Implementation and Evaluation of Intrinsic Authentication in Quantum Key Distribution Protocols

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, Oliver Maurhart
Digital Safety & Security Department
Austrian Institute of Technology, Klagenfurt, Austria
email: {sandra.koenig, stefan.schauer, oliver.maurhart}@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. To practically verify the expected improvement in terms of bandwidth consumption during the public discussion part of BB84, we implemented the scheme within an existing BB84 framework, and emulated the additional public channel used by Bob with the help of additional messages on the same channel. On this implementation, simulations were conducted that confirm the efficiency, bandwidth improvements and to illustrate the difficulties in forging an authentication based on the qubit streams only (as a person-in-the-middle attack is already detected before the public discussion part in our variant of BB84).**

Keywords*–*Quantum Key Distribution; Authentication; BB84; QKD Implementation; Experimental Quantum Key Distribution

I. Introduction

It is a well recognized requirement of any quantum key distribution protocol to employ an authenticated public channel for the key distillation. This channel can be constructed in various ways, for example by embedding pseudorandom bits in the initial qubit streams to authenticate, as we already showed in [1]. In this extended version of the article, we will show how this method can be implemented and described its benefits.

Most existing QKD protocols use information-theoretically secure authentication based on universal hashing [2] to continuously attach message authentication codes (MACs) to all data being exchanged during the public discussion. Thus, an interception of the qubit streams is not detected until the public discussion starts. This continuous authentication [3] shall thwart person-in-the-middle attacks by an eavesdropper sitting in between Alice and Bob, running BB84 [4] 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 sequences), 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 III-A and II give details on BB84 to the extent needed in the following, and relate the proposal to other solutions in the literature. Section IV expands the technique how we embed pseudorandom bits into the qubit stream during BB84. Section V discusses the security of our modified version of BB84, and Section VII draws conclusions.

II. State of the Art

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 [5], 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 [6]. Such protocols make use of quantum authentication, a topic that has been studied for more than 15 years and which has already been formally defined in 2002 [7]. 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 [8][9][10] or use quantum error correction for the authentication of the communication parties [11]. Other quantum authentication protocols also use entanglement as a source for authentication (e.g., [12][13][14][15][16] to name a few), or employ a third party [17].

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 [18], as well as Clauser et al. [19], this correlation can be verified if the measurement results violate some special form of inequalities. In some QKD protocols, for example the Ekert protocol [20] (among others [21]), this argument is used to generate a secure key (cf. the next section), but these protocols still require an authenticated classical channel (cf. [20]).

III. Quantum Key Distribution Protocols

In this section, we will provide a short overview on basic QKD protocols together with their key concepts. We will focus on the so-called "prepare and measure" protocols describing the BB84 protocol [4] (which we will use later on as an example for the implementation of our methodology), the B92 protocol [22], the six-state protocol [23] as well as the BBM92 protocol [24]. There are, of course, more advanced versions of QKD protocols, like the SARG protocol [25], but we will not look at them in the scope of this article and will refer the interested reader to the literature.

A. BB84 Protocol

The BB84 protocol has first been presented by Bennett and Brassard [4]. 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* [26], 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 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. [27]. 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* [28] performed by Alice and Bob uses *strongly-universal*$_2$ *hash functions* (as presented in [29] and recently discussed in [30]) 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 [31] or [32]. 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 $\simeq 11\%$ [31].

B. B92 Protocol

In 1992 Charles Bennett pointed out that two non-orthogonal states instead of four would be enough to perform the BB84 protocol [22]. The idea is that two non-orthogonal states can not be perfectly distinguished but they can be distinguished without making a wrong decision using positive operator-valued measurement (POVM) [33]. That means when Bob measures the state sent by Alice he will never make a wrong decision but sometimes he will not be able to make any decision at all.

