BB84 Quantum Key Distribution with Intrinsic Authentication

Stefan Rass
Department of Applied Informatics, System Security Group
Universität Klagenfurt, Universitätsstrasse 65-67
9020 Klagenfurt, Austria
email: stefan.rass@aau.at

Sandra König, Stefan Schauer
Digital Safety & Security Department
Austrian Institute of Technology, Klagenfurt, Austria
email: {sandra.koenig, stefan.schauer}@ait.ac.at

***Abstract*—We describe a method to authenticate the qubit stream being exchanged during the first phases of the BB84 quantum key distribution without pre-shared secrets. Unlike the conventional approach that continuously authenticates all protocol messages on the public channel, our proposal is to authenticate the qubit stream already to verify the peer's identity. To this end, we employ a second public channel that is physically and logically disjoint from the one used for BB84. This is our substitute for the otherwise necessary assumption on the existence of pre-shared secrets. Shifting authentication to the first phase of BB84 spares bandwidth during public discussion and thus makes the overall protocol also somewhat more efficient.**

Keywords–Quantum Key Distribution; Authentication; BB84

I. INTRODUCTION

It is a well recognized requirement of any quantum key distribution protocol to employ an authenticated public channel for the key distillation. Traditionally, such authentication utilizes universal hashing [1] to continuously attach message authentication codes (MACs) to all protocol messages. This continuous authentication [2] shall thwart person-in-the-middle attacks by an eavesdropper sitting in between Alice and Bob, running BB84 [3] with both of them. In that sense, quantum key distribution does not really create keys from nothing, but is rather a method of key expansion. The question discussed in this work relates to whether we can cast BB84 into a protocol that in fact *does* create keys from nothing, while retaining the security of "conventional BB84".

To this end, observe that it may already be sufficient for Alice to verify Bob's identity, if she can somehow verify that Bob is really the person from which her received qubit stream originated. One possibility to do so is to ask Bob for the way in which he created the stream, say as a pseudorandom sequence, so as to prove his identity. Of course, it is neither viable nor meaningful in our setting to let Bob create his entire qubit stream pseudorandomly, but it may indeed be useful to have him embed pseudorandom bits at a priori unknown places, while leaving the rest of the stream truly random. Alice, in an attempt to verify Bob as the "owner" of the qubit stream, may ask Bob for the seeds to recover the pseudorandom bits and their positions. An eavesdropper, on the other hand, cannot reasonably pre-compute Bob's response to Alice's inquiry, if the pseudorandom bits cannot be recognized (distinguished from) the truly random bits. While this apparently induces a flavour of computational security (indistinguishability of pseudorandom from really random), we can almost avoid threats by computationally unbounded adversaries. To see why, assume that the pseudorandom sequence originates via iterative bijective transformations from a uniformly distributed and truly random seed. If so, then all pseudorandom bits will themselves enjoy a uniform distribution. As being embedded inside another sequence of independent uniformly distributed bits, the distribution of the pseudorandom bits is identical to that of the truly random bits. Despite the correlation that inevitably exists among the pseudorandom bits, the distributions are nevertheless indistinguishable, except in case when the positions of the pseudorandom bits are known a priori. However, since these positions are chosen secretly and independently of any publicly available information, the attacker has no hope better than an uninformed guess about which positions matter.

Organisation of the paper: The following Sections I-A and I-B give details on BB84 to the extent needed in the following, and relate the proposal to other solutions in the literature. Section II expands the technique how we embed pseudorandom bits into the qubit stream during BB84. Section III discusses the security of our modified version of BB84, and Section IV draws conclusions.

A. BB84 at a Glance

The BB48 protocol has first been presented by Bennett and Brassard [3]. It allows two communication parties, Alice and Bob, to generate a classical key between them by using the polarization of single photons to represent information. Therefore, Alice is in possession of a single photon source and prepares the photons randomly according to the horizontal/vertical basis (Z-basis) and the diagonal basis (X-basis), i.e., for each photon she prepares one of states $\{|0\rangle, |1\rangle\}$ and $\{|x+\rangle, |x-\rangle\}$, respectively. After Alice choses the basis, the qubit is sent to Bob, who performs a measurement on it. Since Bob does not know which basis Alice used for the preparation he does not know which measurement basis he should use and thus he will not be able to retrieve the full information from each qubit. Hence, the best strategy for him is to randomly choose between the Z- and X-basis for his measurement himself. In this case Bob will choose the correct basis half of the time – but he does not know in which cases he has guessed right. Thus, Alice and Bob compare the choice of their bases in public after Bob measured the last qubit.

