Quantum readout of Physical Unclonable Functions:

Remote authentication without trusted readers and authenticated Quantum Key Exchange without initial shared secrets

B. Škorić

Abstract

Physical Unclonable Functions (PUFs) are physical structures that are hard to clone and have a unique challenge-response behaviour. The term PUF was coined by Pappu et al. in 2001. That work triggered a lot of interest, and since then a substantial number of papers has been written about the use of a wide variety of physical structures for different security purposes such as identification, authentication, read-proof key storage, key distribution, tamper evidence, anti-counterfeiting, software-to-hardware binding and trusted computing.

In this paper we propose a new security primitive: the **quantum-readout PUF** (QR-PUF). This is a classical PUF which is challenged using a quantum state, e.g. a single-photon state, and whose response is also a quantum state. By the no-cloning property of unknown quantum states, attackers cannot intercept challenges or responses without noticeably disturbing the readout process. Thus, a verifier who sends quantum states as challenges and receives the correct quantum states back can be certain that he is probing a specific QR-PUF without disturbances, even in the QR-PUF is far away 'in the field' and under hostile control. For PUFs whose information content is not exceedingly large, all currently known PUF-based authentication and anti-counterfeiting schemes require trusted readout devices in the field. Our quantum readout scheme has no such requirement.

Furthermore, we show how the QR-PUF authentication scheme can be interwoven with Quantum Key Exchange (QKE), leading to an authenticated QKE protocol between two parties. This protocol has the special property that it requires no a priori secret shared by the two parties, and that the quantum channel is the authenticated channel, allowing for an unauthenticated classical channel.

1 Introduction

1.1 Physical Unclonable Functions

The term *Physical Unclonable Function* (PUF) was coined by Pappu et al. in [20, 21]. It refers to a physical object that is hard to clone and that can be subjected to challenges, yielding different random-looking outputs. A cryptographic equivalent of such challenge-response behaviour would be a keyed hash function, where the precise structure of the object represents the key. Pappu et al. also used the term *Physical One-Way Function* (POWF). Although the use of hard-to-clone (classical) physical structures for authentication purposes dates back a long time, the work [20, 21] was the first to introduce the 'function' behaviour of such objects and to consider mathematical unclonability as well (difficulty of modelling). It was shown that an optical medium with a high density of scatterers makes an extremely good PUF: A challenge consists e.g. of the angle of incidence of a laser beam; the response is the speckle pattern resulting from multiple coherent scattering. The speckle pattern has high entropy and strongly depends on the precise locations of the scatterers, which makes the object hard to clone.

The results of Pappu et al. have sparked a lot of interest in the use of (classical) physics for different security purposes such as identification, authentication, read-proof key storage, key distribution, tamper evidence, anti-counterfeiting, software-to-hardware binding and trusted computing. By now there is a whole zoo of PUF-like systems that have appeared in the literature: optical PUFs, delays in integrated circuits [11], dielectric properties of security coatings [24], two-dimensional fiber-optic configurations [16], radio-frequent probing of wire configurations [7] and thin-film resonators [28], laser probing of fibers in paper [3], startup values of SRAM cells [13], butterfly PUFs [17], phosphor patterns [5], phase-change memory states [18]. What all these have in common is a strong dependence of the measurement results on uncontrollable aspects of the manufacturing process. A partial overview of the field is given in [25].

Because of the wide variety of different physical systems and security goals involved, the terminology used in the literature can be confusing. There exist multiple definitions of a PUF, differing in their list of properties that must be satisfied. Often mentioned properties are physical unclonability, mathematical unclonability, uniqueness, tamper evidence, high response entropy, large number of different challenges and read-proofness. Descriptions like Physical One-Way Function, Physical Unknown Function, Physically Obfuscated/Obscured Key, and Physical Pseudorandom Function are sometimes used to specify which properties are most important for a certain application.

We mention explicitly that in this paper we rely only on the following properties of the pair {physical object, measurement method}:

- Physical unclonability. It is technically/financially infeasible to make a physical clone of a given QR-PUF (given full knowledge of this QR-PUF), such that it behaves exactly as the original one for the given measurement method.
- Quantum-computational unclonability. This is a new physical assumption. It is technically/financially infeasible to build a quantum computer and input/output handling which emulates a given QR-PUF (given full knowledge of this QR-PUF) with a sufficiently small delay time.
- Uniqueness. Different challenges can be applied to the QR-PUF. The number of different challenges does not have to be large. Together, the responses to these challenges (measurements) have to contain enough entropy so that all the to-be-authenticated QR-PUFs out in the field can be distinguished from each other, e.g. at least 20 bits of entropy to distinguish between a million QR-PUFs. In fact, uniqueness is implied by physical unclonability; if there are too few possible PUFs, then collisions can be created by manufacturing many random PUFs.

The entropy of optical PUFs was studied in [26, 27, 25]. We stress that the responses to all challenges, for each manufactured QR-PUF, are allowed to be public knowledge. In this paper, there is no secrecy concerning any aspect of the QR-PUFs.

Note that the PUF literature is concerned only with *classical* physics. The word 'unclonability' is an assumption about the *effort* it takes to produce a clone; it does not indicate that it is fundamentally impossible to produce one. There is no relation to the *provable* no-cloning theorem [29, 8] of unknown quantum states. Our QR-PUF is classical in itself, but the measurement is quantum, and we will make use of the no-cloning theorem to detect tampering with the measurement process.

1.2 Getting rid of the trusted remote reader

Some of the early PUF-based remote authentication protocols rely on the vastness of the PUF's entropy. At enrolment, Alice measures PUF responses for a large number of random challenges. She stores the table of challenge-response pairs (CRPs). Then the PUF is given to Bob. When Alice wants to authenticate Bob, she sends him a challenge, randomly selected from her CRP table. This is done over a public channel. Bob feeds the challenge to his PUF and measures the response. He sends the response to Alice over a public channel. If Bob's response is correct, Alice is convinced that he has access to the PUF. Alice deletes the used CRP from her list.

The security of such a protocol (assuming that Alice and Bob are honest) is based on the following physical assumptions: (I) Knowledge of eavesdropped CRPs gives negligible information about the response to a new challenge different from the eavesdropped ones; (II) It is infeasible for an attacker to characterize Bob's PUF in a short amount of time (e.g. the time needed to verify a credit card) with enough accuracy to predict the response to a new random challenge.

Although optical PUFs come a long way [26, 27] towards satisfying these assumptions, it is not clear whether high-entropy PUFs will be feasible in practice.

Even if one gives up the high-entropy property, PUFs are very useful. For instance[1], an effective authentication/anti-counterfeiting method can be designed that is based solely on the physical unclonability and uniqueness properties. Consider the following infrastructure. When a PUF gets manufactured, a PUF certification authority (PCA) enrolls it. This can be done in either of two ways. (i) A PUF identifier I and a precise characterization of the PUF (e.g. a CRP table) are entered into a publicly readable, PCA-maintained tamper proof database, or (ii) the PCA signs a digital certificate containing I and the PUF characterization, which certificate is then stored publicly (possibly attached to the PUF itself). Both options provide for a way to reliably obtain the enrolled data about a PUF. When a verifier wants to see if a certain PUF is authentic, he can check its challenge-response behaviour against the enrolled data. As long as the verifier knows for certain that responses are coming directly from a real PUF (as opposed to a mathematical emulation or a replay of data traffic), he is able to verify that a physical structure is the same as the enrolled one.

