Article

Information-Theoretically Secure Data Origin Authentication with Quantum and Classical Resources

Georgios M. Nikolopoulos [1,2,*] and **Marc Fischlin** [3]

1   Institute of Electronic Structure and Laser, FORTH, P.O. Box 1385, GR-70013 Heraklion, Greece
2   Institut für Angewandte Physik, Technische Universität Darmstadt, D-64289 Darmstadt, Germany
3   Cryptoplexity, Technische Universität Darmstadt, D-64289 Darmstadt, Germany;
    marc.fischlin@cryptoplexity.de
*   Correspondence: nikolg@iesl.forth.gr

Abstract: In conventional cryptography, information-theoretically secure message authentication can be achieved by means of universal hash functions, and requires that the two legitimate users share a random secret key, which is at least twice as long as the tag. We address the question of whether quantum resources can offer any advantage over classical unconditionally secure message authentication codes. It is shown that a broad class of symmetric prepare-and-measure quantum message-authentication schemes cannot do better than their classical counterparts.

1. Introduction

One of the main information security objectives is to provide assurance about the original source of a received message [1–4]. This goal is usually referred to as data origin authentication, and it is a stronger version of another cryptographic goal, the so-called data integrity. The latter addresses the unauthorized (including accidental) alteration of the message, from the time it was created, transmitted or stored by an authorized user. Data origin authentication, on the other hand, provides assurance of the identity of the sender of the message, in addition to data integrity. From another point of view, data origin authentication implicitly provides data integrity, in the sense that if the message is somehow modified, then essentially the source of the message has changed.

Another security objective that is closely related to data origin authentication, is the so-called non-repudiation, which prevents the original sender of a specific message from denying to a third party his/her action. This is a stronger requirement than data origin authentication, because the latter provides this assurance to the receiver of the message, but it does not provide any evidence that could be presented to a third party in order, for example, to resolve a dispute between the sender and the receiver.

In modern cryptography, data origin authentication is provided by message-authentication codes (MACs), which require the two legitimate users (sender and receiver) to share a common secret key [1–5]. Typically, MACs are built from block ciphers [1,6] or hash functions [1,3–5,7]. A MAC takes as input the message and the key, and produces an authentication tag, which is sent from the sender to the receiver, together with the message. MACs that rely on block ciphers or collision resistant hash functions offer computational security, as opposed to the Wegman and Carter scheme, which exploits universal hash functions and offers information-theoretic (unconditional) security [3–5,7]. On the other hand, digital signature schemes are the main mechanism for providing non-repudiation and

they typically rely on public-key cryptography [1,2]. Both MACs and digital-signature schemes offer data origin authentication, but only the latter can ensure non-repudiation. Hence, digital-signature schemes are of vital importance in cases where the sender and the receiver of the message do not trust each other (e.g., business applications), and there is the potential of dispute over the message. MACs are widely used in every task, when non-repudiation is not an issue (e.g., in authenticated end-to-end communication), mainly because the computational cost associated with the generation and the verification of a tag is considerably smaller than for digital signatures. It is worth noting, however, that MACs can provide non-repudiation in certain realistic scenarios e.g., when a trusted third party is involved [4].

Data origin authentication and data integrity have also been discussed in a quantum setting. More precisely, Curty and Santos have proposed an authentication protocol for 1-bit message, which requires the two legitimate users to share a maximally entangled state of qubits [8]. To the best of our knowledge, this is the only quantum MAC (QMAC) scheme in the literature, which claims an advantage over the Wegman–Carter scheme. The first quantum digital-signature scheme has been proposed by Gottesman and Chuang [9], and relies on the notion of a quantum one-way function, which maps classical bit strings (private keys) on quantum public keys (see also [10–12] for other applications of quantum public keys). Various authors improved on the original scheme of Gottesman and Chuang, by removing the need for quantum memory, for authenticated quantum channels, etc. [10,13–16]. These develpments go beyond the scope of the present work, and the interested reader may refer to Refs. [17,18], for an extensive list of publications related to quantum digital signatures. It is worth noting, however, that until now all of these quantum digital-signature schemes have been far less efficient than classical schemes, which renders them impractical [19,20].

By contrast to the thorough investigation of quantum digital-signature schemes, QMACs remain largely unexplored. The main question we address in the present work is whether prepare-and-measure QMACs can outperform classical schemes for information-theoretically secure data origin authentication. To address this question, we define a rather general theoretical framework for symmetric prepare-and-measure QMACs, which is absent from the literature. Subsequently, we show that such schemes cannot do better than their classical counterparts. This result is rather general, and implies that the QMAC scheme of Curty and Santos cannot outperform classical MACs.

The paper is organized as follows. For the sake of completeness, Section 2 contains a brief summary of unconditionally secure classical MACs. In Section 3, we discuss prepare-and-measure QMACs, and our main results are presented in Section 4. A summary with concluding remarks is given in Section 5.

2. Unconditionally Secure Classical MACs

Two honest users, Alice and Bob, share a common secret random key k, which is uniformly distributed over the set $\mathbb{K}$. The distribution of the secret key is not our concern here, since it can be achieved by various classical or quantum means that go beyond the scope of data origin authentication.