During the *sifting phase* [4], Alice and Bob eliminate their measurement results for those measurements where they used different bases. The remaining measurement results are converted into classical bits using the mapping

$$\begin{aligned} \{|0\rangle, |x+\rangle\} &\longrightarrow 0 \\ \{|1\rangle, |x-\rangle\} &\longrightarrow 1. \end{aligned} \tag{1}$$

At this stage, Alice and Bob should have identical classical bit strings if the channel is perfect (noiseless channel, no eavesdropper). In reality, a certain error rate is introduced in the

 ISBN: 978-1-61208-431-2

protocol due to physical limitations (lossy and noisy channels, imperfect devices, no single photon sources, etc.). To estimate this error rate, Alice and Bob publicly compare a fraction of their results in public to check whether they are correlated. Then, classical error correction protocols are used to identify and eliminate the differences in their bit strings. Such a procedure that has been heavily used for error correction is the *CASCADE* algorithm first introduced by Bennett et al. [5]. Due to the fact that Alice and Bob publicly compare some information during the error correction, an adversary is able to obtain further information about the secret bit string (assuming Eve's presence has not been detected during error correction). Therefore, a last process called *privacy amplification* [6] performed by Alice and Bob uses *strongly-universal$_2$ hash functions* (as presented in [7] and recently discussed in [8]) to minimize the amount of information leaked to the adversary. After all, the security of QKD protocols has been discussed in depth and various security proofs have been provided, for example, in [9] or [10]. A main result of these proofs shows that Alice and Bob are still able to establish a secret key, if the error rate is below a maximum value of $\simeq 11\%$ [9].

B. Related Work

There have been several approaches to replace the authentication protocol for the classical channel by quantum approaches. For example, an authentication scheme is presented in [11], which provides an increased conditional entropy for the seed of the adversary and which is optimized for scenarios where the shared symmetric key used in the authentication becomes extremely short.

Other protocols entirely eliminate the classical channel thus also eliminating the need for classical authentication [12]. Such protocols make use of quantum authentication, a topic which has been studied for more than 15 years and which has already been formally defined in 2002 [13]. Quantum authentication protocols perform the task of authentication with little or no help of classical cryptography solely using quantum mechanical sources. Hence, some of these protocols combine QKD protocols with authentication [14] or use quantum error correction for the authentication of the communication parties [15]. Other quantum authentication protocols also use entanglement as a source for authentication (e.g., [16][17][18] to name a few). Entangled states consist of two or more particles which have the specific property that they give completely correlated results when the respective particles are measured separately. As it has been shown by Bell [19], as well es Clauser et al. [20], this correlation can be verified if the measurement results violate some special form of inequalities. In some QKD protocols, for example the Ekert protocol [21], this argument is used to generate a secure key, but these protocols still require an authenticated classical channel (cf. [21]).

II. Assembling Authentication into the Protocol

In a standard person-in-the-middle scenario, we have Eve sitting in between Alice and Bob, executing BB84 with both of them simultaneously.

Alice and Bob, to authenticate one another, make contact *out of band*, by contacting the other on a physically and logically separate channel that Eve has not intercepted. In that sense, we augment the usual picture of BB84 by another channel, shown dashed in Figure 1.

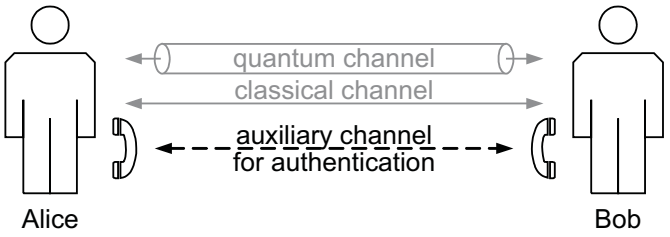

Figure 1. Channel configuration of our enhanced protocol

The key point here is that during the public discussion phase of BB84, Alice and Bob both reveal to each other their entire random sequence of polarization settings, along which their – so far private – random sequences are disclosed. Within these private random sequences, Alice will embed a pseudorandom subsequence that is indistinguishable from the truly random rest of the sequence, but for which she can tell Bob the way in which she constructed the bits and their positions. Our intuition behind this is that Alice, running BB84 with Eve, and Eve in turn running BB84 with Bob, Eve will not know (nor can determine) which of the transmitted bits are pseudorandom, and which are not. In turn, she cannot reproduce or relay these specific bits to her communication with Bob, in order to mimic Alice's behavior correctly.