In the above scheme the verifier must be in control of the measurement device in order to prevent spoofing. This gives rise to an extra requirement for remote verification: the verifier has to trust a remotely located piece of measurement and processing hardware. One of the main results of this paper is that we achieve remote PUF authentication *without the trusted remote reader.*

1.3 Authenticated Quantum Key Exchange

Quantum Key Exchange (QKE), also known as Quantum Key Distribution (QKD), Quantum Key Agreement, and Quantum Cryptography, was first proposed in 1984 [1] (BB84). QKE is a protocol that allows Alice and Bob to establish an unconditionally secure shared secret if they have a channel at their disposal over which they can send quantum states. The security is based on the laws of quantum physics, in particular the no cloning theorem [29, 8], which ensures that eavesdropping and other attacks are detected. In its most easy to understand realization the protocol makes use of single-photon polarization states. Polarization can be measured in any direction perpendicular to light's direction of motion, i.e. there is a continuum of observables. However, the result of a measurement is a binary 'yes/no' answer.

The BB84 protocol can be summarized as follows in a nutshell. Alice generates two random bits. The first bit determines a basis: vertical/horizontal ('+') vs. diagonal ('×'). The second bit determines a direction within that basis, e.g. 0/1 for horizontal/vertical in the + basis. Alice sends a photon to Bob prepared in the state as described by the two bits. Bob randomly selects the + or × basis to measure the polarization. After a number of repetition of these steps Bob tells Alice which bases he has used. Alice discards all events where her basis and Bob's did not coincide. In the remaining cases Alice and Bob should have a shared secret bit. They publicly verify a random subset of their secret bitstring (which subset is then discarded) to see if there has been an attack. Next they perform information reconciliation (error correction to remove leftover noise) on their remaining bits and privacy amplification. The security of the protocol is derived from the fact that an eavesdropper, not knowing Alice's basis, has a probability of $< 100\%$ of correctly guessing her basis and hence being able to correctly clone the photon.

A huge number of papers and books on QKE has been written since 1984. Progress has been made on all relevant aspects: single-photon sources, detectors, fiber optic cables, attacks and defense, use of entanglement [10], error-correction codes, privacy amplification and security proof methods. QKE products based on BB84 are now commercially available. Quantum observables other than polarization have been proposed for QKE, e.g. phase [15] and squeezed coherent states [12].

The classical communication channel between Alice and Bob is allowed to be public, but it has to be authenticated in order to prevent man-in-the-middle attacks. Public key crypto can provide

[1] Another example is secure key storage, which relies only on read-proofness.

authentication. However, the aim of QKE is to achieve *unconditional* (information-theoretic) security, i.e. not relying on the kind of computational assumptions that public key crypto needs. One way to achieve information-theoretic authentication is to let Alice and Bob share a short initial MAC key. Though this may look like cheating, it is not. QKE serves to indefinitely lengthen an initial shared secret. Another way to achieve authentication is to let Alice and Bob each possess one part of an entangled state [22]. This approach has a number of practical drawbacks, such as the requirement that the entangled state has to be stored for a long time.

1.4 Our contributions

In this paper we introduce the concept of a Quantum Readout PUF (QR-PUF): a classical PUF that is challenged using a quantum state, and whose response is also a quantum state. (The only practical realization we can suggest at the moment is an optical PUF. Other options are not excluded, however.) In analogy with QKE, the no-cloning theorem ensures that eavesdropping on challenges or responses cannot go unnoticed. We rely on physical assumptions about the QR-PUF: physical unclonability and quantum-computational unclonability.

We present a protocol for authenticating a QR-PUF remotely without reliance on a trusted remote reader device. The protocol can be based on the reflection properties of the QR-PUF, or on both reflection and transmission. The remote authentication also serves as a distance bounding protocol. We give a security analysis, assuming that all QR-PUF properties are public, i.e. the only secrets in the protocol are the challenge states sent by the verifier. We prove that intercept-resend attacks fail. However, a QR-PUF can be spoofed by an attacker who has a sufficiently powerful quantum computer, combined with sufficiently fast ways of measuring qubit states as well as transferring challenge/response states into qubits and back. One of our physical assumptions says that such a powerful combination of quantum physical techniques is infeasible.

Then we show how the QR-PUF authentication can be intertwined with QKE. The idea is based on two main observations:

- The reflected states are used to authenticate the QR-PUF.
- The QR-PUF is completely 'transparent' with respect to transmitted states, in the sense that Alice can choose which quantum state reaches Bob after transmission through the QR-PUF, even if the transmission process is complicated.

We sketch an authenticated QKE protocol for n-dimensional challenge states. (BB84 readily follows as a special case for $n=2$.) We prove that intercept-resend attacks fail. The combination of QR-PUF authentication and QKE achieves interesting security properties:

1. The initial authentication between parties is achieved *without any shared secret* such as a MAC key or entangled state.
2. The security of the initial authentication is based on *physical assumptions* about the QR-PUF, combined with trust in the enrolled data (e.g. Alice enrolled the QR-PUF herself, or obtains the data from a trusted database). Thus, we do not have unconditional security. However, we find it worth showing that physical assumptions can be used in this way.
3. Traditional QKE schemes require an authenticated classical channel between Alice and Bob. We have the completely opposite situation: an authenticated quantum channel. Hence we do not require the classical channel to be authenticated.
4. The authentication of the quantum channel is based on the possession of an object, instead of knowledge of a secret. A secret can be stolen from Bob without him noticing the theft. Theft of an object usually does not go unnoticed.

In this paper we present the theoretical concepts. Implementations issues are left for future work. The outline of this paper is as follows. In Section 2 we briefly review quantum physics notation and explain which physical assumptions we make about the challenges and responses. In Section 3 we present two QR-PUF authentication protocols, including a security analysis. Finally, we combine QR-PUF authentication with QKE in Section 4.

2 Preliminaries

2.1 Quantum physics notation

Quantum states are represented as vectors in a Hilbert space. We adopt the usual 'bra' and 'ket' notation; $|\psi\rangle$ stands for a quantum state labelled by some description ψ which summarizes all the knowable information about the state. The Hermitian conjugate is denoted as $\langle\psi|$. The notation for the inner product between two states is $\langle\psi_1|\psi_2\rangle$. We will only consider states satisfying $\langle\psi|\psi\rangle = 1$, so-called normalized states.

Real-valued observables are represented by Hermitian operators acting on the Hilbert space. The j'th eigenvalue of an observable X is denoted as x_j, and the corresponding eigenvector as $|x_j\rangle$. We have $X|x_j\rangle = x_j|x_j\rangle$. The scalars $\langle e_i|X|e_j\rangle$, for some basis e, are called the matrix elements of X. The eigenvectors of any Hermitian operator X form an orthonormal basis of the Hilbert space, i.e. $\langle x_a|x_b\rangle = \delta_{ab}$. The completeness of this basis (in a finite Hilbert space of dimension n) is expressed as

$$\sum_{j=1}^{n} |x_j\rangle\langle x_j| = \mathbf{1}. \tag{1}$$

We will often write $[n]$ for the set $\{1, 2, \ldots, n\}$. The operator X can be written as

$$X = \sum_{j=1}^{n} x_j |x_j\rangle\langle x_j|. \tag{2}$$

Any state ψ can be expressed in terms of an orthonormal basis,

$$|\psi\rangle = \sum_{j=1}^{n} c_j|x_j\rangle \quad ; \quad c_j = \langle x_j|\psi\rangle. \tag{3}$$

Note that $c_j \in \mathbb{C}$ and $\sum_{j=1}^{n} |c_j|^2 = 1$. Measurement of X collapses the state onto one of the eigenvectors (or eigenspaces) of X, and yields the corresponding eigenvalue as the measurement result. When a measurement of X is performed on a state $|\psi\rangle$, the probability that $|\psi\rangle$ collapses to the eigenvector $|x_j\rangle$ is given by $|\langle x_j|\psi\rangle|^2$. For more background we refer to standard textbooks on quantum mechanics.