Alice wants to send an authenticated message m to Bob, and let $\mathbb{M}$ denote the message space, with $|\mathbb{M}| > 1$. To authenticate the message, she evaluates the tag t, through a publicly known function $t := h(k, m)$. The message and the tag (m, t) are sent to Bob over a classical channel (throughout this work we focus on data origin authentication, and hence we assume that the message is sent in the clear together with the tag. If confidentiality is also an issue, the message has to be encrypted). In general, as a result of forgery or noise, Bob receives (m', t') and he accepts the message only if $t' = h(k, m')$. In the framework of MACs, we can define the deception probability $P_l^{(\mathrm{D})}$, to be the probability for an adversary (Eve) to produce a successful forgery after observing l valid message-tag pairs. In particular, we can distinguish between an impersonation and a substitution attack (also known as key-only and chosen-message attacks, respectively). In the former attack, the adversary does not have access to any message-tag pair (i.e., $l = 0$), and her task is to create a pair, without knowing the secret key k, that will pass Bob's verification. In the substitution attack, Eve has access to a single valid

message-tag pair (m, t), i.e., $l = 1$, and her task is to produce another message $m' \neq m$, such that $t' = h(k, m')$. It is straightforward to generalize the substitution attack, by giving Eve access to $l > 1$ valid message-tag pairs.

Definition 1. *A MAC is l-time ε-secure, if for all (including unbounded) adversaries, $P_l^{(D)} \leq \varepsilon$.*

Note that there is no MAC scheme with $P_0^{(D)} = 0$. Although Eve does not know the actual secret key, she may guess the correct tag for her message m with probability at least $1/|\tilde{\mathbb{T}}|$, where $\tilde{\mathbb{T}}$ denotes the set of different possible tags and it is assumed to be the same for all messages [3–5]. Hence, we have

$$P_0^{(D)} \geq \frac{1}{|\tilde{\mathbb{T}}|}, \tag{1}$$

and the best we can expect from a MAC scheme is to be l-time $1/|\tilde{\mathbb{T}}|$-secure. One can readily show the following fundamental theorem [4,7].

Theorem 1. *An l-time ε-secure MAC must have keys of length at least $(l + 1)|\log_2(\varepsilon)|$.*

A 1-time $1/|\tilde{\mathbb{T}}|$-secure MAC can be obtained by means of the Wegman–Carter construction, and the use of a strongly universal hash function h_k [3,4,7], which is chosen at random from a class of such functions, and it is identified uniquely by the shared secret key k. In this case we have

$$P_0^{(D)} = P_1^{(D)} = \frac{1}{|\tilde{\mathbb{T}}|}, \tag{2a}$$

which are the lowest deception probabilities one can aim at (it is worth noting, and keeping in mind, that the calculation of deception probabilities for classical MACs typically pertains to the worst-case scenario i.e., it involves a maximization over all possible cheating strategies for Eve). However, the cost one has to pay for attaining these probabilities is that the key scales linearly with the length of the message. More efficient 1-time $\varepsilon-$secure MACs can be constructed by means of $\varepsilon-$almost strongly universal hash functions, for some $\varepsilon > 1/|\tilde{\mathbb{T}}|$. For instance, in this context, Wegman and Carter have shown that one can have a 1-time $2/|\tilde{\mathbb{T}}|-$secure MAC with a key length which scales linearly with the length of the tag, and logarithmically with the length of the message i.e., $|k| \simeq 4 \log_2(|\tilde{\mathbb{T}}|) \log_2[\log_2(\mathbb{M})]$. Various $\varepsilon-$almost strongly universal hash functions have been proposed in the literature (e.g., see references in [3–5]), and one can readily build a MAC scheme based on each one of them, with

$$P_0^{(D)} = \frac{1}{|\tilde{\mathbb{T}}|}, \quad P_1^{(D)} = \varepsilon. \tag{2b}$$

The precise value of the security parameter ε and the length of the key vary from scheme to scheme. Strongly universal functions can be viewed as $1/|\tilde{\mathbb{T}}|-$almost strongly universal hash functions, and it is only in this case that $\varepsilon = 1/|\tilde{\mathbb{T}}|$. Finally, universal hash functions have also been exploited in the development of $l-$time unconditionally secure MACs, with $l > 1$.

The main question we address in the following section is whether there are QMACs which can, in principle, compete with $\varepsilon-$secure classical MACs, in terms of the achievable deception probabilities and/or perhaps the required key lengths. A corollary of Theorem 1 is that there is no MAC with unbounded-length keys that can provide information-theoretic security for an unbounded number of messages. Hence, following standard textbooks in the field [3,4] as well as existing work on QMACs [8] and quantum digital-signature schemes [10,13–18], we will focus on the most basic scenario pertaining to the authentication of a single message. Moreover, although losses and imperfections during transmission are inevitable in the realization of any quantum protocol, it is always of vital importance

to know beforehand if a task can be achieved at least ideally, in the most basic communication scenario. In this spirit, we address the aforementioned question for an ideal scenario i.e., in the absence of noise and imperfections during the transmission of the quantum states.