Upon authentication, which happens after the public discussion phase and before the final key is distilled, Bob will get the information required to reproduce Alice's pseudorandom sequence on his own. If he were talking to Eve instead, his recorded bitstream will – with a high likelihood – not match what he received from Eve, thus revealing her presence.

Now, let us make this more rigorous. In the following, let $|x|$ denote the bitlength of a string x, and let $t \in \mathbb{N}$ be a security parameter. By the symbol $x \xleftarrow{r} \Omega$, we denote a uniformly random draw of an element x from the set Ω. Let $\mathcal{H} = \left\{ H_k : \{0,1\}^t \to \{0,1\}^t \,|k \in \{0,1\}^t \right\}$ be a family of *permutations*, which will act as uniform hash-functions in our setting (note that our scenario permits this exceptional assumption, as our goal is not as usual on hashing arbitrarily long strings, but on producing pseudorandom sequences by iteration). Furthermore, let m be an integer that divides 2^t.

Under this setting, let us collect some useful observations: take $x \xleftarrow{r} \{0,1\}^t$, then for any k, the value $H_k(x)$ must again be uniformly distributed over $\{0,1\}^t$, since H_k is a permutation. Likewise, since m divides 2^t, the value $H_k(x) \mod m$ is uniformly distributed over $\{0,1,\ldots,m-1\}$.

To embed authentication information in her bit stream, Alice secretly chooses two secret values $k_v, k_p \xleftarrow{r} \{0,1\}^t$ define a permutation H_{k_v} on $\{0,1\}^t$ and a function $h_k(x) := 1 + [H_{k_p}(x) \mod m]$ on $\{1,2,\ldots,m\}$. Using these two functions, she produces a pseudorandom sequence of *values* $v_{n+1} = H_{k_v}(v_n)$ and another (strictly increasing) pseudorandom sequence of *positions* $p_{n+1} = p_n + h_{k_p}(p_n)$, with starting values $v_0, p_0 \xleftarrow{r} \{0,1\}^t$.

Within the first phase of BB84, i.e., when the randomly polarized qubits are being transmitted, Alice uses the pseudorandom information $f(v_i)$ whenever the p_i-th bit is to be transmitted, and true randomness otherwise. In other words, Alice constructs the bitstream

$$(b_n)_{n\in\mathbb{N}} = (b_0, b_1, \ldots, b_{p_i-1}, b_{p_i} = f(v_i), b_{p_i+1}, \ldots) \quad (2)$$

 ISBN: 978-1-61208-431-2

with truly random b_i whenever $i \notin \{p_0, p_1, \ldots\}$ and inserts a pseudorandom value v_i at each position p_i for $i = 1, 2, \ldots$. This sequence determines the respective qubit stream upon polarizing photons according to $(b_n)_{n\in\mathbb{N}}$.

A. Authentication

To authenticate, Bob calls Alice on a separate line and asks for k_p, k_v, v_0, p_0, which enables him to reproduce the pseudorandom sequence and bits and to check if these match what he has recorded. He accepts Alice's identity as authentic if and only if all bits that he recorded match what he expects from the pseudorandom sequence. The converse authentication works in the same way.

B. The Auxiliary Public Channel

We stress that the auxiliary public channel does not need to be confidential. However, some sort of authenticity is assumed, but without explicit measures for it. This is because authenticity in our proposal relies on the assumption that the adversary is unable to intercept *both* public channels at the same time (otherwise, a person-in-the-middle attack is impossible to counter in the absence of pre-shared secrets).

