Secure Quantum Signatures Using Insecure Quantum Channels

Ryan Amiri[1],* Petros Wallden[2], Adrian Kent[3,4], and Erika Andersson[1]
[1]*SUPA, Institute of Photonics and Quantum Sciences, Heriot-Watt University, Edinburgh EH14 4AS, United Kingdom*
[2]*LFCS, School of Informatics, University of Edinburgh, 10 Crichton Street, Edinburgh EH8 9AB, United Kingdom*
[3]*Centre for Quantum Information and Foundations, DAMTP, Centre for Mathematical Sciences, University of Cambridge, Wilberforce Road, Cambridge, CB3 0WA, United Kingdom*
[4]*Perimeter Institute for Theoretical Physics, 31 Caroline Street North, Waterloo, ON N2L 2Y5, Canada*

EXTENDED ABSTRACT

Signature schemes allow for the exchange of messages from one sender to multiple recipients, with the guarantee that messages cannot be forged or tampered with. Additionally, messages can be transferred (if one recipient accepts a message, she is guaranteed that others will accept the same message) and cannot be repudiated (if a recipient accepts a message, the sender cannot later successfully deny that she sent it). Digital signatures are widely used and are often said to be one of the most important inventions of modern cryptography. Unfortunately, the security of commonly used signature protocols relies on the assumed computational difficulty of certain problems. In the United States, for example, there are currently three approved algorithms for generating digital signatures – RSA, DSA and ECDSA – all of which rely on the difficulty of finding discrete logarithms or factoring large primes. With the advent of quantum computers, such assumptions will no longer be valid. Due to their importance, it would be desirable to develop signature schemes providing unconditional or information-theoretic security.

Different quantum signature schemes, including the original quantum digital signature (QDS) scheme proposed in [1], are one possible solution. Their security is unconditional, relying only on laws of quantum mechanics. The simplest case for a signature scheme is the three-party scenario with a sender, Alice, and two recipients, Bob and Charlie. Any participant may be dishonest, but there are restrictions on how many participants may be dishonest. With three participants, two dishonest parties working together can trivially cheat, and thus with three parties, it is assumed that at most one party is dishonest. A recently proposed quantum signature scheme [2] uses only the same experimental components as required for quantum key distribution, and is thus the most practical such scheme to date. Essentially, Alice here randomly chooses a sequence of qubits, in the X or Z basis states. One copy of the qubit sequence was sent to Bob and one to Charlie, who make measurements to gain information about Alice's sequence of states. To later sign a message, Alice presents the message together with the full classical information of the corresponding sequence of qubit states (there is one qubit sequence per possible one-bit message, and to sign longer messages, the scheme should be suitably iterated). Since Alice uses complementary bases, neither Bob or Charlie can gain full information about her state sequences, which prevents forging, but Alice also cannot know exactly what information each of them did gain. Further, to protect against repudiation and ensure transferrability, Bob and Charlie use a secret classical channel to exchange half of their measurement outcomes. This symmetrises Bob's and Charlie's measurement statistics and ensures that Alice cannot make them disagree on the validity of a message, except with negligible probability.

So far, however, all practical quantum signature protocols have suffered from two main issues. First, they make unrealistic trust assumptions [2], [3]. In particular, also in [2] it is assumed that dishonest participants cannot eavesdrop on the quantum channels, with the expectation that this assumption could be removed by the use of a parameter estimation procedure similar to that employed in quantum key distribution (QKD). Explicitly showing that this is the case is one of the most important outstanding questions for quantum signature schemes. Second, the length of the signature required to sign a message has been too large for practical use, see e.g. [4], [5], [6]. In this paper, we present a three-party quantum signature protocol that removes all trust assumptions on the quantum channels. The protocol is shown to be secure and, in terms of resources, entirely realistic – it requires only authenticated classical channels as well as untrusted, noisy quantum channels. In addition, the protocol is much more efficient than previous protocols and significantly reduces the signature length of a message.