2.2 Challenge and response quantum states

We will be working with a physical system that has 'external' degrees of freedom (such as direction of motion) as well as an 'internal' degree of freedom (e.g. spin or polarization). This is formally denoted as a tensor product of Hilbert spaces: $\mathcal{H} = \mathcal{H}_{\text{ext}} \otimes \mathcal{H}_{\text{int}}$, where $\mathcal{H}$ is the full Hilbert space. We will be dealing with three types of state:

- **Challenge.** A quantum state is moving from Alice to Bob's PUF.
- **Reflected.** The particle has interacted with Bob's PUF, and its internal state has changed. The system moves back to Alice.
- **Transmitted.** The particle has interacted with Bob's PUF, and its internal state has changed. The particle does not return to Alice, but moves on.

These three situations are represented in only *two* states of motion: moving away from Alice or towards her. Any state $|\psi\rangle \in \mathcal{H}$ can be decomposed as

$$|\psi\rangle = |\text{outgoing}\rangle \otimes |\psi_1\rangle + |\text{incoming}\rangle \otimes |\psi_2\rangle \tag{4}$$

where $|\text{outgoing}\rangle, |\text{incoming}\rangle \in \mathcal{H}_{\text{ext}}$ and $|\psi_1\rangle, |\psi_2\rangle \in \mathcal{H}_{\text{int}}$. We have $\langle\text{outgoing}|\text{incoming}\rangle = 0$. The following notation can also be used,

$$|\psi\rangle = \begin{pmatrix} |\psi_1\rangle \\ |\psi_2\rangle \end{pmatrix}. \tag{5}$$

We assume that the internal Hilbert space $\mathcal{H}_{\text{int}}$ is finite-dimensional. The number of dimensions is n.

The interaction between the quantum system and the PUF is assumed to be completely coherent: time evolution is determined by the Schrödinger equation, without any state collapse. We abstractly represent the interaction with the PUF as a unitary time evolution operator S, also known in physics as the scattering matrix or S-matrix. This operator maps 'before' states to 'after' states. Let $|\psi'\rangle \in \mathcal{H}$ be the state after the interaction, then in the notation of (5) we have

$$\begin{pmatrix} |\psi'_1\rangle \\ |\psi'_2\rangle \end{pmatrix} = S \begin{pmatrix} |\psi_1\rangle \\ |\psi_2\rangle \end{pmatrix} \quad ; \quad S = \begin{pmatrix} T & -R^\dagger \\ R & T^\dagger \end{pmatrix}. \tag{6}$$

Here the operator T (the 'transmission matrix') contains all the details of how the internal state has changed when the particle emerges at the other side of the PUF, and the operator R ('reflection matrix') does the same for reflected states. The unitary nature of the evolution ($S^\dagger S = SS^\dagger = \mathbf{1}$) implies that $T^\dagger T + R^\dagger R = \mathbf{1}$ and that T, $T^\dagger$, R and $R^\dagger$ all commute with each other[2].

Together R and T completely determine the challenge-response behaviour of the PUF. Hence, in this formalism, physical unclonability of a PUF means that it is difficult to create a PUF which behaves precisely according to some pre-specified R and T.

In most of the rest of the paper we will completely omit any reference to the external degree of freedom, for notational simplicity. Only the internal state will be written. It will always be understood that Challenge and Transmitted states are moving away from Alice, and that Reflected states are moving towards her.

2.3 Assumptions about state preparation and observables

We assume that there is a lot of freedom in doing measurements and in preparing quantum states. More precisely, we assume that Alice can prepare basically any internal state $|\psi\rangle \in \mathcal{H}_{\text{int}}$. Similarly, there is a large number of different observables that Alice and Bob can measure. (In the case of photon polarization there is even a continuum of observables, namely the polarization component in any direction.)

This freedom allows one to define a set of measurements that accurately characterize a PUF. Let X and Y be two different observables, whose eigenvectors do not coincide. Let us write $R_{ab} := \langle x_a|R|x_b\rangle = |R_{ab}|e^{i\rho_{ab}}$ for the (complex) matrix elements of R. In practice the characterization of R could consist of the following steps:

- By repeatedly applying the same challenge $|x_i\rangle$ and measuring X, an accurate estimate is obtained for the absolute values $\{|R_{ji}|^2\}_{j=1}^n$. These numbers are the probabilities of measuring $|x_j\rangle$.

- Then part of the phase information of the matrix elements can be determined by applying 'mixed' challenges, i.e. challenges that are not an eigenstate of X. For instance, repeated application of the mixed challenge $\cos\alpha|x_i\rangle + e^{-i\varphi}\sin\alpha|x_k\rangle$ and measurement of X allows one to obtain an accurate estimate for the probabilities $p_j := |R_{ji}\cos\alpha + R_{jk}e^{-i\varphi}\sin\alpha|^2$ for $j \in [n]$. Since the absolute values $|R_{ab}|$ are known, one can compute

$$\frac{p_j - |R_{ji}|^2\cos^2\alpha - |R_{jk}|^2\sin^2\alpha}{|R_{ji}|\cdot|R_{jk}|\sin\alpha\cos\alpha} = 2\cos(\varphi + \rho_{ji} - \rho_{jk}).$$

[2] We can write $T = U^{-1}\Lambda U$ and $R = U^{-1}\Gamma U$, where U is a unitary matrix and Λ and Γ are complex-valued diagonal matrices satisfying $|\Lambda_i|^2 + |\Gamma_i|^2 = 1$ for all $i \in [n]$. The basis vectors contained in U can be thought of as eigenmodes of the S-matrix, i.e. modes which are transmitted and reflected without being changed by the QR-PUF (other than multiplication by a constant factor).

Doing this for two (or more) different values of φ yields the phase difference $\rho_{ji} - \rho_{jk}$. Repetition of this procedure for different i, j, k yields all the phase differences *within each row of* R.

- The phase differences within the *columns* of R are obtained in a way analogous to the previous step. The challenges are of the form $|x_i\rangle$, but the measured observable is Y.

The above procedure, or any variant of it, gives all the complex values R_{ji} up to a global phase factor. This global phase can be chosen e.g. such that $R_{11} \in \mathbb{R}$.
Of course, the accuracy of the characterization depends on the number of repetitions N of each experiment. The relative error in the matrix elements is proportional to $1/\sqrt{N}$. Determination of T is completely analogous.
Finally we assume that a measurement of the internal state is able to discern whether or not there is a particle present at all. This statement is not trivial. Filter-based polarization measurements for instance do not see the difference between darkness and polarization perpendicular to the applied filter. Measurements using a polarization splitter and measurement of differential phase shift [15], on the other hand, do distinguish between presence and absence of a photon.

3 Remote authentication of a QR-PUF

We present two protocols for remote authentication of a QR-PUF. The first one is applicable when every conceivable projection operator corresponds to an actual measurement that can be performed. The second one is geared to more restricted circumstances where Alice has only a limited number of projection measurements at her disposal. Both protocols are based on reflected states only. We consider the case $T = 0$.[3] In Section 4 a protocol will be discussed with $T \neq 0$.

3.1 Attack model

Alice wants to verify if Bob has *real-time access* to a certain QR-PUF. The main attack to protect against is impersonation: someone may be trying to convince Alice that he has access to the QR-PUF even though in reality he does not. Either he has never had access to the QR-PUF at all, or he has had access at some point in the past.
Alice and Bob send quantum states over the quantum channel as described in Section 2. Bob has physical access to challenge states as well as reflected states. He can destroy quantum states, perform measurements on them, and insert new states. However, he cannot clone a state. We assume that R and T are fully known to Bob. (Either because it is public information, or because he has had access to the QR-PUF in the past.) However, as discussed in Section 1.1, it is assumed infeasible to create a new QR-PUF whose reflection matrix is R. It is also assumed infeasible to build a quantum computer that emulates the QR-PUF with a very small time delay.
There is a source of enrollment data trusted by Alice (e.g. she enrolls QR-PUFs herself).