The assumption of an auxiliary public channel puts security to rest on Eve not intercepting now two public channels simultaneously. If more such channel redundancy is available, then known techniques of multipath transmission allow to relax our assumption towards stronger security (by enforcing Eve to intercept > 2 paths in general). We believe this approach to practically impose only mild overhead, since many reference network topologies and multi-factor authentication systems successfully rely on and employ multiple independent and logically disjoint channels, at least for reasons of communication infrastructure availability. Suitable multipath transmission techniques [22] are well developed and successfully rely on exactly this assumption (although pursuing different goals [23]). Moreover, a common argument against multipath transmission (which technically offers an entirely classical alternative to quantum key distribution with very similar security guarantees) that relates to the blow-up of communication overhead does not apply to our setting here. The amount of information being exchanged over the auxiliary (multipath) channel is very small, thus making the additional overhead negligibly small. Therefore, the only physical obstacle that remains is a topology permitting the use of multiple channels; however, many physical network reference topologies are at least bi-connected graphs and thus offer the assumed additional channel (besides the usually valid assumption on the co-existence of independent communication infrastructures besides the quantum network).

III. Security

First, observe that endowing Eve with infinite computational power could essentially defeat any form of authentication, since Eve in that case could then easily intercept Alice and Bob's communication by a two-stage attack: First, she would let Alice and Bob do a normal run of BB84, sniffing on the authenticated public discussion and doing passive eavesdropping to make Alice and Bob abort the protocol and abandon the key. Before Alice and Bob restart again, Eve can – thanks to unlimited computing power – extract or simply guess-and-check the authentication secret, so as to perfectly impersonate Alice and Bob as person-in-the-middle during their next trial to do BB84. If Alice and Bob decide to use another authentication secret this time, Eve will fail the authentication but will have further data to learn more authentication secrets, until Alice and Bob eventually run out of local keys. Thus, Eve has a good chance to succeed ultimately.

Even if a universal hash function is in charge, the universality condition and the fact that strings of arbitrary length are hashed, both guarantee the existence of more than one possible key (hashes) that would produce the given result. Thus, the residual uncertainty about the authentication secret remains strictly positive. However, this residual uncertainty is not necessarily retained in cases where consistency with three or more MACs is demanded.

Therefore, it appears not too restrictive to assume that Eve cannot recognize the pseudorandom part in $(b_n)_{n\in\mathbb{N}}$ from the truly random portion, as neither the number nor the position of the pseudorandom bits is known. In other words, if N bits have been used, then Eve would have to test all 2^N subsets against their complements to decide which bits to pass through in either direction. However, even if she succeeds and recognizes which bits are the pseudorandom ones and how they have been created (i.e., if she finds the proper keys and preimages to the hash-values), this information becomes available too late, as the relevant protocol phase has been completed by this point.

Let us compute the likelihood for Alice to tell Bob the correct values, although Bob ran BB84 with Eve who impersonated Alice. Hence, the chances for Eve to remain undetected equal the likelihood for Alice's and Bob's pseudorandom sequences to entirely match by coincidence. We compute this probability now.

Let $X_1, \ldots, X_n$ be the random variables (position *and* value) corresponding to Alice's pseudorandom part in $(b_n)_{n\in\mathbb{N}}$. Likewise, let $y_1, \ldots, y_n$ be what Bob expects these values to be upon Alice's response to his authentication request. Define the random indicator variable $\chi_k = 1 :\Longleftrightarrow X_k = y_k$, for $1 \leq k \leq n$. Bob buys Alice's claimed identity if and only if $\sum_{k=1}^{n} \chi_k = n$. Hence, we look for a tail bound to $S_n := \sum_{k=1}^{n} \chi_n$ in terms of n.

By construction, the sequence $X_1, \ldots, X_n$ is identically but not independently distributed. More precisely, each realization x_k of X_k points to a position p_k and value $v_k = b_{p_k}$ expected at this position, where position and value are stochastically independent.