3. Theoretical Framework for Unconditionally Secure Prepare-and-Measure QMACs

We begin with a rather general theoretical framework for unconditionally secure prepare-and-measure QMACs, which is absent from the literature. For the sake of consistency, the adopted framework follows closely the one for classical MACs that was summarized in the previous section.

Two honest users, Alice and Bob, share a random secret key k, uniformly distributed over the set $\mathbb{K}$, and Alice wants to send an authenticated classical message $m \in \mathbb{M}$ to Bob, where $|\mathbb{M}| \geq 2$. The key is independent of the message, and we have the condition

$$\Pr(k|m) = \Pr(k) = \frac{1}{|\mathbb{K}|}, \ \forall\, m \in \mathbb{M}. \tag{3}$$

We will assume that the tagging of the message involves the state of a $d-$dimensional quantum system, which is initially prepared in some publicly known quantum state $|\Psi_{\text{in}}\rangle$. Typically, a QMAC involves a publicly known set of (unitary) tagging operations $\{\hat{\mathcal{E}}_\tau \ : \ \tau \in \mathbb{T}\}$, where the classical label is a function of the key and the message i.e., $\tau = f(k,m)$ with publicly known $f \ : \ \mathbb{K} \times \mathbb{M} \to \mathbb{T}$. For a given pair (k,m), the operation $\hat{\mathcal{E}}_\tau$ is applied on the initial state of the system, thereby obtaining the quantum state

$$|\Psi_\tau\rangle := \hat{\mathcal{E}}_\tau |\Psi_{\text{in}}\rangle. \tag{4}$$

Let $\mathbb{Q}_m := \{|\Psi_\tau\rangle \ : \ \tau = f(k,m),\ k \in \mathbb{K}\}$ denote the set of possible quantum states corresponding to a given message $m \in \mathbb{M}$. Each quantum state is identified by the label $\tau = f(k,m)$, and the tagging operation is chosen such that for *any* possible message $m \in \mathbb{M}$ there exist distinct labels $\tau, \tau' \in \mathbb{T}$ such that $\lambda_{\tau,\tau'} := |\langle\Psi_{\tau'}|\Psi_\tau\rangle| > 0$. Given that m is fixed, the distinct labels correspond to distinct keys.

The quantum state $|\Psi_\tau\rangle$ serves as a quantum tag of the message m when Alice and Bob share the secret key k, and it is sent together with the message to Bob. As a result of noise or Eve's intervention, Bob will receive the pair $(m', |\varphi\rangle)$, and his task is to infer whether the received message has originated from Alice or not. In prepare-and-measure QMACs, this decision is made based solely on a local measurement, perhaps after a local operation, on the received quantum tag. That is, there is no need for additional communication between Alice and Bob, and the latter accepts the message as authentic only if the outcome of the measurement is consistent with the expected quantum tag $|\Psi_\tau\rangle$. We are interested in protocols with deterministic decision making, where Bob always accepts (with probability 1) the message-tag pair of honest Alice, with whom he shares the secret key. Completeness/correctness of the protocol implies that the same must also hold if Eve succeeds in guessing a valid message-tag pair. This is because, as far as Bob is concerned, the only feature that discriminates Alice from Eve is the secret key that he shares with Alice. If Eve happens to correctly guess a valid message-tag pair, this feature ceases to exist.

In general, different keys may yield the same label (and thus quantum tag) for the same message. Hence, for a given message m, the key space $\mathbb{K}$ can be partitioned into smaller non-overlapping subspaces

$$\mathbb{K}_{m,\tau} := \{k \in \mathbb{K} \ : \ \tau = f(k,m) \text{ for } m \in \mathbb{M},\ \tau \in \mathbb{T}\}.$$

Each subspace contains all the keys that lead to the same label $\tau \in \mathbb{T}$ for the given message $m \in \mathbb{M}$, while different subspaces correspond to different labels, and thus we have as many subspaces as labels.

The following discussion focuses on prepare-and-measure QMACs and thus from now on the term prepare-and-measure will be omitted for the sake brevity. For direct comparison to standard $\varepsilon-$secure classical MACs (see Section 2), throughout this work we consider symmetric QMACs, which treat

equally all of the possible messages and keys. Hence, $|\mathbb{K}_{m,\tau}| = L$ for all $m \in \mathbb{M}$, and $\tau \in \mathbb{T}$, while the number of labels is related to the size of the key space as follows $|\mathbb{T}| = |\mathbb{K}|/L$. The probability for a quantum tag $|\phi\rangle$ to be equal to $|\Psi_\tau\rangle$ for a given m, is given by

$$\Pr(|\phi\rangle = |\Psi_\tau\rangle \, | m) = \frac{(\# \, k \in \mathbb{K} : |\phi\rangle = |\Psi_\tau\rangle \text{ given } m)}{|\mathbb{K}|} = \frac{1}{|\mathbb{T}|}. \tag{5}$$

The number of different possible quantum tags is the same for any given message $m \in \mathbb{M}$, and moreover, all of the quantum tags are equally probable. There are no preferable (i.e., more probable) messages, keys or tags. Of course, the partition of the key space varies from message to message, in the sense that a key has to yield a different tag for different messages (i.e., $h(k, m) \neq h(k, m')$), and thus it will appear at different subspaces (If this is not satisfied, then Eve can easily cheat on Bob by substituting m with m', because the details of the protocol are publicly known and the message is sent in the clear).