The increase in efficiency is largely due to the fact that in our protocol Alice sends *different* states to Bob and Charlie, whereas in most existing protocols, including the original QDS protocol [1] and the one realised in [5], she sent them the same quantum states. In previous protocols, then, even without eavesdropping, a potential forger had access to a legitimate copy of each of the states Alice sent to the participants. In generalising to N par-

ticipants with up to t colluding dishonest parties, this problem becomes more serious, since the collusion must be assumed to have t legitimate copies of each state. By sending different states to each participant, there is no such problem. A potential forger can only gain information by eavesdropping. This is a quantum-mechanical version of the classical protocol "P2" in [2]. Even though Alice sends different states to Bob and Charlie, security against repudiation still holds due to the secret exchange of elements between Bob and Charlie. We show how security against forging is given by a parameter estimation step (similar to QKD) that quantifies the amount of information a potential forger, say Bob, could have gained through eavesdropping on the states sent to Charlie.

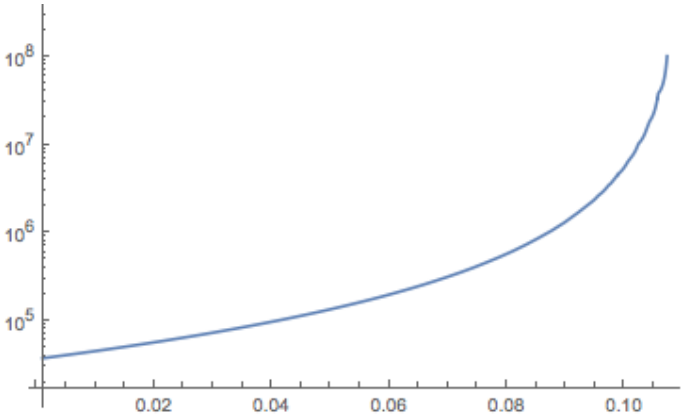

FIG. 1. Total signature length as a function of channel noise

Interestingly, the protocol can tolerate relatively high levels of noise in the quantum channels. Figure 1 shows the total signature length as a function of channel noise. Essentially, in this scheme the keys or signatures are distributed using the BB84 implementation of QKD, but without the classical post-processing typically associated with QKD, that is, without privacy amplification and error correction. In the asymptotic limit, quantum signatures are possible up to a noise level of $\approx 11\%$, the same as the asymptotic limit for BB84 QKD (ignoring pre-processing) [7]. However, for finite key or signature size, the allowable channel noise is reduced for QKD [8], due in large part to imperfect error correction, leaking extra information to Eve. For quantum signatures on the other hand, the protocol can be made secure using a finite signature length on any quantum channel with noise less than 11%, since no error correction has to be performed. In other words, quantum signatures are possible for some noise levels which render QKD impossible.

* ra2@hw.ac.uk

[1] D. Gottesman and I. Chuang, "Quantum Digital Signatures", arXiv:quant-ph/0105032v2

[2] P. Wallden, V. Dunjko, A. Kent, E. Andersson, "Quantum digital signatures with quantum-key-distribution components", Phys. Rev. A **91**, 042304 (2015).

[3] V. Dunjko, P. Wallden, E. Andersson, "Quantum Digital Signatures without Quantum Memory", Phys. Rev. Lett. **112**, 040502 (2014).

[4] P. J. Clarke et al., "Experimental demonstration of quantum digital signatures using phase-encoded coherent states of light", Nat. Commun. **3**, 1174 (2012).

[5] R. Collins et. al, "Realization of Quantum Digital Signatures without the requirement of quantum memory", Phys. Rev. Lett. **113**, 040502 (2014).

[6] R. Donsldson, R. Collins, K. Kleczkowska, R. Amiri, P. Wallden, V. Dunjko, E. Andersson, G. Buller, "Experimental demonstration of kilometre range quantum digital signatures", In preparation.

[7] R. Renner, N. Gisin, and B. Kraus, "Information-theoretic security proof for quantum-key-distribution protocols", Phys. Rev. A **72**, 012332 (2005).