So, let us compute the likelihood that Bob finds the expected bit at the told position, i.e.,

$$\Pr[X_k = y_k] = \mathbb{E}[\chi_k] = \Pr[b_{p_k} = v_k] \tag{3}$$

Since each b_i in the sequence $(b_i)_{i=1}^{n}$ is uniformly distributed irrespectively of its particular position, we get $\Pr[b_{p_k} = v_k] = 1/2$. Hence, as $\mathbb{E}[\chi_k]$ is bounded within $[0, 1]$ and the expectations of all $\mathbb{E}[\chi_k]$ are independent (although the χ_k's themselves are indeed dependent as emerging from a deterministic process), we can apply Smith's version [24] of the Hoeffding-bound to obtain

$$\Pr[S_n - \mathbb{E}[S_n] \geq \varepsilon] \leq \exp\left(-\frac{2\varepsilon^2}{n}\right) \tag{4}$$

Applied to the event $S_n \geq \varepsilon + \mathbb{E}[S_n] = n$ and considering $\mathbb{E}[S_n] = \sum_{k=1}^{n} \mathbb{E}[\chi_k] = n/2$ we may set $\varepsilon = n/2$ to conclude

 ISBN: 978-1-61208-431-2

that a pseudorandom sequence constructed from random, i.e., incorrect, authentication secrets, will make Bob accept with likelihood

$$\Pr[\text{all } X_n \text{ match}|\text{incorrect seeds}] = \Pr[S_n \geq n] \leq e^{-n/2}. \quad (5)$$

Now, we can compute the overall probability of a successful impersonation from the law of total probability. Eve will successfully convince Bob to be Alice, if any of the following two events occur:

E_1: She correctly guesses the authentication secrets, in which case Bob's reconstructed pseudorandom sequence matches his expectations. Thus, $\Pr[\text{all } X_n \text{ match}|\text{correct seeds}] = 1$, obviously. However, $\Pr[E_1] = 2^{-O(t)}$, since the authentication secrets are chosen independently at random and have bitlength t (implied by the security parameter).

E_2: She incorrectly guesses the authentication secrets, and thus presents a "random" pseudorandom sequence to Bob. The likelihood of success is bounded by (5), and the likelihood for E_2 to occur is $1 - 2^{-O(t)}$.

The law of total probability then gives

$$\Pr[\text{Bob accepts}] = \Pr[\text{all } X_n \text{ match}] = \quad (6)$$
$$= \Pr[\text{all } X_n \text{ match}|E_1]\Pr[E_1]$$
$$+ \Pr[\text{all } X_n \text{ match}|E_2]\Pr[E_2] \quad (7)$$
$$\leq e^{-n/2}(1 - 2^{-O(t)}) + 2^{-O(t)} \leq 2^{-O(t+n)}, \quad (8)$$

where n is the number of pseudorandom bits embedded, and t is the security parameter (bitlength of authentication secrets).

IV. Conclusion

Authentication is a crucial issue for quantum key distribution and can be tackled in several ways. Traditionally, this matter is handled by authentication based on strong symmetric cryptography, which makes shared secrets necessary in the standard setting. These shared secrets can, however, be replaced by assumptions on the availability of additional communication channels, similarly as in multipath communication. Indeed, by having the peers in a BB84 protocol embed pseudorandomness in their qubit stream, we can use out of band authentication in a straightforward form to secure a BB84 execution. Our treatment here so far does not account for measurement errors, say when a pseudorandom qubit goes lost (recovery from measurement errors may be easy upon simply discarding lost qubits from the check; at the cost of taking more pseudorandom bits accordingly), or discusses applications to other forms of quantum key distribution. Details, issues and implications of such modifications in other protocols are to be discussed in future work.

References

[1] D. R. Stinson, "Universal hashing and authentication codes," in CRYPTO '91: Proceedings of the 11th Annual International Cryptology Conference on Advances in Cryptology. London, UK: Springer, 1992, pp. 74–85.

[2] G. Gilbert and M. Hamrick, "Practical quantum cryptography: A comprehensive analysis (part one)," 2000, [retrieved: june, 2015]. [Online]. Available: http://arxiv.org/abs/quant-ph/0009027

[3] C. Bennett and G. Brassard, "Public key distribution and coin tossing," in IEEE International Conference on Computers, Systems, and Signal Processing. Los Alamitos: IEEE Press, 1984, pp. 175–179.

[4] B. Huttner and A. Ekert, "Information Gain in Quantum Eavesdropping," J. Mod. Opt., vol. 41, no. 12, 1994, pp. 2455–2466.