Alice prepares one of the states $|\varphi\rangle$ and $|\psi\rangle$, where $|\varphi\rangle$ codes for a classical 0 and $|\psi\rangle$ for a classical 1. She sends the qubit to Bob, who uses three POVM operators, which are designed to distinguish between $|\varphi\rangle$ and $|\psi\rangle$ in one-half of the cases. In detail, when Bob measures the qubit coming from Alice he obtains a correct result half of the time. For the other half he obtains an inteterminate result and both parties have to eliminate that qubit. Similarly to the BB84 protocol, Bob announces where his measurements were indeterminate and the corresponding measurement results must be discarded in the end. For the remaining results, Alice and Bob publicly announce a fraction of them to check whether they are really correlated. If the error rate is above some predefined threshold, they have to assume that it is due to the presence of an eavesdropper rather than a noisy quantum channel or imperfect devices and they restart the protocol.

C. Six-State Protocol

A natural extension of the BB84 protocol is the *six state protocol* [23]. In this protocol, additionally to the Z- and the

X-basis the third complementary basis, i.e., the Y-basis is introduced, having

$$|y+\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle + i|1\rangle\Big), \qquad |y-\rangle = \frac{1}{\sqrt{2}}\Big(|0\rangle - i|1\rangle\Big). \tag{2}$$

This extension is called "natural" because in this case all three dimensions of the Bloch sphere are used. Alice chooses randomly one of the six states and sends it to Bob. Bob has to select one out of three (instead of two as in the BB84 protocol [4]) bases and performs a measurement on the received qubit. Hence, his choice will correspond to Alice's preparation only in $1/3$ of the cases such that they will have to discard a greater amount of qubits when they publicly compare their measurement bases. As in the other protocols described above, Alice and Bob choose a certain fraction of the remaining measurement results and compare them in public to check if an eavesdropper is present. The major advantage of the six state protocol is that it is more sensitive to attacks and an adversary will have a smaller chance to stay undetected.

D. BBM92 Protocol

Whereas the BB84 protocol just discussed above is based on single photon sources, Ekert presented a protocol in 1991 [20], which uses a source emitting maximally entangled qubit pairs, i.e., the Bell states $|\Phi^{\pm}\rangle, |\Psi^{\pm}\rangle$. In principle, this source is located between Alice and Bob and one qubit of the entangled state is flying to Alice and the other one to Bob. In practice, when looking at implementations of the Ekert protocol it will be more common that one of the communication parties is in possession of the source.

In the Ekert protocol, Alice and Bob also randomly measure the polarization of their qubit, but they use different angles at Alice's and Bob's side. These angles are non-orthogonal and are later used to violate the CHSH-inequalities [19]. The CHSH-inequalities provide an indication that the quits are originally coming from an entagled state, i.e., the inequalities are violated if an entangled state is present.

In 1992 Bennett, Brassard and David Mermin presented a variant of the Ekert protocol where they show that a test of the CHSH-inequalities is not necessary for the security of the protocol [24]. Instead, Alice and Bob use two complementary measurement bases as in the BB84 protocol and randomly apply them on the received qubits. In detail, Alice and Bob receive qubits coming from the source located in the middle of them (as pointed out above, the protocol does not change if the source is in possession of Alice or Bob). Again, the qubits are parts of a Bell state, e.g., $|\Psi^{-}\rangle$. After receiving both qubits, Alice and Bob randomly and independently choose either the Z- or the X-basis to measure the qubit. Due to the entanglement of the qubits, Alice's measurement completely determines the state of Bob's qubit, i.e., if Alice measures a $|1\rangle$, Bob's qubit is in the state $|0\rangle$, and vice versa. If Bob measures in a different basis than Alice he destroys the information carried by the qubit and thus will not obtain the same result as Alice. Therefore, after the measurements are finished, both parties publicly compare their measurement bases and discard their results where they used different bases (i.e., similar to the BB84 protocol).

The remaining results should be perfectly correlated and the communication parties compare a randomly chosen fraction in public. If there is too much discrepancy between their results they have to assume that an adversary is present and they start over the protocol. It has also been shown by Bennett et al. in this paper that the security of this version of the protocol is equal to the security of the BB84 scheme [24].