[8] V. Scarani and R. Renner, "Quantum cryptography with finite resources: unconditional security bound for discrete-variable protocols with one-way post-processing", Phys. Rev. Lett. **100**, 200501 (2008).

Technical Details - Secure Quantum Signatures Using Insecure Quantum Channels

Ryan Amiri[1],* Petros Wallden[2], Adrian Kent[3,4], and Erika Andersson[1]
[1]*SUPA, Institute of Photonics and Quantum Sciences, Heriot-Watt University, Edinburgh EH14 4AS, United Kingdom*
[2]*LFCS, School of Informatics, University of Edinburgh, 10 Crichton Street, Edinburgh EH8 9AB, United Kingdom*
[3]*Centre for Quantum Information and Foundations, DAMTP, Centre for Mathematical Sciences, University of Cambridge, Wilberforce Road, Cambridge, CB3 0WA, United Kingdom*
[4]*Perimeter Institute for Theoretical Physics, 31 Caroline Street North, Waterloo, ON N2L 2Y5, Canada*

Quantum signature schemes allow for the exchange of messages from one sender to multiple recipients, with the guarantee that messages cannot be forged or tampered with. Additionally, messages cannot be repudiated – if one recipient accepts a message, she is guaranteed that others will accept the same message as well. While messaging with these types of security guarantees are routinely performed in the modern digital world, current technologies only offer security under computational assumptions. Quantum signature schemes on the other hand, offer unconditional security guaranteed by quantum mechanics. Here, we build on earlier work and remove all trust assumptions on the quantum channels to present a information theoretically secure scheme implementable with current technology. Further, in [2] it was shown that whenever QKD is possible, it is possible to perform an information theoretically secure quantum signature protocol. Here we show that there exists quantum channels for which quantum unconditionally secure signatures is possible when the underlying QKD protocol is not.

INTRODUCTION

In this paper we consider a three-party protocol with a sender, Alice, and two receivers Bob and Charlie. Previous signature schemes [1], [2] improved on the original Gottesman-Chuang scheme [3] by removing the need for quantum memory. Alice encoded her signature into quantum states and sent a copy to both Bob and Charlie, who are only able to gain partial information on the overall signature due to the quantum nature of the states. However, to prove security they relied on the assumption of authenticated quantum channels that did not allow eavesdropping. This meant that a potential forger (Bob) only had access to his own copy of the signature states sent from Alice. In reality a fraudulent Bob would be able to gain extra information on Alice's signature through eavesdropping on the signature states sent from Alice to Charlie. The protocol presented here differs from previous work in three respects: first, we remove all trust assumptions on the quantum channels, greatly increasing the actual security of quantum signatures in a practical setting; second, we show that this quantum signature protocol is possible using quantum channels which are too noisy for the underlying QKD protocol; and third, we allow Alice to send *different* signatures to Bob and Charlie, thereby increasing efficiency.

THE MODEL

We assume that between Alice and Bob and Alice and Charlie there exists authenticated classical channels as well as untrusted, noisy quantum channels. We assume Bob and Charlie share a QKD link which can be used to transmit classical messages in full secrecy. The protocol makes use of a key generating protocol (KGP) performed in pairs separately by Alice-Bob and Alice-Charlie. The KGP uses the noisy quantum channels and has just one function – it is a method of generating two bit strings, one for the sender and one for the receiver. The strings are such that the correlation between the receiver's string and the sender's string is greater than the correlation any eavesdropper could have with the sender's string. The KGP is discussed in section III.

The quantum signature protocol is split into two parts, a distribution stage and a messaging stage. We show how the protocol would work for signing a 1-bit message.

Distribution Stage

1. For each possible future one bit message, m, Alice uses the KGP to generate four different length L keys, $A_0^B, A_1^B, A_0^C, A_1^C$, with the superscript denoting with whom she performed the KGP and the subscript denoting the future message. On the other side, Bob holds the length L strings K_0^B, K_1^B and Charlie holds the length L strings K_0^C, K_1^C. Due to the KGP, we know that A_0^B is more highly correlated with K_0^B than any eavesdropper and similarly for the other strings. Alice's signature for the future message m is $Sig_m = (A_m^B, A_m^C)$.