[5] C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, "Experimental Quantum Cryptography," J. Crypt., vol. 5, no. 1, 1992, pp. 3–28.

[6] C. H. Bennett, G. Brassard, and J. M. Robert, "Privacy Amplification by Public Discussion," SIAM Journal of Computing, vol. 17, no. 2, 1988, pp. 210–229.

[7] M. N. Wegman and J. L. Carter, "New Hash Functions and their Use in Authentication and Set Equality," Journal of Computer and System Science, vol. 22, 1981, pp. 265–279.

[8] T. Tsurumaru and M. Hayashi, "Dual Universality of Hash Functions and Its Applications to Quantum Cryptography," IEEE Transactions on Information Theory, vol. 59, no. 7, 2013, pp. 4700–4717.

[9] P. Shor and J. Preskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol," Phys. Rev. Lett., vol. 85, no. 2, 2000, pp. 441–444.

[10] R. Renner, "Security of quantum key distribution," Ph.D. dissertation, Dipl. Phys. ETH, Zurich, Switzerland, 2005.

[11] F. M. Assis, A. Stojanovic, P. Mateus, and Y. Omar, "Improving Classical Authentication over a Quantum Channel," Entropy, vol. 14, no. 12, 2012, pp. 2531–2549.

[12] N. Nagy and S. G. Akl, "Authenticated quanntum key distribution without classical communication," Parallel Processing Letters, vol. 17, no. 03, 2007, pp. 323–335.

[13] H. Barnum, C. Crepeau, D. Gottesman, A. Smith, and A. Tapp, "Authentication of Quantum Messages," in Proceedings of the 43rd Annual IEEE Symposium on the Foundations of Computer Science (FOCS'02). IEEE Press, 2002, pp. 449–458.

[14] M. Dušek, O. Haderka, M. Hendrych, and R. Myska, "Quantum Identification System," Phys. Rev. A, vol. 60, no. 1, 1999, pp. 149–156.

[15] J. G. Jensen and R. Schack, "Quantum Authentication and Key Distribution using Catalysis," quant-ph/0003104 v3, 2000, [retrieved: june, 2015]. [Online]. Available: http://arxiv.org/abs/quant-ph/0003104

[16] H. N. Barnum, "Quantum Secure Identification using Entanglement and Catalysis," quant-ph/9910072 v1, 1999, [retrieved: june, 2015]. [Online]. Available: http://arxiv.org/abs/quant-ph/9910072

[17] Y.-S. Zhang, C.-F. Li, and G.-C. Guo, "Quantum Authentication using Entangled State," quant-ph/0008044 v2, [retrieved: june, 2015]. [Online]. Available: http://arxiv.org/abs/quant-ph/0008044

[18] M. Curty and D. J. Santos, "Quantum Authentication of Classical Messages," Phys. Rev. A, vol. 64, no. 6, 2001, p. 062309.

[19] J. Bell, "On the Einstein Podolsky Rosen Paradox," Physics, vol. 1, 1964, pp. 403–408.

[20] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, "Proposed Experiment to Test Local Hidden-Variable Theories," Phys. Rev. Lett., vol. 23, no. 15, 1969, pp. 880–884.

[21] A. Ekert, "Quantum Cryptography Based on Bell's Theorem," Phys. Rev. Lett., vol. 67, no. 6, 1991, pp. 661–663.

[22] M. Fitzi, M. K. Franklin, J. Garay, and S. H. Vardhan, "Towards optimal and efficient perfectly secure message transmission," in 4th Theory of Cryptography Conference (TCC), ser. Lecture Notes in Computer Science LNCS 4392, S. Vadhan, Ed. Springer, 2007, pp. 311–322.

[23] H. Han, S. Shakkottai, C. V. Hollot, R. Srikant, and D. Towsley, "Multi-path TCP: a joint congestion control and routing scheme to exploit path diversity in the internet," IEEE/ACM Trans. Netw., vol. 14, December 2006, pp. 1260–1271.

[24] W. D. Smith, "Tail bound for sums of bounded random variables," scorevoting.net/WarrenSmithPages/homepage/imphoeff.ps, April 2005, [retrieved: june, 2015].

 ISBN: 978-1-61208-431-2