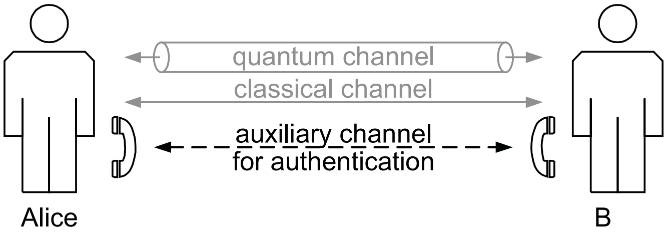

Figure 1. Channel configuration of our enhanced protocol

IV. 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.

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 $x \overset{r}{\leftarrow} \Omega$, 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 $x \overset{r}{\leftarrow} \{0,1\}^t$, 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 $H_k(x) \bmod m$ is uniformly distributed over $\{0,1,\ldots,m-1\}$.

To embed authentication information in her bit stream, Alice secretly chooses two secret values $k_v, k_p \overset{r}{\leftarrow} \{0,1\}^t$ 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 $v_0, p_0 \overset{r}{\leftarrow} \{0,1\}^t$.

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

$$(b_n)_{n\in\mathbb{N}} = (b_0, b_1, \ldots, b_{p_i-1}, b_{p_i} = f(v_i), b_{p_i+1}, \ldots) \qquad (3)$$

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 [34] are well developed and successfully rely on exactly this assumption (although pursuing different goals [35]). 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).

V. 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 (see [36] for a recent proposal), 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. 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 $\chi_k = 1 :\iff X_k = y_k$, 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.,

$$\Pr[X_k = y_k] = \mathbb{E}[\chi_k] = \Pr[b_{p_k} = v_k] \tag{4}$$

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 [37] of the Hoeffding-bound to obtain

$$\Pr[S_n - \mathbb{E}[S_n] \geq \varepsilon] \leq \exp\left(-\frac{2\varepsilon^2}{n}\right). \tag{5}$$

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

$$\Pr[\text{all } X_n \text{ match}|\text{incorrect seeds}] = \Pr[S_n \geq n] \leq e^{-n/2}. \tag{6}$$

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 (6), and the likelihood for E_2 to occur is $1 - 2^{-O(t)}$.

The law of total probability then gives

$$\begin{aligned} \Pr[\text{Bob accepts}] &= \Pr[\text{all } X_n \text{ match}] = && (7)\\ &= \Pr[\text{all } X_n \text{ match}|E_1] \Pr[E_1] \\ &\quad + \Pr[\text{all } X_n \text{ match}|E_2] \Pr[E_2] && (8)\\ &\leq e^{-n/2}(1 - 2^{-O(t)}) + 2^{-O(t)} \leq 2^{-O(t+n)}, && (9) \end{aligned}$$

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

VI. Evaluation

For the evaluation we used two common low level machines, each one Intel i5-3470 CPU, having four cores running at 3.20GHz, 3GB memory, 48 GB hard disk and Debian 8.2 as operating system. The machines have been connected using standard Ethernet with an average round trip time of 0.017 milliseconds.

We implemented the proposed protocol on a branch of the current available AIT QKD R10 software stack V9.9999.7 [38]. This Open Source software contains a full featured QKD post processing environment containing BB84 sifting, error correction, privacy amplification and other steps necessary.

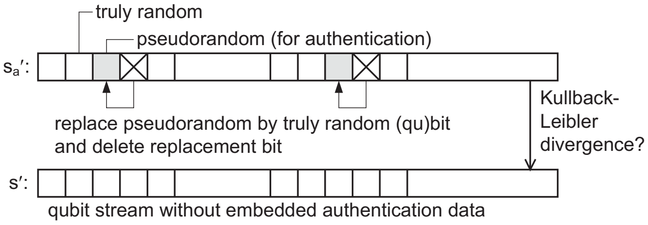
truly random
pseudorandom (for authentication)
s_a′:
replace pseudorandom by truly random (qu)bit
and delete replacement bit
Kullback-
Leibler
divergence?
s′:
qubit stream without embedded authentication data

Figure 2. Comparison of BB84 with and without authentication data

For the development at hand the protocol was built full-duplex, i.e., BB84 basis comparison is run with with separately added authentication bits both ways: Alice and Bob choose their v_i, p_i independently and add this information to their base strings before transmission to their peer. A second message exchange emulates the second auxiliary channel by sending k_v, k_p, v_0, p_0 to the peer.