2. For each future message, Bob and Charlie symmetrise their keys by choosing half of the bit values in their K_m^B, K_m^C and sending them over the Bob-Charlie secret classical channel to the other participant. If they chose to forward a bit value, they also "forget" its value. That is, they will not check a fu-

ture declaration of Alice against these values, they will only check her future declaration against the values they kept and the values they received from the other participant [**?**]. We denote their symmetrised keys by S_m^B and S_m^C with superscript indicating whether the key is held by Bob or Charlie. Bob (and Charlie) will keep a record of whether an element in S_m^B came directly from Alice or whether it was forwarded on to him by Charlie (or Bob).

At this point in the protocol, Bob and Charlie each know half of K_m^B and half of K_m^C (in the honest case). If, say, Bob is dishonest, he can know all of K_m^B and half of K_m^C, but will not know the half of K_m^C that Charlie chose to keep. Therefore, for each future message Bob and Charlie each have a bit string of length L and Alice has no information on whether it is Bob or Charlie who holds a particular element of the 2L length string (K_m^B, K_m^C).

Messaging Stage

1. To send a signed one-bit message m, Alice sends (m, Sig_m) to the desired recipient (say Bob).

2. Bob checks whether (m, Sig_m) matches his S_m^B and records the number of mismatches he finds. He separately checks the part of his key received directly from Alice and the part of the key received from Charlie. If there are fewer than $s_a(L/2)$ mismatches in both halves of the key, where s_a is a small authentication threshold, Bob accepts the message.

3. To forward the message to Charlie, Bob forwards the pair (m, Sig_m) that he received from Alice.

4. Charlie tests for mismatches in the same way, but in order to protect against repudiation by Alice he uses a different threshold. Charlie accepts the forwarded message if the number of mismatches in both halves of his key is below $s_v(L/2)$ where s_v is the verification threshold, with $0 < s_a < s_v < 1$.

KEY GENERATION PROTOCOL

In this section we describe how two parties, Alice and Bob, perform the KGP. As mentioned above, the aim of the KGP is to produce two classical bit strings, one held by Alice and one held by Bob, such that Alice's string is more highly correlated with Bob's string than any eavesdropper can be, even if that eavesdropper is Charlie. To do this, Alice and Bob essentially perform QKD, but without the classical post processing steps of error correction and privacy amplification. In what follows, the underlying QKD protocol upon which the KGP is built will be the BB84 protocol (with no pre-processing) described in [5]. Although we present a version of the KGP based on BB84, we note that the six-state protocol and/or pre-processing steps could be introduced without difficulty. It should be stressed that in signature schemes it cannot be assumed that either Alice or Bob is honest. As explained below, however, neither gain from dishonesty during the KGP and so we can assume they are honest. As is common in QKD, we present the entanglement-based version of the protocol with the understanding that this can be reduced to a prepare-and-measure scheme implementable with current technology [5]. Here we present the protocol as well as show why it achieves the desired functionality.

1. Alice and Bob agree on a small value of p such that they will choose to measure in the Z basis with probability $1-p$ and the X basis with probability p.

2. Bob creates $|\Phi^+\rangle^{\otimes(L+k)}$.

3. Bob sends the second half of each qubit pair to Alice over the quantum channel. When Alice receives all of the qubits, she announces this fact to Bob.

4. For each qubit, Alice and Bob jointly (and publicly) agree to apply $\sigma_x \otimes \sigma_x$ with probability 1/2, and independently, agree to apply $\sigma_z \otimes \sigma_z$ with probability 1/2.

5. Bob randomly chooses k of the qubits to use for parameter estimation (PE). For each pair of qubits, they jointly pick a basis (according to p) and both measure their qubit with respect to that basis (either X or Z). When comparing results, it is Alice who announces her measurement outcome first and it is Bob who checks this against his outcome. (*This is important for the security against repudiation.*)

6. Based on the disturbance level found in PE, Alice and Bob estimate the number of errors they have, as well as estimating the possible information Eve has. If the disturbance is too high, they abort the protocol.

