP28 or CFP4 transceivers. Given the bounds derived in [9], this remains secure for up to $2^{32}$ qubits, which is still greater than the minimum number required to overcome finite key effects [10]. Thus, with the QKD technology described in [7], it is possible to implement our protocol with an optical device the size of two transceivers (one for the quantum channel, one for the classical), which is no different to the physical size of that required for BB84.

## References


[1] C. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," in *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing*, 1984.

[2] H.-K. Lo *et al.*, "Decoy State Quantum Key Distribution," *Physical Review Letters*, 2005.

[3] H.-K. Lo *et al.*, "Efficient Quantum Key Distribution Scheme and a Proof of its Unconditional Security," *Journal of Cryptology*, 2005.

[4] V. Scarani *et al.*, "Quantum Cryptography Protocols Robust Against Photon Number Splitting Attacks for Weak Laser Pulse Implementations," *Physical Review Letters*, 2004.

[5] See full version (attached).

[6] ID Quantique SA, "Quantum Key Distribution System Clavis2 User Guide (v 3.0)," 2013.

[7] P. Sibson *et al.*, "Chip-based Quantum Key Distribution," *Nature Communications*, 2017.

[8] J. Black *et al.*, "UMAC: Message Authentication Code using Universal Hashing," *Network Working Group, The Internet Society*, 2006.

[9] D. Bernstein, "Stronger Security Bounds for Wegman-Carter-Shoup Authenticators," *Ann. Int. Conf. on the Theory and Applications of Cryptographic Techniques (EUROCRYPT)*, 2005.

[10] V. Scarani and R. Renner, "Quantum Cryptography with Finite Resources: Unconditional Security Bound for Discrete-Variable Protocols with One-Way Postprocessing," *Physical Review Letters*, 2008.