We used a $GF(2^{32})$ with $P(x) = x^{32} + x^7 + x^3 + x^2 + 1$ as irreducible polynomial to construct a universal hash family $\mathcal{H}$, with members H_k acting on this finite field. For hashing a message M under a secret $k = (k_1, k_2) \in \{k_p, k_v\}$, we split into chunks of equal size $M = m_1 \| m_2 \| \ldots \| m_n$ with $|m_i| = 32$. Using the partial key k_1, we calculate a tag t as $t = m_1 k_1 + m_2 k_1^2 + \ldots + m_n k_1^n$ within the finite field using polynomial multiplication. For the message, we take the current values p and v, respectively, and the result of the hashing under k is $H_k(M) = t \oplus k_2$, where $\oplus$ denotes the bitwise XOR (cf. [39]).

The experiment has been done with raw data grabbed from the current setup of the AIT's QKD-Telco project [40]. The QKD-TELCO aims to integrate quantum key distribution in telecom networks to provide a modern, trustworthy ICT infrastructure. This is an approach to use DWDM (Dense Wavelength Division Multiplexing) communication as an seamless integration of QKD systems in existing and next-generation metro-access architectures. The measurement data consisting of 64 Bit photon detector timestamps sums up to 4.7 GB data covering a timespan of nearly 5465 seconds.

For a practical evaluation, we drained a total of $3,272,234$ bits from the BB84 implementation, including a total of $375,142$ pseudorandom authentication bits embedded in the string. Call s_a a bitstring with authentication data in it, as opposed to s denoting a bitstring without such data (e.g., as obtained from a plain BB84 execution). From our experiment, we directly obtained s_a, and constructed the string s by replacing the pseudorandom bits (at the known positions) with truly random ones picked from the same string (to have these obey the same randomness in terms of distribution as the remaining string). The replacement bits were removed from both strings later on, to obtain strings s'_a and s' of equal length, which differ only in those positions where pseudorandom bits were inserted in s'_a. So, the only differences between s'_a and s' are due to the pseudorandom bits. Figure 2 summarizes the details.

To measure how much difference is noticeable in information-theoretic terms, we evaluated the Kullback-Leibler divergence $KL(s'_a[1 : n], s'[1 : n]) = K(n)$, where the notation $s[1 : n]$ denotes the first n bits of the string n. Figure 3 shows the plot, illustrating that the difference comes

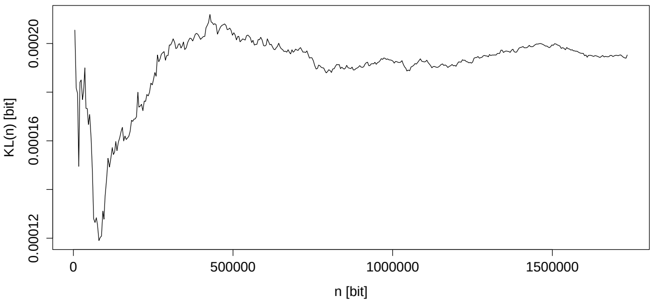

Figure 3. Kullback-Leibler divergence $KL(s'_a, s')$ (for the first n bits)

to ≈ 0.00019 bits near the end of the plot.

For a second experiment, we divided the total string s'_a and s' into consecutive chunks of 70 bits (after additionally removing bits that were marked as measurement errors). From the so-obtained set of strings of 70 bits each, we computed the empirical joint distribution of 70 bits with and without authentication data in them. Let $b_a[i]$ and $b[i]$ for $1 \leq i \leq 70$ denote the i-th bits from the chunk/string with and without authentication data, respectively, then the difference was measured by $\max_{1 \leq i \leq 70} |\Pr(b_a[i] = 1) - \Pr(b[i] = 1)| \approx 0.01414979 < 1/70 \approx 0.01428571$. Thus, the change in the empirical distribution due to the pseudorandom authentication data is numerically less than 1 bit different over 70 trials (consequently, both empirical distribution seemingly converge to the uniform mass function $1/70$ as the number of chunks approaches infinity). However, even if distinguishing a plain from an authenticated BB84 would be effective based on empirical distributions, the problem of *where* the pseudorandom bits are located remains; based on the quality of the universal hash function being used, this problem should remain practically infeasible.