The impersonation and the substitution attacks in the quantum setting can be defined in complete analogy to the classical setting.

Definition 2. *Impersonation attack—Eve wants to impersonate Alice without knowing the actual secret key k, and without having access to any valid message-tag pair. To this end, she chooses a pair $(m, |\Psi_{\tau'}\rangle)$ with $\tau' = f(k', m)$, and sends it to Bob, hoping that Bob will accept it as a valid message originated from Alice.*

Definition 3. *Substitution attack—Eve does not know the secret key k of Alice and Bob, but she has access to a single valid message-tag pair $(m, |\Psi_\tau\rangle)$. Her task is to produce another message $m' \neq m$, such that the pair $(m', |\Psi_{\tilde{\tau}}\rangle)$ with $\tilde{\tau} = f(k, m')$ will be accepted by Bob as a valid message originated from Alice.*

In closing, it is worth noting that the theoretical framework that we have just presented includes the unconditionally secure classical MACs discussed in Section 2. More precisely, one recovers the classical MACs when for any $m \in \mathbb{M}$, the possible classical tags $t \in \tilde{\mathbb{T}}$ are encoded on mutually orthogonal quantum states i.e., $t \to |\Psi_t\rangle$ with $\lambda_{t,t'} = |\langle \Psi_t | \Psi_{t'} \rangle| = 0$, $\forall t, t' \in \tilde{\mathbb{T}}$ with $t \neq t'$. In this case, the security is ensured only by the classical tagging, and not by the encoding on the mutually orthogonal states.

4. Results

At this stage, we have defined a rather general theoretical framework for unconditionally secure QMACs. We can prove the following theorem.

Theorem 2. *For any QMAC that falls within the aforementioned framework and involves deterministic decision making, the deception probability for the impersonation attack is higher than what can be achieved by unconditionally secure classical MACs.*

Proof. As discussed in Section 2, for unconditionally-secure classical MACs $P_0^{(\mathrm{D})} = 1/|\mathbb{T}|$. We will show that this is not possible for the QMACs discussed in Section 3, when Bob always accepts (with probability 1) Alice's message.

In view of conditions (3) and (5), all of the keys are equally probable, and for any possible message, there are $|\mathbb{T}|$ different possible quantum tags. For any message, there exist at least two distinct labels, say τ and τ', such that $\lambda_{\tau,\tau'} > 0$, and in this case Bob cannot discriminate perfectly between the quantum states $|\Psi_{\tau'}\rangle$ and $|\Psi_\tau\rangle$.

The probability for Eve to choose the valid message-tag pair $(m, |\Psi_\tau\rangle)$ is $|\mathbb{T}|^{-1}$, and in this case, Bob will certainly accept the pair. By contrast to the classical setting, however, in the case of QMACs, there is also a non-vanishing probability for Bob to accept the wrong pair $(m, |\Psi_{\tau'}\rangle)$ as valid, because $\lambda_{\tau,\tau'} > 0$. The maximum probability for successful cheating is given by

$$P_0^{(D)} = \frac{1}{|\mathbb{T}|} + \left(1 - \frac{1}{|\mathbb{T}|}\right) \max_{\tau, \tau', m} \{Q(\text{acc}|\tau, \tau', m)\} \tag{6}$$

where $Q(\text{acc}|\tau, \tau', m)$ with $\tau' \neq \tau$, is the conditional probability for Bob to accept Eve's pair, given that Eve has sent $(m, |\Psi_{\tau'}\rangle)$, whereas the unknown secret key shared with Alice is k so that Bob expects $|\Psi_\tau\rangle$ for $\tau = h(k, m)$.

In classical unconditionally secure classical MACs, the second term in Equation (6) vanishes, because Bob can perfectly discriminate between different classical tags. So, the probability for Bob to accept the wrong message-tag pair as valid is zero, thereby obtaining $P_0^{(D)} = 1/|\mathbb{T}|$. However, for the QMACs of Section 3, there exists at least one message, such that $\lambda_{\tau, \tau'} > 0$. This implies a non-vanishing probability for Bob to accept the wrong pair (i.e., $\max_{\tau, \tau', m}\{Q(\text{acc}|\tau, \tau', m)\} > 0$), and thus $P_0^{(D)} > 1/|\mathbb{T}|$, which is worse than what can be achieved in terms of classical unconditionally secure MACs. $\square$

Based on the above, we conclude that one can have $P_0^{(D)} = 1/|\mathbb{T}|$ only when the quantum tags with distinct labels $\tau, \tau' \in \mathbb{T}$ are mutually orthogonal for any possible message. In this case, however, we essentially deal with a classical MAC, because one can perfectly discriminate between the different quantum tags, and thus the security of the protocol may rely only on the choice of the classical function $f(\cdot)$. The same conclusion can be reached if one works with the average rather than the maximum deception probability. It is also worth emphasizing that these observations and arguments do not depend on the type or the size of the key. This point becomes clearer in the following subsection.