3.2 Authentication protocol 1

This is a protocol for the reflection degree of freedom only. We consider the case $T = 0$ (and hence $R^\dagger R = 1$). It is assumed that Alice can perform a projection measurement onto any state in the Hilbert space.

Enrollment phase
A QR-PUF with identifier I is accurately characterized (see Section 2.3). This yields the matrix R. The QR-PUF is given to Bob.

Authentication phase
Bob claims that he has access to the QR-PUF with identifier I. Alice fetches the enrollment data R corresponding to I.

[3] There is no loss of generality; transmitted states can always be re-routed to become part of the reflected state.

She initializes counters $n_{\rm ret}$ and $n_{\rm ok}$ to zero. She then repeats the following procedure m times:

1. Alice prepares a state $|\psi\rangle$ uniformly at random and sends it to Bob.
2. Alice receives either nothing ('$\perp$') or a returning state $|\omega\rangle$. If she receives a state[4], then
   (a) She increases $n_{\rm ret}$ by one.
   (b) If $|\psi\rangle$ was properly reflected by Bob's QR-PUF, then the returned state should be $|\omega_\psi\rangle := R|\psi\rangle$. Alice measures the projection of $|\omega\rangle$ onto $|\omega_\psi\rangle$, i.e. she performs a measurement of the operator $|\omega_\psi\rangle\langle\omega_\psi|$, obtaining either '0' or '1' as the outcome. If the outcome is 1, then she increases $n_{\rm ok}$ by one.

If the fraction $n_{\rm ret}/m$ of returned states is not consistent with the expected noise level, then the protocol is aborted.
If $n_{\rm ok} \geq (1-\varepsilon)n_{\rm ret}$ then Alice is convinced that she has probed the QR-PUF with identifier I. Here ε is a parameter denoting the tolerable fraction of wrong responses.

3.3 Security of authentication protocol 1

In the above protocol, and the other protocols in this paper, Alice waits for a returning state before sending her next challenge state. This considerably simplifies the security proofs, since in this setting it suffices to look at the security of an isolated round without having to worry about (entanglement) attacks on multiple challenge states. We leave more general protocols and their security proof as a subject for future work.

3.3.1 Intercept-resend attacks

We consider the type of attack where an impostor tries to convince Alice that he has the QR-PUF. Since he does not know Alice's random ψ, the best he can do is the following. (a) For each of the m rounds he picks a random orthonormal basis of the n-dimensional Hilbert space. The corresponding Hermitian operator is denoted as B, with eigenvalues b_j and eigenstates $|b_j\rangle$ that form the basis. (b) He measures B, obtaining outcome b_k for some $k \in [n]$. (c) He chooses a state $|\zeta\rangle$ such that $\langle b_k|\zeta\rangle = 0$ and a parameter $\alpha \in [0, \pi/2]$ according to some (possibly probabilistic) strategy $\mathcal{A}$ that may depend on B and k. He computes $|\chi\rangle$,

$$|\chi\rangle = \cos\alpha|b_k\rangle + \sin\alpha|\zeta\rangle, \tag{7}$$

which is his guess for $|\psi\rangle$. Finally he prepares a state $|\omega\rangle$ and sends it to Alice,

$$|\omega\rangle = R|\chi\rangle. \tag{8}$$

Theorem 1 *In the intercept-resend attack described above, the impostor's probability p_1 of success in a single round of protocol 1 is bounded as*

$$p_1 \leq \frac{2}{n+1}.$$

Proof: In a given round, the impostor is successful if Alice's measurement of the operator $|\omega_i\rangle\langle\omega_i|$ produces outcome '1'. Let $\mathbb{E}_\psi$ and $\mathbb{E}_B$ denote the expectation values over ψ and B respectively. (We will use the '$\mathbb{E}$' notation as a function that acts on everything to the right.) Then the success probability p_1 in a single round is given by

$$p_1 = \mathbb{E}_\psi \mathbb{E}_B \sum_{k\in[n]} |\langle b_k|\psi\rangle|^2 \sum_\alpha \sum_\zeta \mathcal{A}[\alpha, \zeta|B, k] \; |\langle\omega_\psi|\omega\rangle|^2. \tag{9}$$

[4] A state that arrives too late is counted as $\perp$. This is a form of distance bounding. If Alice has a rough idea where Bob should be located, she knows what round-trip time to expect.

The factor $|\langle b_k|\psi\rangle|^2$ is the probability of the outcome b_k when B is measured. The $\mathcal{A}[\alpha,\zeta|B,k]$ stands for the probability that the impostor chooses α,ζ for given B,k. The factor $|\langle\omega_\psi|\omega\rangle|^2$ is the probability that the returned state projects onto $|\omega_\psi\rangle$. We have

$$\langle\omega_\psi|\omega\rangle = \langle\chi|R^\dagger R|\psi\rangle = \langle\chi|\psi\rangle. \tag{10}$$

Using (10) and changing the order of the summations/expectation values we can rewrite (9) as

$$p_1 = \mathbb{E}_B \sum_{k\in[n]} \sum_\alpha \sum_\zeta \mathcal{A}[\alpha,\zeta|B,k]\; \mathbb{E}_\psi |\langle b_k|\psi\rangle|^2 \left|\cos\alpha\langle b_k|\psi\rangle + \sin\alpha\langle\zeta|\psi\rangle\right|^2. \tag{11}$$

Since the expectation value $\mathbb{E}_\psi$ is over uniformly chosen random ψ, the $\mathbb{E}_\psi$ has no preferred direction in Hilbert space. Consequently, the expression $\mathbb{E}_\psi(\cdots)$ in (11) cannot depend on the actual directions of $|b_k\rangle$ and $|\zeta\rangle$, but only on α and the inner product $\langle b_k|\zeta\rangle$ (which vanishes by definition). We can replace $\langle b_k|$ by some fixed state $\langle e_1|$ and $\langle\zeta|$ by a fixed $\langle e_2|$, with $\langle e_2|e_1\rangle = 0$. The sum over ζ becomes trivial and turns $\mathcal{A}[\alpha,\zeta|B,k]$ into the marginal probability $\mathcal{A}[\alpha|B,k]$. So we can write

$$\begin{aligned} p_1 &= \sum_\alpha \mathbb{E}_\psi\left[|\langle e_1|\psi\rangle|^2 \left|\cos\alpha\langle e_1|\psi\rangle + \sin\alpha\langle e_2|\psi\rangle\right|^2\right] \mathbb{E}_B \sum_{k\in[n]} \mathcal{A}[\alpha|B,k] \\ &= \sum_\alpha \sum_{k\in[n]} \mathbb{E}_B \mathcal{A}[\alpha|B,k] \left\{ \cos^2\alpha\, \mathbb{E}_\psi[|\langle e_1|\psi\rangle|^4] + \sin^2\alpha\, \mathbb{E}_\psi[|\langle e_1|\psi\rangle|^2 |\langle e_2|\psi\rangle|^2] \right\}. \end{aligned} \tag{12}$$

In the last step we have used the fact that $\mathbb{E}_\psi[\langle e_2|\psi\rangle\langle\psi|e_1\rangle^3] = 0$ because of symmetry reasons. Without loss of generality we parametrize the uniformly random state as $|\psi\rangle = \sum_{j\in[n]}(x_j + iy_j)|e_j\rangle$, with coordinates $x_j\in\mathbb{R}$, $y_j\in\mathbb{R}$ uniformly drawn from the hypersphere $\sum_j x_j^2 + \sum_j y_j^2 = 1$. This gives

$$\begin{aligned} \mathbb{E}_\psi[|\langle e_1|\psi\rangle|^4] &= \mathbb{E}_\psi[x_1^4 + y_1^4 + 2x_1^2 y_1^2] \qquad (13) \\ \mathbb{E}_\psi[|\langle e_1|\psi\rangle|^2 |\langle e_2|\psi\rangle|^2] &= \mathbb{E}_\psi[(x_1^2 + y_1^2)(x_2^2 + y_2^2)]. \qquad (14) \end{aligned}$$