7. Assuming the disturbance was not too high, they go ahead and measure the rest of the qubits in a basis agreed randomly according to p. Alice and Bob now share a classical key which, with high probability, is more highly correlated than the key of any eavesdropper.

We will consider the case when Eve is restricted to collective attacks, and show that she is less correlated with Bob's bit string than Alice. For the case of asymptotically large L, security against coherent attacks follows using the Exponential de Finetti theorem [4]. At the end of Step 4, as in [5], Alice and Bob will share the product state $\sigma_{AB}^{\otimes(L+k)}$ where σ_{AB} is a mixture of Bell states. The aim of PE in step 5 is to take k of these states and use

them to bound Eve's possible information. Following [6], for any level of noise, Q_z, observed during PE, and for any fixed choice of some parameter $\xi > 0$, there exists a choice of k such that the participants can be sure that the true noise introduced by Eve's eavesdropping is less than $\overline{Q}_z = Q_z + \xi$, except with probability ϵ_{PE}. Importantly, the value ϵ_{PE} decreases exponentially with increasing k according to

$$\epsilon_{PE} = (k+1)e^{-\frac{1}{2}k\xi^2}. \tag{1}$$

The same is true for Q_x, so in fact we will use $k/2$ of the states to bound the noise in the X basis and $k/2$ states to bound the noise in the Z basis. We can use these bounds to bound Eve's information, which is what we do now.

We give Eve full power and assume she holds a purification of each σ_{AB}. In order to generate correlated keys, Alice and Bob will make local measurements on their systems to obtain classical bits. Eve's goal is to correctly guess Bob's measurement outcome given her quantum systems $E_1, ..., E_L$. Since we are dealing with collective attacks, Eve will in general perform a collective measurement. Our goal is to bound the uncertainty Eve has on the random variable, Y_i, which represents Bob's i^{th} measurement outcome. That is, we aim to find the conditional Shannon entropy $H(Y_i|E'_1, E'_2, ..., E'_L)$, where the E'_j are classical random variables representing the possible outcomes of a general collective measurement. Taking results from [10] we find

$$\begin{aligned} H(Y_i|E_1, ..., E_n)_\rho &= H(Y_i|E_i)_\rho \\ &\leq H(Y_i|E'_1, ..., E'_L) \\ &:= h(p_e), \end{aligned} \tag{2}$$

where the last equality follows because the random variable $Y_i|E'_1, ..., E'_L$ is a classical random variable with two possible outcomes, and so $H(Y_i|E'_1, ..., E'_L)$ must equal the binary entropy, $h(p_e)$, for some $p_e \leq 1/2$. Assume that, conditional on Eve's knowledge, Bob's measurement outcome is b with probability $1 - p_e \geq 1/2$. Eve's best strategy is then to guess $Y_i = b$, leading to an error rate of p_e. Therefore, in order to lower bound p_e, it suffices to find $H(Y_i|E_i)_\rho$.

Let Q_x, Q_z be the disturbance levels in the X and Z bases observed during PE, and $\overline{Q}_x, \overline{Q}_z$ be the worst case estimates consistent with Γ_ξ from PE. Assuming the worst case, when Bob measures in the Z basis we find [7]

$$H(Y_i|E_i)_\rho = 1 - h(\overline{Q}_x). \tag{3}$$

Alice's error rates with Bob are estimated directly from PE as $\overline{Q}_z$ and $\overline{Q}_x$ for measurements in the Z and X bases respectively. Since we have a sequence of identically distributed and independent two-qubit states, overall Eve will make about Lp_e mistakes, while Alice should make at most $L\overline{Q}_z$ mistakes. For Alice to be more correlated with Bob's string than Eve, we require that $\overline{Q}_z < p_e$. If $p_e, \overline{Q}_z \leq 1/2$, this condition is equivalent to $h(\overline{Q}_z) < h(p_e)$, or

$$1 - h(\overline{Q}_x) - h(\overline{Q}_z) > 0. \tag{4}$$

If (4) is not satisfied, then Alice and Bob will abort the protocol. If it is satisfied, then they have the assurance that $p_e > \overline{Q}_z$, except with probability ϵ_{PE}. Intuitively, if there is a reasonably large (but finite) number of remaining states, it is likely that Eve will make more than $L\overline{Q}_z$ errors because her minimum error rate, p_e, is higher than $\overline{Q}_z$. This allows us to prove security against forging for the full quantum signature protocol, which is done rigorously below.