4.1. A QMAC with Quantum Key

Curty and Santos have proposed a QMAC for the authentication of a binary message, by means of a quantum key [8]. In their protocol, Alice (A) and Bob (B) share a pure entangled state

$$|\Psi\rangle_{AB} = \frac{1}{\sqrt{2}} \left(|01\rangle_{AB} - |10\rangle_{AB}\right), \tag{7}$$

which plays the role of a secret key. The message and the tag are carried by a four-dimensional quantum system "C" (e.g., two qubits), and let $\{|\phi_j\rangle : j = 0, 1, 2, 3\}$ be an orthonormal basis.

When Alice wants the send message $m \in \{0, 1\} := \mathbb{M}$, she sends state $|\phi_m\rangle$ to Bob, after applying a publicly known tagging operation $\hat{\mathcal{E}}$ controlled by the state of her half of the entangled state. More precisely, the tagging operation is given by $\hat{\mathcal{E}}_{AC} = (|0\rangle \langle 0|_A \hat{\mathbf{1}}_C + |1\rangle \langle 1|_A \hat{\mathcal{U}}_C)$, for a publicly known unitary $\hat{\mathcal{U}}$, and the overall state becomes

$$|\Psi\rangle_{ABC} = \frac{1}{\sqrt{2}} \left[|01\rangle_{AB} |\phi_m\rangle_C - |10\rangle_{AB} \hat{\mathcal{U}}_C |\phi_m\rangle_C\right]. \tag{8}$$

Tracing out the entangled state, the state of the transmitted message-tag pair reads

$$\tilde{\rho}_m = \frac{1}{2} \left(|\phi_m\rangle \langle \phi_m| + \hat{\mathcal{U}}_C |\phi_m\rangle \langle \phi_m| \hat{\mathcal{U}}_C^\dagger\right). \tag{9}$$

Upon receipt of the message-tag pair, Bob performs the decoding operation $\hat{\mathcal{D}}_{BC} = (|0\rangle \langle 0|_B \hat{\mathcal{U}}_C^\dagger + |1\rangle \langle 1|_B \hat{\mathbf{1}}_C)$, and subsequently a projective measurement on the orthonormal basis $\{|\phi_j\rangle : j = 0, 1, 2, 3\}$. He accepts the pair if the measurement returns one of the first two elements in the basis, i.e., $j \in \{0, 1\}$, and rejects it otherwise. One can readily confirm that Bob always accepts Alice's message with probability 1.

In this protocol, Alice and Bob essentially share a secret key $k \in \mathbb{K} := \{0, 1\}$ in the form of an entangled state. For message m, Alice sends $|\phi_m\rangle$ to Bob if $k = 0$, and $\hat{\mathcal{U}} |\phi_m\rangle$ if $k = 1$. The basis state $|\phi_m\rangle$ can be viewed as if obtained from some publicly known initial state $|\Psi_{\text{in}}\rangle$ by applying $\hat{\mathcal{V}}_m |\Psi_{\text{in}}\rangle := |\phi_m\rangle$. Hence, the present scheme can be viewed as a special case of the quantum tagging

defined in Equation (4), where the function $f(\cdot)$ is the identity function, and $\hat{\mathcal{E}}_{k,m} = \hat{\mathcal{U}}_k \otimes \hat{\mathcal{V}}_m$ with $\hat{\mathcal{U}}_0 = \hat{\mathbf{1}}$ and $\hat{\mathcal{U}}_1 = \hat{\mathcal{U}}$. The label τ is essentially $\tau = (k, m)$ and for a given $m \in \{0, 1\}$ it can take two possible values depending on the value of k, namely $\{(0, m), (1, m)\}$. According to Theorem 2 and the related proof, the present scheme cannot achieve $P_0^{(D)} = 1/|\mathbb{T}|$ for the impersonation attack, unless $\lambda_{\tau, \tau'} = 0$ for all possible messages in $\mathbb{M}$ and $\tau, \tau' \in \mathbb{T}$, with $\tau \neq \tau'$. This condition reduces to

$$\langle \phi_m | \hat{\mathcal{U}} | \phi_m \rangle = 0, \ \forall m \in \{0, 1\}. \tag{10}$$

(See also Appendix A for an example of the impersonation attack.)

Let us consider now the substitution attack. Suppose that Eve has access to a valid message-tag pair, which is sent from Alice to Bob. Eve's task is to decide whether the transmitted system is in state $|\phi_m\rangle$ or $\hat{\mathcal{U}} |\phi_m\rangle$. If she succeeds, then she knows whether Bob will apply $\hat{\mathcal{U}}^\dagger$ or not. Given that $\hat{\mathcal{U}}$ is a publicly known unitary, in this case Eve can cheat successfully by changing m to $m \oplus 1$ and by sending $|\phi_{m \oplus 1}\rangle$ or $\hat{\mathcal{U}} |\phi_{m \oplus 1}\rangle$ to Bob. In order to prevent such an attack, one needs

$$\langle \phi_m | \hat{\mathcal{U}} | \phi_m \rangle \neq 0, \ \forall m \in \{0, 1\}, \tag{11}$$

so that Eve cannot perfectly distinguish between $|\phi_m\rangle$ and $\hat{\mathcal{U}} |\phi_m\rangle$. However, this requirement contradicts the conditions (10), required for attaining $P_0^{(D)} = 1/\mathbb{T}$. Thus, there is no unitary operation $\hat{\mathcal{U}}$ that can satisfy both of these conditions simultaneously.