We compute these expectation values as follows. If f is a function that depends only on the squares of the x_j, y_j coordinates then we can write $\mathbb{E}_\psi[f] \propto \int_0^1 \mathrm{d}^{2n}p\; \mathbf{p}^{-1/2}\delta(1-\sum_{a\in[2n]} p_a) f(\mathbf{p})$, where $p_1 = x_1^2$, $p_2 = y_1^2$, $p_3 = x_2^2$, $\cdots$, $p_{2n} = y_n^2$, and $\mathbf{p}^{-1/2}$ is multi-index notation for $\prod_a p_a{}^{-1/2}$. We make use of the Dirichlet integral identity $\int_0^1 \mathrm{d}^{2n}p\; \mathbf{p}^{-1/2}\delta(1-\sum_a p_a)\mathbf{p}^{\mathbf{s}} = B(\frac12 1_{2n} + \mathbf{s})$, where $\mathbf{p}^{\mathbf{s}}$ is multi-index notation for $\prod_a p_a^{s_a}$, 1_{2n} is a vector consisting of $2n$ ones, and B is the generalized Beta function, defined as $B(\mathbf{t}) = [\prod_a \Gamma(t_a)]/\Gamma(\sum_a t_a)$. We obtain

$$\begin{aligned} \mathbb{E}_\psi[x_j^4] &= \frac{\int_0^1 \mathrm{d}^{2n}p\; \mathbf{p}^{-1/2}\delta(1-\sum_{a\in[2n]} p_a)\; p_j^2}{\int_0^1 \mathrm{d}^{2n}p\; \mathbf{p}^{-1/2}\delta(1-\sum_{a\in[2n]} p_a)} = \frac{B(\frac12 1_{2n} + 2e_j)}{B(\frac12 1_{2n})} = \frac{3}{4n(n+1)} \qquad (15) \\ \mathbb{E}_\psi[x_i^2 x_j^2] &= \frac{\int_0^1 \mathrm{d}^{2n}p\; \mathbf{p}^{-1/2}\delta(1-\sum_{a\in[2n]} p_a)\; p_i p_j}{\int_0^1 \mathrm{d}^{2n}p\; \mathbf{p}^{-1/2}\delta(1-\sum_{a\in[2n]} p_a)} = \frac{B(\frac12 1_{2n} + e_i + e_j)}{B(\frac12 1_{2n})} = \frac{1}{4n(n+1)}. \qquad (16) \end{aligned}$$

In the last line it holds that $i\neq j$. Using (15,16) we get

$$\mathbb{E}_\psi[|\langle e_1|\psi\rangle|^4] = \frac{2}{n(n+1)} \quad ; \quad \mathbb{E}_\psi[|\langle e_1|\psi\rangle|^2 |\langle e_2|\psi\rangle|^2] = \frac{1}{n(n+1)}. \tag{17}$$

Here we have also made use of the fact that $\mathbb{E}_\psi[y_j^4] = \mathbb{E}_\psi[x_j^4]$ and $\mathbb{E}_\psi[x_i^2 y_j^2] = \mathbb{E}_\psi[x_i^2 x_j^2]$ due to symmetry. Substitution of (17) into (12) shows that the factor multiplying $\cos^2\alpha$ is larger than the factor multiplying $\sin^2\alpha$. Hence the best strategy for the impostor is to always set $\alpha = 0$, independent of B and k. The $\mathbb{E}_B$ then gives a factor 1, and $\sum_k$ gives a factor n. The end result follows. □

3.3.2 Attack by quantum computer

It is possible in theory to break the QR-PUF authentication scheme if one has [i] a sufficiently powerful quantum computer (QC) *and* [ii] a sufficiently fast way of transferring challenge states into the QC's qubits and transferring the computation result back to a response state;

We give a high-level description of the attack. It has three steps. First the challenge state $|\psi\rangle$ is transferred to the working memory of the QC (qubits or higher-alphabet digits). This can be done without measuring $|\psi\rangle$, namely by quantum teleportation [2], in particular a form of teleportation that transfers states from one type of physical system to another [9, 19]. Then the QC does a computation that has the effect of applying R. This is possible in theory since R is known publicly, and applying R is a unitary operation. The result of the computation is teleported to a response state and sent to Alice over the quantum channel.

Our assumption denoted as 'quantum-computational unclonability' states that it is either technically/financially too difficult to pull off the above given steps or, if all the hardware works, the attack is too slow.

It is not yet clear to us how to make quantitative statements about the difficulty of launching an effective 'quantum' attack. For instance, the challenge ψ could comprise a random choice of photon wavelength λ, with the R-matrix depending on λ. How is the information about λ transferred to the quantum memory? How does the attacker know which R to apply in the quantum computation step? Does he have to construct a big unitary operation that acts on all wavelengths simultaneously? That would certainly strain the QC hardware.

3.3.3 Attack with an imperfect physical clone

Consider the case of an attempted physical clone which is not quite equal to the original one.

Theorem 2 *Let $\delta > 0$ be a constant. Let the imperfect clone have a unitary reflection matrix R'. Let the eigenvalues of $R^{-1}R'$ be denoted as $\{e^{i\varphi_k}\}_{k\in[n]}$. Let these eigenvalues satisfy*

$$|\sum_{k\in[n]} e^{i\varphi_k}|^2 \leq n^2(1-\delta). \tag{18}$$

Then the impostor's per-round probability of success is bounded by

$$p_1 \leq 1 - \frac{n}{n+1}\delta. \tag{19}$$

Proof: Since the imperfect clone reflects a challenge $|\psi\rangle$ as $R'|\psi\rangle$, we have $p_1 = \mathbb{E}_\psi|\langle\psi|R^\dagger R'|\psi\rangle|^2$, where $R^\dagger$ is not quite the inverse of R'. The matrix $R^\dagger R'$ is unitary and hence it can be written as $U^\dagger \text{Diag}(e^{i\varphi_k})U$, where U is unitary. The U can be absorbed into the dummy integration variable ψ, since averaging over $U|\psi\rangle$ is the same as averaging over ψ. Thus we have $p_1 = \mathbb{E}_\psi|\langle\psi|\text{Diag}(e^{i\varphi_k})|\psi\rangle|^2$. Next we decompose $|\psi\rangle$ in the basis where $R^\dagger R'$ is diagonal, $|\psi\rangle = \sum_k c_k|k\rangle$. This gives

$$p_1 = \mathbb{E}_\psi \left|\sum_k |c_k|^2 e^{i\varphi_k}\right|^2 = \mathbb{E}_\psi \left(\sum_k |c_k|^4 + \sum_{k,l\ (k\neq l)} |c_k|^2|c_l|^2 e^{i\varphi_k}e^{-i\varphi_l}\right). \tag{20}$$

We use the $\mathbb{E}_\psi$ expectation values listed in (17). This yields

$$p_1 = \sum_k \frac{2}{n(n+1)} + \sum_{k,l\ (k\neq l)} \frac{1}{n(n+1)} e^{i\varphi_k}e^{-i\varphi_l} = \frac{1}{n+1} + \frac{1}{n(n+1)}\left|\sum_k e^{i\varphi_k}\right|^2. \tag{21}$$

Finally, using the condition (18) we get the end result (19). □

3.4 Authentication protocol 2

The 2nd protocol also considers the case of complete reflection ($T = 0$). The difference with protocol 1 is a restriction on the measurements available to Alice. She can no longer choose any projection measurement $|\psi\rangle\langle\psi|$. Instead she has a limited set of s different observables $\{X_\alpha\}_{\alpha=1}^{s}$ at her disposal. These are Hermitian operators, and hence they have orthonormal sets of eigenvectors. The i'th eigenstate of X_α is denoted as $|\alpha i\rangle$, with $i \in [n]$. We make two assumptions about the set of observables:

- The X_α all have non-degenerate eigenvalues. This allows Alice to effectively turn a measurement of X_α into a (projection) measurement of $|\alpha i\rangle\langle\alpha i|$ for some i.
- For $\alpha \neq \beta$ it holds that $\forall i, j \in [n] : \; |\langle\alpha i|\beta j\rangle| < D$, where $D \in [1/\sqrt{n}, 1)$ is a constant.