SECURITY

In this section, we prove security of the main quantum signature protocol.

Robustness

Bob aborts if either the $(1/2)L$ states received from Alice or Charlie have error rate higher than s_a. For any fixed choice of parameter $\xi > 0$, PE in the KGP is successful except with probability ϵ_{PE}, which decreases exponentially in the size of the sample used, according to (1). Let Q_B, Q_C be the Alice error rates observed during PE with Bob and Charlie respectively. Then the maximum error rate consistent with PE will be $\overline{Q} := \max\{Q_B, Q_C\} + \xi$. Choose s_a such that $s_a > \overline{Q}$, then, using Hoeffding's inequalities, the probability that Bob will find an error rate higher than s_a is bounded by

$$\mathbb{P}(\text{Honest Abort}) \leq 2\exp\left(-(s_a - \overline{Q})^2 L\right) + 2\epsilon_{PE}. \tag{5}$$

The ϵ_{PE} is added to account for the possibility of failure of PE. The factors of 2 arise due to the possibility of abort due to either the states received from Alice or the states received from Charlie.

Security Against Forging

In order to forge a message, Bob must give a declaration (m, Sig_m) to Charlie that has fewer than $s_v(L/2)$ mismatches with the unknown (to Bob) half of S_m^C sent directly from Alice to Charlie, and fewer than $s_v(L/2)$ mismatches with the half he himself forwarded to Charlie. We can assume that Bob will make fewer than $s_v(L/2)$ errors on the half that he forwarded to Charlie, and we consider only the unknown half. If parameter estimation is successful in the KGP, then we know the worst case rates at which Alice and Bob/Eve will make errors with Charlie's key; denote them $\overline{Q}, p_e$ respectively. If

the protocol was not aborted, then $\overline{Q} < p_e$, so we can choose s_v such that $\overline{Q} < s_v < p_e$. On each of the $L/2$ signature elements he is guessing, Bob will make an incorrect guess with probability p_e, independent of all other guesses (since we consider only collective attacks). Using Hoeffding's inequalities [8], the probability that Bob makes fewer than $s_v(L/2)$ errors is bounded by

$$\mathbb{P}(\text{Forge}) \leq \exp(-(p_e - s_v)^2 L) + \epsilon_{PE}. \tag{6}$$

The addition of ϵ_{PE} is to account for the possibility that parameter estimation fails, in which case the bound $p_e > \overline{Q}$ may not hold. Note that security against a fraudulent Bob derives from the Alice-Charlie KGP, in which Bob plays no part. Any dishonesty on Bob's part during the Alice-Bob KGP cannot improve his ability to forge.

Security Against Repudiation

Alice aims to send a declaration (m, Sig_m) which Bob will accept and which Charlie will reject. To do this, we must have that Bob accepts both the elements that Alice sent directly to him and the elements that Charlie forwarded to him. In order for Charlie to reject he need only reject one of either the elements he received from Alice, or the elements Bob forwarded to him. Intuitively, security against repudiation follows because of the symmetrisation performed by Bob and Charlie using the secret classical channel. Even if Alice knows and can control the error rates between A_m^B, A_m^C and K_m^B, K_m^C, she cannot control whether the errors end up with Bob or Charlie. After symmetrisation the keys S_m^B and S_m^C will each have the same expected number of errors. Using results in [11], we find

$$\mathbb{P}(\text{Repudiation}) \leq 2\exp(-(s_v - s_a)^2 L/4). \tag{7}$$

Note that security against repudiation derives from the symmetrisation performed by Bob and Charlie, in which Alice plays no part. Any dishonesty on Alice's part during either KGP can only lead to higher error rates found by Bob/Charlie. This can only harm Alice's chances to repudiate as it would lead to a larger value of L.