4.2. Decision Making Based on a Symmetry Test

We have seen that a broad class of symmetric QMACs cannot attain $P_0^{(D)} = 1/|\mathbb{T}|$, irrespective of the length of the key. The natural question arises as of whether QMACs in the particular class allow for shorter keys than their classical counterparts, at the cost of accepting slightly larger deception probabilities for the impersonation attack. In this context one may, for instance, accept $P_0^{(D)} = 1/|\mathbb{T}| + \delta$ in Equation (6), for some small correction $0 < \delta \leq 1/|\mathbb{T}|$. The precise value of δ is determined by the set of overlaps $\{\lambda_{\tau, \tau'} : \tau, \tau' \in \mathbb{T} \text{ with } \tau \neq \tau'\}$, as well as by the strategy based on which Bob accepts/rejects a message-tag pair. In general, $Q(\mathrm{acc} | \tau, \tau', m)$ increases with increasing $\lambda_{\tau, \tau'}$, which in turn implies increasing deviations of $P_0^{(D)}$ from the lowest possible value $1/|\mathbb{T}|$. To keep $P_0^{(D)}$ close to $1/|\mathbb{T}|$, one would like to have the maximum overlap $\lambda_{\max} := \max_{k, k', m} \{\lambda_{\tau, \tau'}\}$ as small as possible (close to zero) which, however, facilitates Eve's cheating by means of a substitution attack (states with different τ become nearly orthogonal).

One way to circumvent this stumbling block for any given $0 < \lambda_{\max} < 1$ is to use message-tag pairs of the form $(m, |\Psi_\tau\rangle^{\otimes n-1})$. Hence, the probability for Bob to accept an invalid message-tag pair can be reduced to any $0 < \epsilon \leq 1/(|\mathbb{T}| - 1)$ for a suitable $n = \mathcal{O}(|\log_2(\epsilon)|)$ [9,11], without the necessity for choosing $\lambda_{\max}$ close to 0.

It is worth noting here that Bob's task is not to infer the precise state of the quantum tag, but rather to decide on whether this state equals the expected state. In other words, given $(n - 1)$ copies of $|\Psi_{\tau'}\rangle$ (received tag) and one copy of the expected tag $|\Psi_\tau\rangle$ (which can be prepared locally), Bob has to decide whether $|\Psi_{\tau'}\rangle = |\Psi_\tau\rangle$ or $|\langle \Psi_{\tau'} | \Psi_\tau \rangle| < 1$. In the former (latter) case, he concludes that the received message-tag pair has (not) originated from Alice, and he accepts (rejects) it. This task can be performed, for instance, by means of a symmetry-test [21], which is optimal (with respect to the one-sided error requirement). Bob never rejects a valid message-tag pair, while for $\tau \neq \tau\prime$, the maximum error probability is given by [21,22]

$$\max_{\tau, \tau', m} \{ Q(\mathrm{acc} | \tau, \tau', m) \} = \frac{1}{n} \left[1 + (n - 1) \lambda_{\max}^2 \right]. \tag{12}$$

Inserting the resulting expression into Equation (6), and asking for $P_0^{(D)} = 1/|\mathbb{T}| + \delta$, we obtain

$$n = \frac{(|\mathbb{T}| - 1)(1 - \lambda_{\max}^2)}{\delta |\mathbb{T}| - (|\mathbb{T}| - 1)\lambda_{\max}^2}, \tag{13}$$

which is meaningful for $\lambda_{\max} < \sqrt{\delta |\mathbb{T}|/(|\mathbb{T}| - 1)}$. Recalling that $\delta \leq 1/|\mathbb{T}|$, we have

$$n > |\mathbb{T}| - 2, \tag{14}$$

which shows that for any chosen $0 < \delta \leq 1/|\mathbb{T}|$, the number of copies n required for attaining $P_0^{(D)} = 1/|\mathbb{T}| + \delta$ is more than $|\mathbb{T}| - 2$.

In order to have 1-time $\varepsilon-$secure QMAC, the entropy of the tags should be at least $|\log_2(\varepsilon)| + I_{\text{gain}}$, where I_{gain} is the information that Eve can extract from $(n - 1)$ copies of the $d-$dimensional quantum state $|\Psi_\tau\rangle$, while according to the Holevo bound, $I_{\text{gain}} \leq (n - 1) \log_2(d)$. Given that the message is known, this entropy can originate only from the key, and thus we ask for $\log_2(|\mathbb{K}|) \geq |\log_2(\varepsilon)| + (n - 1) \log_2(d)$. Using Inequality (14), we find that $\log_2(|\mathbb{K}|) > |\log_2(\varepsilon)| + (|\mathbb{T}| - 3) \log_2(d)$, which scales linearly with $|\mathbb{T}|$. This is in striking contrast to known $1-$time $\varepsilon-$ secure classical MACs with $\varepsilon \sim 1/|\mathbb{T}|$, which attain similar deception probabilities for $\log_2(|\mathbb{K}|) \sim \log_2(|\mathbb{T}|)$ (see Section 2 and related references).