The impostor has no restrictions on his choice of observable B. There are no restrictions on the state preparation, neither for Alice nor the impostor.

Enrollment phase
A QR-PUF with identifier I is accurately characterized (see Section 2.3). This yields the matrix R. The QR-PUF is given to Bob.

Authentication phase
Bob claims that he has access to the QR-PUF with identifier I. Alice fetches the enrollment data R corresponding to I.
She initializes counters $n_{\rm ret}$ and $n_{\rm ok}$ to zero. She then repeats the following procedure m times:

1. Alice draws $\alpha \in [s]$ and $i \in [n]$ uniformly at random. She prepares the state $R^{-1}|\alpha i\rangle$ and sends it to Bob.
2. Alice receives either nothing ('$\perp$') or a returning state $|\omega\rangle$. If she receives a state, then
   (a) She increases $n_{\rm ret}$ by one.
   (b) She performs a measurement of the operator $|\alpha i\rangle\langle\alpha i|$, obtaining either '0' or '1' as the outcome. If the outcome is 1, then she increases $n_{\rm ok}$ by one.

If the fraction $n_{\rm ret}/m$ of returned states is not consistent with the expected noise level, then the protocol is aborted.
If $n_{\rm ok} \geq (1-\varepsilon)n_{\rm ret}$ then Alice is convinced that she has probed the QR-PUF with identifier I. Here ε is a parameter denoting the tolerable fraction of wrong responses.

3.5 Security of authentication protocol 2

The intercept-resend attack is of the same kind as in Section 3.3.1. The impostor performs a measurement of some strategically chosen B and obtains outcome b_k. He has some strategy $\mathcal{A}$ to choose a state $|\omega\rangle$ as a function of B and k. He sends $|\omega\rangle$ to Alice.

Theorem 3 *In the above described intercept-resend attack on protocol 2, the per-round success probability p_2 is bounded by*

$$p_2 < \frac{1+(s-1)D}{s}.$$

Proof: We write

$$p_2 = \mathbb{E}_\alpha \mathbb{E}_i \mathbb{E}_B \sum_{k\in[n]} |\langle b_k|R^{-1}|\alpha i\rangle|^2 \sum_\omega \mathcal{A}[\omega|B,k] \; |\langle\omega|\alpha i\rangle|^2. \tag{22}$$

The sum over i can be interpreted as a weighted average of some quantity, with weights $|\langle\omega|\alpha i\rangle|^2$. The average of a list cannot exceed the largest element in the list. Thus we can write

$$\begin{aligned} p_2 &\leq \mathbb{E}_\alpha \mathbb{E}_B \sum_{k\in[n]} \frac{1}{n} \max_{i\in[n]} |\langle b_k|R^{-1}|\alpha i\rangle|^2 \sum_\omega \mathcal{A}[\omega|B,k] \\ &= \frac{1}{ns}\mathbb{E}_B \sum_{k\in[n]} \sum_{\alpha\in[s]} \max_{i\in[n]} |\langle b_k|R^{-1}|\alpha i\rangle|^2. \end{aligned} \tag{23}$$

In the last line we have used the fact that $\mathcal{A}[\omega|B,k]$ is a probability distribution for ω. We have also changed the order of some of the summations.
We introduce the notation $i_*(\alpha)$ for the value of i that achieves the maximum in (23), suppressing its dependence on k in the notation. We define $|v_\alpha\rangle = |\alpha i_*(\alpha)\rangle$, $Y = \sum_\alpha |v_\alpha\rangle\langle v_\alpha|$ and $|\omega_k\rangle = R|b_k\rangle$. We then have

$$\sum_{\alpha\in[s]} \max_{i\in[n]} |\langle b_k|R^{-1}|\alpha i\rangle|^2 = \langle\omega_k|Y|\omega_k\rangle. \tag{24}$$

An expectation value of this form cannot exceed the largest eigenvalue of Y. (Note that Y is Hermitian and hence all its eigenvalues are real.) If we decompose an eigenstate $|y\rangle$ as $|y\rangle = \sum_\beta d_\beta|v_\beta\rangle$ (the v_β are *not* orthogonal) then the eigenvalue equation $Y|y\rangle = y|y\rangle$ implies $\forall\alpha$: $\sum_\beta\langle v_\alpha|v_\beta\rangle d_\beta = yd_\alpha$. Hence an equivalent problem is to look for the largest eigenvalue of the Hermitian matrix V, defined as $V_{\alpha\beta} = \langle v_\alpha|v_\beta\rangle$. This type of matrix is called a Gram matrix, and it has the property that all its eigenvalues are nonnegative. The diagonal entries of V are all 1, and all the off-diagonal entries are bounded by $|V_{\alpha\beta}| \leq D$. The largest eigenvalue $y_{\max}$ is maximal when the $|v_\alpha\rangle$ vectors align as much as possible, i.e. the inner products $\langle v_\alpha|v_\beta\rangle$ are as large as possible. (In that case the projection operators $|v_\alpha\rangle\langle v_\alpha|$ have maximum overlap.) Setting $V_{\alpha\beta} = D$ we get $y_{\max} = 1 + (s-1)D$. Substitution into (23) gives

$$p_2 \leq \frac{1}{ns}\mathbb{E}_B \sum_{k\in[n]} [1 + (s-1)D]. \tag{25}$$

The k-sum gives a factor n. The expectation $\mathbb{E}_B$ is trivial. □

Just as protocol 1, this protocol is vulnerable to a 'quantum' attack employing quantum teleportation and a quantum computer. The attack and the requirements are exactly the same as in Section 3.3.2.

3.6 Limitations on the state preparation

If there are also restrictions on Alice's state preparation, it is still possible to construct an effective authentication scheme. Consider the most pessimistic case: Alice is only capable of preparing eigenstates of the observables X_α. This is still sufficient for her to fully characterize Bob's QR-PUF. All she has to do is select random α and j, send $|\alpha j\rangle$ and do a measurement of X_α on the reflected state. After many repetitions, this procedure gives her all the matrix elements $\langle\alpha j|R|\alpha k\rangle$, i.e. all the information about R (even in multiple bases).
That is a perfectly viable method. The only drawback is proof-technical. Proving security cannot be done by finding a bound on a per-round success probability of spoofing; even if Bob's return states are correct, Alice's measurement results are stochastic, since in general $R|\alpha j\rangle$ is not an eigenstate of X_α. Hence Alice cannot assign a label 'correct' to a single round.

4 Combining QR-PUF authentication with QKE

In this section we combine the authentication with a Quantum Key Exchange protocol that is performed on the Transmitted states. The intuition is as follows. Since Alice knows T, she can prepare $|\psi\rangle \propto T^{-1}|\varphi\rangle$, for arbitrary φ, such that Bob receives φ if transmission occurs. In this sense the QR-PUF is ‘transparent’ for the purpose of sending specific states to Bob. In particular this means that Alice and Bob can run a Quantum Key Exchange protocol *through the QR-PUF*. Some of Alice’s challenges will be reflected back to Alice. She uses these to authenticate the QR-PUF. We assume that Alice can perform arbitrary projection measurements.