COMPARISON TO QKD

For the BB84 protocol performed with one way post-processing (and no pre-processing), Appendix A of [7] gives the asymptotic secret key rate as

$$r = 1 - h(Q_x) - h(Q_z). \tag{8}$$

Comparing this to (4), we see that the asymptotic condition for quantum signatures to be possible is exactly the same as the condition that the secret key rate in QKD is above zero. In both cases, for symmetric disturbance (i.e. $Q = Q_x = Q_z$), the maximum channel noise allowed is $Q \approx 11\%$.

The finite case is more interesting. For quantum signatures to be possible, the channel noise must be low enough for (4) to be satisfied. For QKD, the finite secret key rate for the asymmetric BB84 protocol used above is given in [6] to be

$$r = 1 - h(\overline{Q}_x) - (\text{Leak}_{EC} - \Delta)/L, \tag{9}$$

where Δ is a constant depending on the probabilities of failure for parameter estimation, error correction and privacy amplification. The term Leak_{EC} depends on the implementation of error correction, but must be at least equal to the asymptotic value of $Lh(Q_z)$ (perfect error correction). In practice, error correction will not be perfect and it is common to write $\text{Leak}_{EC} = Lf_{EC}h(Q_z)$ where f_{EC} is an efficiency parameter commonly estimated to be about 1.2 [6]. Overall, we get

$$r = 1 - h(\overline{Q}_x) - f_{EC}h(Q_z) - \frac{\Delta}{L}. \tag{10}$$

Comparing equations (4) and (10), we immediately see that there are channels for which quantum signatures are possible and yet QKD is not. While quantum signatures is still possible at noise levels below 11%, the QKD secret key rate drops to zero at $Q \approx 9.5\%$. Again, it should be stressed that these numbers are protocol specific, and there are different QKD protocols for which the quoted rates can be slightly increased. However, by modifying the KGP to reflect the new underlying QKD protocol, the same gains can be carried through to quantum signatures. The important point is that, because the quantum signature scheme omits the inefficient process of error correction, there should always be some region where quantum signatures is possible but QKD is not.

DISCUSSION

In this paper we have presented a quantum unconditionally secure signature protocol which improves on previous quantum signature protocols by removing all trust assumptions on the quantum channels between participants. It may be imagined that by removing such strong assumptions the efficiency of the protocol would decrease. In fact the opposite is true – our protocol significantly reduces the length signature needed to sign a message. For a typical QBER of 4% as in [13], [14], a total signature length of 9.74×10^4 is required to reduce all probabilities in (5), (6), (7) to below 10^{-4}. We compare this to previous quantum signature protocols which require a signature length of the order of 10^{10} to achieve the same level of security over 1km [14]. This comparison isn't entirely fair, as the signature length 10^{10} includes losses, whereas

our signature length is the number of states needed to be sent *and received* (in the same basis) to have security. However, it can be expected that for reasonable transmission distances the loss rate will be significantly less than the 10^{-5} difference.