5. Summary

We have discussed unconditionally secure data origin authentication by means of classical and quantum resources. The main question we have addressed is whether prepare-and-measure QMACs can outperform classical unconditionally secure MACs. This fundamental question is of pivotal importance for the field, and to the best of our knowledge, it has not been addressed adequately in the literature so far. Although losses and imperfections are inevitable in the realization of any quantum protocol, it is always important to know beforehand if a task can be achieved, at least ideally, in the most basic communication scenario. Hence, the above question has been addressed in the framework of 1-time authentication under an ideal scenario. We showed that even under such favorable conditions, a broad class of prepare-and-measure QMACs cannot do better than their classical counterparts, in the sense that they cannot attain deception probabilities $P_0^{(D)} = 1/|\mathbb{T}|$. This result contradicts certain conjectures that have been made in previous related work [8]. Moreover, we showed that the key length required for attaining both $P_0^{(D)} = 1/|\mathbb{T}| + \delta$ (with $0 < \delta \leq 1/|\mathbb{T}|$) and $P_1^{(D)} \sim 1/|\mathbb{T}|$ increases linearly with the size of the tag space $|\mathbb{T}|$, as opposed to the logarithmic scaling in known classical schemes with similar deception probabilities.

The present analysis and results pertain to a particular yet rather broad class of symmetric prepare-and-measure QMACs. From practical point of view, such a type of QMACs is of particular interest, because the receiver can decide on the authenticity of the message based solely on the received message-tag pair, and there is no need for additional communication between the sender and the receiver. The present work may serve as a benchmark for future work in the field. More precisely, the generality of the results suggests that any future efforts for the development of unconditionally secure QMACs, which can outperform their classical counterparts, should focus on protocols outside the present class of protocols (this is for instance the case of interactive and/or entanglement-assisted QMACs). An alternative possible direction of research involves the use of physical unclonable functions with quantum readout (e.g., see [23,24] and references therein).

Author Contributions: Conceptualization, G.M.N.; Formal analysis, G.M.N.; Investigation, G.M.N.; Methodology, G.M.N. and M.F.; Supervision, G.M.N. and M.F.; Validation, G.M.N. and M.F.; Writing—original draft, G.M.N.; Writing—review & editing, G.M.N. and M.F. Both authors have read and agreed to the published version of the manuscript.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

MAC　　　Message authentication code
QMAC　　Quantum message authentication code

Appendix A

In the absence of imperfections and cheating, the decoding operation applied by Bob essentially undoes the encoding operation performed by Alice and leaves Alice and Bob with the state

$$|\Psi\rangle_{ABC} = \frac{1}{\sqrt{2}}\left(|01\rangle_{AB} - |10\rangle_{AB}\right) \otimes |\phi_m\rangle_C. \tag{A1}$$

We consider now the impersonation attack introduced in Section 3.

Eve does not have access to a valid message-tag pair, and she sends to Bob some state $|\psi\rangle$. As a result, Bob's decoding operation is not canceled by Alice's decoding operation, and the state shared between Alice and Bob reads,

$$|\Psi\rangle_{ABC} = \frac{1}{\sqrt{2}}\left[|01\rangle_{AB}\,|\psi\rangle_C - |10\rangle_{AB}\left(\hat{\mathcal{U}}_C^\dagger\,|\psi\rangle_C\right)\right], \tag{A2}$$

where $|\psi\rangle$ denotes the state sent by Eve. Hence, the reduced state of the message-tag pair on which Bob performs the measurement is

$$\tilde{\rho}_C = \frac{1}{2}\left(|\psi\rangle\langle\psi| + \hat{\mathcal{U}}^\dagger\,|\psi\rangle\langle\psi|\,\hat{\mathcal{U}}\right)_C. \tag{A3}$$

The probability for Eve to deceive Bob is given by

$$P_0^{(D)}(\psi) = \sum_{j=0,1}\langle\phi_j|\,\tilde{\rho}_C\,|\phi_j\rangle = \frac{1}{2}\sum_{j=0,1}|\langle\phi_j\,|\psi\rangle|^2 + \frac{1}{2}\sum_{j=0,1}|\langle\psi|\,\hat{\mathcal{U}}\,|\phi_j\rangle|^2, \tag{A4}$$

and depends on Eve's state $|\psi\rangle$. If Eve sends $|\varphi_{j'}\rangle$ with $j' \in \{0,1\}$, then $P_0^{(D)}(\varphi_{j'})$ is larger than or equal to $1/2$, because $|\langle\varphi_j|\varphi_j\rangle| = 1$ and $|\langle\varphi_j|\varphi_{j'}\rangle| = 0$ for $j \neq j'$. The equality is attained only if the unitary operation used in the protocol satisfies

$$\langle\phi_{j'}|\,\hat{\mathcal{U}}\,|\phi_0\rangle = \langle\phi_{j'}|\,\hat{\mathcal{U}}\,|\phi_1\rangle = 0, \tag{A5}$$

for all $j' \in \{0,1\}$. One immediately sees that this condition contradicts condition (11).