The protocol presented in this section authenticates Bob to Alice. If mutual authentication is required, the protocol can be run twice: first authenticating one party, then the other.

4.1 Attack model

Bob claims that he possesses a QR-PUF with identifier I. Alice’s goal is to authenticate QR-PUF I and to generate a shared secret key with the party possessing that QR-PUF. Eve’s goal is to learn the generated key. If Bob is malicious, his goal is to convince Alice that he has real-time access to the QR-PUF even though he does not.

We make the following assumptions. Alice is honest. Bob may be acting in one of the following ways: (i) He is honest. (ii) He has access to the QR-PUF but does not hold it personally. He is in collusion with the party holding the QR-PUF. (iii) He has access to the QR-PUF but does not hold it personally. The party holding the QR-PUF is not cooperating with him. (iv) He does not have access to the QR-PUF.

In cases (i) and (ii) the protocol should result in authentication and a shared key, even though in case (ii) the secret key is shared between Alice and the PUF holder, while Bob may not even know the key. Case (iii) should result in authentication without a shared key. Case (iv) should not even result in authentication.

Eve has physical access to Challenge and Reflected states, but *not* to Transmitted states. (Only the QR-PUF holder has access to those.) She can destroy quantum states, perform measurements on them and insert new states. However, she cannot clone a state.

We assume that the R and T matrices are both public information. Creation or real-time emulation of a QR-PUF whose challenge-response matrix is R is assumed infeasible. We make no such assumption about the T matrix.

There is a source of enrollment data trusted by Alice and Bob. We stress that the classical channel between Alice and Bob *does not have to be authenticated*.

4.2 Protocol description

System setup phase

Our scheme makes use of MACs with the *Key Manipulation Security* property (KMS-MAC) [6]. This is necessary since the classical messages are subject to manipulation attacks that influence the key. Use is made of two (publicly known) information-theoretically secure KMS-MACs $M_1 : \{0,1\}^{\ell_1} \times \{0,1\}^{m_1} \to \{0,1\}^{c_1}$ and $M_2 : \{0,1\}^{\ell_2} \times \{0,1\}^{m_2} \to \{0,1\}^{c_2}$. A MAC over message x using key k will be denoted as $M(k;x)$.

A further public ‘system parameter’ is a universal [4] or almost-universal [23] hash function $F : \{0,1\}^N \times \{0,1\}^\sigma \to \{0,1\}^L$ which maps an N-bit string onto an L-bit string using σ bits of randomness.

Finally there is an error-correcting code with messages in $\{0,1\}^N$ and codewords in $[n]^b$, which is chosen to have sufficient error-correcting capability to cope with the expected level of noise. The code word size b is somewhat smaller than $m/2$, namely the expected number of rounds that yield a shared secret (corrected for particle loss). The encoding and decoding operations are denoted as `Code` and `Dec`. Addition modulo n (with output in $[n]$) will be denoted as $\oplus$.

Enrollment phase

A QR-PUF is labeled with identifier I. The R and T matrix are accurately measured. The QR-PUF is given to Bob. Two observables X_0, X_1 are selected. They may be chosen depending on R and T, or independently. The kth eigenstate of X_α is denoted as $|x_{\alpha k}\rangle$. The eigenstates satisfy

$|\langle x_{0i}|x_{1j}\rangle|^2 = 1/n$ for all[5] $i, j \in [n]$. The R, T, X_0 and X_1 are public knowledge.

Authentication and key exchange phase

1. Alice fetches the enrollment data for PUF I. For $\alpha \in \{0,1\}$, $i \in [n]$ she initializes the following counters to zero: $m_{\alpha i}$ (for counting sent states), $g_{\alpha i}$ (returned states), $c_{\alpha i}$ (correct return states). She initializes a set $\mathcal{V}$ to $\emptyset$ (pointers to transmitted states). Alice and Bob both initialize a counter t to zero.

2. The following steps are repeated m times:

   (a) Alice and Bob increase t by 1. Alice selects $\alpha \in \{0,1\}$ and $i \in [n]$ uniformly at random. She increases $m_{\alpha i}$. She stores $\alpha_t = \alpha$ and $i_t = i$. She prepares the state

   $$|\psi_{\alpha i}\rangle := \frac{T^{-1}|x_{\alpha i}\rangle}{\sqrt{\langle x_{\alpha i}|(T^{-1})^\dagger T^{-1}|x_{\alpha i}\rangle}}$$

   and sends it to Bob. She performs a projection measurement $|\omega_{\alpha i}\rangle\langle\omega_{\alpha i}|$, with

   $$|\omega_{\alpha i}\rangle := \frac{RT^{-1}|x_{\alpha i}\rangle}{\sqrt{\langle x_{\alpha i}|(T^{-1})^\dagger R^\dagger RT^{-1}|x_{\alpha i}\rangle}}. \tag{26}$$

   If she detects the existence of a return state, she increases $g_{\alpha i}$; else she adds t to $\mathcal{V}$. If her projection measurement yields outcome '1', she increases $c_{\alpha i}$.

   (b) Bob chooses a random bit β. He performs a measurement of X_β, obtaining either '$\perp$' (no transmitted state) or the j'th eigenvalue of X_β. If he gets $\perp$ then he stores $\beta_t = \perp$; else he stores $\beta_t = \beta$ and $j_t = j$.

3. Bob sends the vector $\vec{\beta}$ to Alice. Alice runs the following tests:

   (a) She checks how many states were lost ($t \in \mathcal{V} \wedge \beta_t = \perp$) and how many double counts occurred ($t \notin \mathcal{V} \wedge \beta_t \neq \perp$). If the number of either one of these occurrences is too high, then the noise level is considered too high and the protocol is aborted.

   (b) She checks if the transmission rates for all α, i were consistent with scattering by the QR-PUF. She does this by verifying if the vector $(1-\frac{g_{01}}{m_{01}}, 1-\frac{g_{11}}{m_{11}}, \cdots, 1-\frac{g_{0n}}{m_{0n}}, 1-\frac{g_{1n}}{m_{1n}})$ is proportional to $(\tau_{01}, \tau_{11}, \cdots, \tau_{0n}, \tau_{1n})$, where the $\tau_{\alpha i}$ are the transmission probabilities,

   $$\tau_{\alpha i} := \langle\psi_{\alpha i}|T^\dagger T|\psi_{\alpha i}\rangle = \frac{1}{\langle x_{\alpha i}|(T^\dagger T)^{-1}|x_{\alpha i}\rangle}. \tag{27}$$

   If there is a significant deviation then authentication has failed and the protocol is aborted.

   (c) For each $\alpha \in \{0,1\}$, $i \in [n]$ she checks if $c_{\alpha i}/g_{\alpha i} \geq (1-\varepsilon)$, where ε is a small constant. If this is not the case, then authentication has failed and the protocol is aborted.

4. Alice compiles $\mathcal{Z} = \{t : t \in \mathcal{V} \wedge \alpha_t = \beta_t\}$ and randomly selects a subset $\mathcal{G} \subset \mathcal{Z}$ of size b. She generates random $a \in \{0,1\}^N$ and $y \in \{0,1\}^\sigma$. She computes $S = F(a,y)$ and parses S as $S = k_1|k_2|S_{\text{rest}}$, with $k_1 \in \{0,1\}^{\ell_1}$ and $k_2 \in \{0,1\}^{\ell_2}$. She computes $w = \vec{\imath}_{\mathcal{G}} \oplus \texttt{Code}(a)$, $\mu_1 = M_1(k_1; \mathcal{G}, w, y)$, $\mu_2 = M_2(k_2; \vec{\beta})$. She sends $\mathcal{G}, w, y, \mu_1$.