VII. Conclusion

a) Application to other QKD Protocols: The methodology that we described in this article is integrating pseudorandom sequences into the randomly chosen bit strings defining the basis choice for Alice and Bob. Thus, the technique is partly unrelated to the protocol executed between Alice and Bob. We focused on the BB84 protocol in sections IV, V, and VI but the general idea can, in principle, also be applied to other QKD protocols described in Section III.

For the B92 protocol, the number of quantum states representing classical bits is reduced, compared to the BB84 protocol, from four to two states. As pointed out in Section III-B, this leads to indeterminate outcomes, which have to be deleted before Alice and Bob can perform the error correction and privacy amplification. Thus, our methodology can in principle also be applied for the non-orthogonal states of the B92 protocol. Nevertheless, one challenge comes up when results have to be deleted, which corresponds to the pseudorandom bits required for authentication. Since no measurement result is available in this case, Alice and Bob have to compensate somehow for the missing bit.

Additionally, an application of the third orthogonal basis, as in the six-state protocol (cf. Section III-C), does not represent a big change to our authentication scheme. The choice of all three bases is still relying on a random sequence where additional pseudorandom elements can be integrated. Due to the fact that Alice and Bob have to choose between three bases instead of two, simple bit strings representing the basis choice will not be sufficient any more (i.e., one bit can only represent two different bases). Under the obvious changes, our authentication method can be applied as described in this article. It remains to investigate whether the reduced efficiency of the six-state protocol [23], which is due to the three bases, also affects the efficiency of our authentication process.

Finally, our authentication scheme can also be integrated into "prepare and measure" protocols using entangled states instead of single photon sources. This explicitly holds for the BBM92 protocol, since the measurement bases are the same as in the BB84 protocol. Hence, the introduction of additional pseudorandom bits in to the bit string defining the basis choice analogously follows the way described in Section IV and all computations can be performed alike.

b) Summary and Outlook: 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). These would have to be discarded from both lists (Alice's and Bob's pseudorandom sequence) upon the checking of the authentication data. For the experiments, we discarded erroneously measured bits for simplicity.

As the experimental evaluation showed, there was no noticeable difference between an authenticated and a non-authenticated BB84 qubit stream in the first phases. However, our variant of BB84 detects person-in-the-middle attacks at a much earlier stage than competing schemes, which do that along the public discussion phase. Thus, efficiency is also gained by earlier termination of the protocol. The most important aspect of our proposed variant is the avoidance of pre-shared secrets, however, which technically turns BB84 from quantum key *growing* into quantum key *establishment*.

References

[1] S. Rass, S. König, and S. Schauer, "Bb84 quantum key distribution with intrinsic authentication," in Proc. of Ninth International Conference on Quantum, Nano/Bio, and Micro Technologies (ICQNM), 2015, pp. 41–44.

[2] 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.

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

[4] 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.

[5] 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.

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

[7] 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.

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

[9] Y. Chang, C. Xu, S. Zhang, and L. Yan, "Controlled quantum secure direct communication and authentication protocol based on five-particle cluster state and quantum one-time pad," Chinese Science Bulletin, vol. 59, no. 21, 2014, pp. 2541–2546. [Online]. Available: http://dx.doi.org/10.1007/s11434-014-0339-x

[10] T. Hwang, Y.-P. Luo, C.-W. Yang, and T.-H. Lin, "Quantum authencryption: one-step authenticated quantum secure direct communications for off-line communicants," Quantum Information Processing, vol. 13, no. 4, 2014, pp. 925–933. [Online]. Available: http://dx.doi.org/10.1007/s11128-013-0702-x