References

1. Menezes, A.; van Oorschot, P.; Vanstone, S. *Handbook of Applied Cryptography*; CRC Press: Boca Raton, FL, USA, 1996.
2. Martin, K.M. *Everyday Cryptography: Fundamental Principles and Applications*; Oxford University Press: Oxford, UK, 2012.
3. Stinson, D.R.; Paterson, M.B. *Cryptography: Theory and Practice*; CRC Press: Boca Raton, FL, USA, 2019.
4. Katz, J.; Lindell, Y. *Introduction to Modern Cryptography*; CRC Press: Boca Raton, FL, USA, 2015.
5. Abidin, A. Authentication in Quantum Key Distribution: Security Proof and Universal Hash Functions. Ph.D. Thesis, Linköping University, Linköping, Sweden, 2013.

6.	Bellare, M.; Kilian, J.; Rogaway, P. The security of the cipher block chaining message authentication code. *J. Comput. Syst. Sci.* **2000**, *61*, 362–399. [CrossRef]

7.	Wegman, M.N.; Carter, J.L. New hash functions and their use in authentication and set equality. *J. Comput. Syst. Sci.* **1981**, *22*, 265–279. [CrossRef]

8.	Curty, M.; Santos, D.J. Quantum authentication of classical messages. *Phys. Rev. A* **2001**, *64*, 062309. [CrossRef]

9.	Gottesman, D.; Chuang, I. Quantum Digital Signatures. *arXiv* **2001**, arXiv:quant-ph/0105032.

10.	Andersson, E.; Curty, M.; Jex, I. Experimentally realizable quantum comparison of coherent states and its applications. *Phys. Rev. A* **2006**, *74*, 022304. [CrossRef]

11.	Nikolopoulos, G.M. Applications of single-qubit rotations in quantum public-key cryptography. *Phys. Rev. A* **2008**, *77*, 032348. [CrossRef]

12.	Ioannou, L.M.; Mosca, M. Public-key cryptography based on bounded quantum reference frames. *Theor. Comput. Sci.* **2014**, *560*, 33–45. [CrossRef]

13.	Dunjko, V.; Wallden, P.; Andersson, E. Quantum Digital Signatures without Quantum Memory. *Phys. Rev. Lett.* **2014**, *112*, 040502. [CrossRef] [PubMed]

14.	Wallden, P.; Dunjko, V.; Kent, A.; Andersson, E. Quantum digital signatures with quantum-key-distribution components. *Phys. Rev. A* **2015**, *91*, 042304. [CrossRef]

15.	Yin, H.L.; Fu, Y.; Chen, Z.B. Practical quantum digital signature. *Phys. Rev. A* **2016**, *93*, 032316. [CrossRef]

16.	Amiri, R.; Wallden, P.; Kent, A.; Andersson, E. Secure quantum signatures using insecure quantum channels. *Phys. Rev. A* **2016**, *93*, 032325. [CrossRef]

17.	Amiri, R.; Andersson, E. Unconditionally Secure Quantum Signatures. *Entropy* **2015**, *17*, 5635–5659. [CrossRef]

18.	Pirandola, S.; Andersen, U.L.; Banchi, L.; Berta, M.; Bunandar, D.; Colbeck, R.; Englund, D.; Gehring, T.; Lupo, C.; Ottaviani, C.; et al. Advances in quantum cryptography. *arXiv* **2019**, arXiv:quant-ph/1906.01645.

19.	Amiri, R.; Abidin, A.; Wallden, P.; Andersson, E. Efficient Unconditionally Secure Signatures Using Universal Hashing. In *Applied Cryptography and Network Security, Proceedings of the 16th International Conference (ACNS 2018), Leuven, Belgium, 2–4 July 2018*; Preneel, B., Vercauteren, F., Eds.; Lecture Notes in Computer Science; Springer: Berlin/Heidelberg, Germany, 2018; Volume 10892, pp. 143–162.

20.	Wang, T.; Cai, X.; Ren, Y.; Zhang, R. Security of quantum digital signatures for classical messages. *Sci. Rep.* **2015**, *5*, 9231. [CrossRef] [PubMed]

21.	Nikolopoulos, G.M.; Ioannou, L.M. Deterministic quantum-public-key encryption: Forward search attack and randomization. *Phys. Rev. A* **2009**, *79*, 042327. [CrossRef]

22.	Chabaud, U.; Diamanti, E.; Markham, D.; Kashefi, E.; Joux, A. Optimal quantum-programmable projective measurement with linear optics. *Phys. Rev. A* **2018**, *98*, 062318. [CrossRef]

23.	Nikolopoulos, G.M.; Diamanti, E. Continuous-variable quantum authentication of physical unclonable keys. *Sci. Rep.* **2017**, *7*, 46047. [CrossRef] [PubMed]

24.	Fladung, L.; Nikolopoulos, G.M.; Alber, G.; Fischlin, M. Intercept-Resend Emulation Attacks against a Continuous-Variable Quantum Authentication Protocol with Physical Unclonable Keys. *Cryptography* **2019**, *3*, 25. [CrossRef]