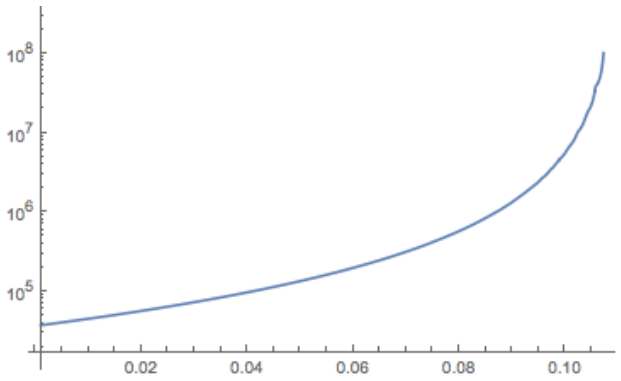

FIG. 1. Total signature length, $L+k$, as a function of channel noise

The increase in efficiency is largely due to the fact that in our protocol Alice sends *different* states to Bob and Charlie, whereas before she sent them the same states. In previous protocols it was thus always the case that, even without any eavesdropping, a potential forger had access to a legitimate copy of each of the states Alice sent to the participants. In generalising to N participants with up to t dishonest parties, this problem became even more serious since the collusion must be assumed to have t legitimate copies of each state. By sending different states to each participant there is no such problem. A potential forger can only gain information by eavesdropping, an activity ignored in previous protocols due to the trusted quantum channel assumption.

We further showed the existence of channels for which quantum unconditionally secure signatures is possible even when QKD is not. For a QBER of 10% the above QKD protocol is not possible. On the other hand, quantum signatures remains possible and a total signature length of $L+k = 5.51 \times 10^6$ again gives security of 10^{-4}.

An important open question is whether the protocol is secure against coherent attacks in the finite setting. Due to its similarity to QKD we expect it to be secure, but leave a rigorous proof for later work.

A feature of this and all other quantum signature protocols is that the length of the signature increases linearly with the size of the message to be signed. This makes such protocols highly inefficient and not well suited to practical use. It would be desirable to find a signature scheme with a better scaling. We are currently investigating a scheme which would scale logarithmically with the size of the message.

Lastly, when generalising this protocol to N participants, the number of quantum channels increases quadratically with N. In the ideal setting, quantum signature schemes exist where the number of channels scale linearly with N. So far, practical considerations (such as channel loss rates) have left all attempts at such protocols insecure. However, there seems no fundamental reason why there shouldn't be a protocol using just N quantum channels and perhaps such a scheme could be found.

* ra2@hw.ac.uk

[1] V. Dunjko, P. Wallden, and E. Andersson, "Quantum Digital Signatures without quantum memory", Phys. Rev. Lett. 112, 040502 (2014).
[2] P. Wallden, V. Dunjko, A. Kent, and E. Andersson, "Quantum digital signatures with quantum-key-distribution components", Phys. Rev. A **91**, 042304 (2015).
[3] D. Gottesman and I. Chuang, "Quantum Digital Signatures", arXiv:quant-ph/0105032v2 (2001).
[4] R. Renner, "Symmetry implies independence", Nat. Phys. **3**, 645 (2007).
[5] R. Renner, N. Gisin, and B. Kraus, "Information-theoretic security proof for quantum-key-distribution protocols", Phys. Rev. A **72**, 012332 (2005).
[6] V. Scarani and R. Renner, "Quantum cryptography with finite resources: unconditional security bound for discrete-variable protocols with one-way post-processing", Phys. Rev. Lett. **100**, 200501 (2008).
[7] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus, and M. Peev, "The Security of Practical Quantum Key Distribution", Rev. Mod. Phys. **81**, 1301 (2009).
[8] W. Hoeffding, "Probability inequalities for sums of bounded random variables", J. Amer. Statist. Assoc., **58**, 301 (1963).
[9] H.-K. Lo, H. F. Chau, and M. Ardehali, "Efficient Quantum Key Distribution Scheme And Proof of Its Unconditional Security", Journal of Cryptology **18** (2), 133-165 (2005).
[10] M. Wilde, "From Classical to Quantum Shannon Theory", arXiv:1106.1445 [quant-ph] (2011).
[11] V. Chvatal, "Tails of Hypergeometric Distributions", Discrete Math. **25**, pp. 285-287 (1979).
[12] A. Ferenczi, "Security proof methods for quantum key distribution protocols", PhD Thesis, University of Waterloo, 2013.
[13] M. Lucamarini et al. "Efficient decoy-state quantum key distribution with quantified security", Opt. Express **21**, 24550 (2013).
[14] R. Donsldson, R. Collins, K. Kleczkowska, R. Amiri, P. Wallden, V. Dunjko, E. Andersson, G. Buller, "Experimental demonstration of kilometre range quantum digital signatures", In preparation.