[11] J. G. Jensen and R. Schack, "Quantum Authentication and Key Distribution using Catalysis," quant-ph/0003104 v3, 2000, (last accessed: June, 2015). [Online]. Available: http://arxiv.org/abs/quant-ph/0003104

[12] H. N. Barnum, "Quantum Secure Identification using Entanglement and Catalysis," quant-ph/9910072 v1, 1999, (last accessed: June, 2015). [Online]. Available: http://arxiv.org/abs/quant-ph/9910072

[13] Y.-S. Zhang, C.-F. Li, and G.-C. Guo, "Quantum Authentication using Entangled State," quant-ph/0008044 v2, 2000, (last accessed: June, 2015). [Online]. Available: http://arxiv.org/abs/quant-ph/0008044

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

[15] Y. Chang, S. Zhang, J. Li, and L. Yan, "Robust EPR-pairs-based quantum secure communication with authentication resisting collective noise," Science China Physics, Mechanics & Astronomy, vol. 57, no. 10, 2014, pp. 1907–1912. [Online]. Available: http://dx.doi.org/10.1007/s11433-014-5434-0

[16] T.-Y. Ye, "Fault-tolerant authenticated quantum dialogue using logical bell states," Quantum Information Processing, vol. 14, no. 9, 2015, pp. 3499–3514. [Online]. Available: http://dx.doi.org/10.1007/s11128-015-1040-y

[17] W.-M. Shi, J.-B. Zhang, Y.-H. Zhou, and Y.-G. Yang, "A novel quantum deniable authentication protocol without entanglement," Quantum Information Processing, vol. 14, no. 6, 2015, pp. 2183–2193. [Online]. Available: http://dx.doi.org/10.1007/s11128-015-0994-0

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

[19] 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.

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

[21] G. L. Long and X. S. Liu, "Theoretically efficient high-capacity quantum-key-distribution scheme," Phys. Rev. A, vol. 65, Feb 2002, p. 032302. [Online]. Available: http://link.aps.org/doi/10.1103/PhysRevA.65.032302

[22] C. H. Bennett, "Quantum Cryptography using any Two Nonorthogonal States," Phys. Rev. Lett., vol. 68, no. 21, 1992, pp. 3121–3124.

[23] D. Bruss, "Optimal Eavesdropping in Quantum Cryptography with Six States," Phys. Rev. Lett, vol. 81, no. 14, 1998, pp. 3018–3021.

[24] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum Cryptography without Bell's Theorem," Phys. Rev. Lett., vol. 68, no. 5, 1992, pp. 557–559.

[25] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, "Quantum Cryptography Protocols Robust Against Photon Number Splitting Attacks for Weak Laser Pulses Implementations," Phy. Rev. Lett., vol. 92, no. 5, 2004, p. 057901.

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

[27] 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.

[28] 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.

[29] 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.

[30] 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.

[31] 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.

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

[33] A. Peres, "How to Differentiate Between Non-orthogonal States," Phys. Lett. A, vol. 128, no. 1-2, 1988, p. 19.

[34] 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.

[35] 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.

[36] M. Hayashi and T. Tsurumaru, "More efficient privacy amplification with less random seeds via dual universal hash function," vol. 62, 2016, pp. 2213–2232.

[37] W. D. Smith, "Tail bound for sums of bounded random variables," scorevoting.net/WarrenSmithPages/homepage/imphoeff.ps, April 2005, (last accessed: June, 2015).

[38] C. Pacher and O. Maurhart, "AIT QKD R10 Software," 2015, https://sqt.ait.ac.at/software/projects/qkd, (last accessed: Feb.23, 2016).

[39] T. Johansson, G. Kabatianskii, and B. Smeets, "On the relation between A-Codes and codes correcting independent errors," in Advances in Crypology (EuroCrypt), ser. LNCS 765, T. Helleseth, Ed. Berlin Heidelberg: Springer, 1994, pp. 1–11.

[40] Austrian Institute of Technology, "QKD-Telco – practical quantum key distribution over telecom-infrastructures," 2015, http://www.qkd-telco.at/, (last accessed: Feb.23, 2016).