5. Bob computes $a' = \texttt{Dec}(\vec{\jmath}_{\mathcal{G}} \oplus w)$ and $S' = F(a', y)$. He parses S' as $S' = k_1'|k_2'|S'_{\text{rest}}$, with $k_1 \in \{0,1\}^{\ell_1}$ and $k_2' \in \{0,1\}^{\ell_2}$. He computes $\mu_1' = M_1(k_1'; \mathcal{G}, w, y)$, $\mu_2' = M_2(k_2'; \vec{\beta})$. He checks if $\mu_1 = \mu_1'$. If not, the protocol is aborted. He sends μ_2'.

[5] Such inner products can be achieved for instance by having

$$|x_{1k}\rangle = \frac{1}{\sqrt{n}}\sum_{j=1}^{n}(e^{-i2\pi/n})^{kj}|x_{0j}\rangle \quad ; \quad |x_{0a}\rangle = \frac{1}{\sqrt{n}}\sum_{k=1}^{n}(e^{i2\pi/n})^{ka}|x_{1k}\rangle.$$

6. Alice checks if $\mu_2' = \mu_2$. If not, the protocol is aborted.

If the protocol does not abort then Alice and Bob have a noiseless shared secret $S_{\rm rest} \in \{0,1\}^{L-\ell_1-\ell_2}$ about which Eve has negligible information, and Alice knows that she has generated this secret together with someone who has real-time access to the QR-PUF. Bob knows that he has a shared secret with someone who has sent challenges over the quantum channel, but has no further knowledge about this person.

4.3 Remarks

We have deliberately not specified what "too high" means in step 3a, and "significant deviation" in step 3b. We give no numbers for m, b, N, L, σ, ℓ_1, ℓ_2, c_1, c_2. These are design choices (threshold values etc.) that have been adequately treated in the existing literature on QKE and KMS-MACs. We do not wish to further elaborate on such design choices in this paper.

The protocol may be modified in numerous ways without changing its essential properties. The classical communication between Alice and Bob may occur in a different order. The moment of checking the reflection rates may be shifted, etc.

As remarked before, if Alice and Bob want *mutual* authentication, the protocol can be run twice: first with Alice authenticating Bob's QR-PUF, then the other way round. The second time, the classical channel is already authenticated (there is a shared secret $S_{\rm rest}$), which allows for ordinary information reconciliation and privacy amplification without the KMS-MACs. The two protocols may also be run intertwined, i.e. alternating their steps 2a,2b before proceeding to step 3. States may also be sent through both PUFs, but this will probably lead to more particle loss.

The KMS-MAC presented in [6] is secure against a 'linear' class of attacks on the MAC key, i.e. the attacker knows which change he is causing to the key, even though he does know the key itself. In our protocol an attack on the exchanged classical data gives no such knowledge to the attacker, since manipulation of the pointer sets $\mathcal{Z}$, $\mathcal{G}$ does not reveal i_t, j_t. Hence the construction in [6] is in fact overkill for our purposes.

We emphasize again that the authentication is in a sense reversed compared to 'standard' QKE: The quantum channel is authenticated without any use of the classical channel, and the data sent over the non-authenticated classical channel has to be checked for consistency with the exchanged quantum states.

4.4 Security of the authenticated QKE protocol

4.4.1 Intercept-resend attacks on the authentication

An impostor has to overcome several hurdles. The first hurdle is the correct mimicking of the transmission rates while he does not know α and i accurately. This is nontrivial if the rates $\tau_{\alpha i}$ are substantially different. As in Section 3, he chooses an observable B, does a measurement and obtains an outcome b_k. His first choice is whether to return a fake reflected state or not. From his viewpoint (only the knowledge that the challenge state projected onto $|b_k\rangle$) the probability distribution of α and i is

$$\Pr[\alpha, i|B, k] = \frac{\Pr[\alpha, i, B, k]}{\Pr[B, k]} = \frac{\Pr[\alpha, i, B, k]}{\sum_{\alpha,i}\Pr[\alpha, i, B, k]} = \frac{|\langle b_k|\psi_{\alpha i}\rangle|^2}{\sum_{\alpha,i}|\langle b_k|\psi_{\alpha i}\rangle|^2}. \tag{28}$$

It is interesting to note that there actually exists a strategy that allows him to correctly mimic all the transmission rates $\tau_{\alpha i}$. In general his strategy consists of a set of probabilities

$$Q_{Bk} := \Pr[\text{transmit}|B, k]. \tag{29}$$

When Alice sends challenge $|\psi_{\alpha i}\rangle$ he will transmit with probability

$$\Pr[\text{transmit}|\alpha, i] = \mathbb{E}_B \sum_{k\in[n]} |\langle b_k|\psi_{\alpha i}\rangle|^2 Q_{Bk} = \langle\psi_{\alpha i}| \left(\mathbb{E}_B \sum_{k\in[n]} Q_{Bk}|b_k\rangle\langle b_k|\right) |\psi_{\alpha i}\rangle. \tag{30}$$

For all α, i he wants this to be exactly equal to

$$\tau_{\alpha i} = \langle\psi_{\alpha i}|T^\dagger T|\psi_{\alpha i}\rangle = \langle\psi_{\alpha i}| \left(\sum_{k\in[n]} t_k |t_k\rangle\langle t_k|\right) |\psi_{\alpha i}\rangle. \tag{31}$$

Here we use the notation $t_k \in [0,1]$ for the k'th eigenvalue of the Hermitian operator $T^\dagger T$. (Note that the t_k and $|t_k\rangle$ are public knowledge.) Comparing (31) to (30), it is clear that equality is obtained by setting $B = T^\dagger T$ and $Q_{Bk} = t_k$.
If the impostor makes any other choice, then Alice will notice that the transmission rates are wrong. Next we show that a measurement of $T^\dagger T$ does not give him enough information to guess α and i. We first give two useful lemmas, and then prove a bound (Theorem 4) on the per-round success probability.

Lemma 1 *Let $q_0, q_1 \in [0,1]$ be constants. Let $|v_0\rangle$ and $|v_1\rangle$ be two normalized states. Let $\lambda_{\max}$ denote the function that returns the maximum eigenvalue of a matrix. Then it holds that*

$$\lambda_{\max}\left(q_0|v_0\rangle\langle v_0| + q_1|v_1\rangle\langle v_1|\right) = \frac{1}{2}\left(q_0 + q_1 + \sqrt{(q_1-q_0)^2 + 4q_0q_1|\langle v_0|v_1\rangle|^2}\right) \le q_0 + q_1.$$

Proof: We want to find the maximum eigenvalue of the Hermitian matrix $Y = q_0|v_0\rangle\langle v_0| + q_1|v_1\rangle\langle v_1|$. The eigenvalue equation $Y|y\rangle = \lambda|y\rangle$ for a vector of the form $|y\rangle = \cos\varphi|v_0\rangle + e^{i\gamma}\sin\varphi|v_1\rangle$ gives

$$\lambda = q_0\left(1 + \mathrm{tg}\,\varphi\, e^{i\gamma}\langle v_0|v_1\rangle\right) = q_1\left(1 + [\mathrm{tg}\,\varphi]^{-1}e^{-i\gamma}\langle v_1|v_0\rangle\right). \tag{32}$$

The eigenvalues have to be real, hence $e^{i\gamma}\langle v_0|v_1\rangle = \pm|\langle v_0|v_1\rangle|$. Without loss of generality we take the plus sign. (The sign can be absorbed into φ.) The second equality in (32) can be read as a quadratic equation in $\mathrm{tg}\,\varphi$; solving it gives

$$\mathrm{tg}\,\varphi = \frac{q_1 - q_0 \pm \sqrt{(q_1-q_0)^2 + 4q_0q_1|\langle v_0|v_1\rangle|^2}}{2q_0\langle v_0|v_1\rangle}. \tag{33}$$

Substitution of (33), with the plus sign, into the first equality in (32) finishes the proof of the equality in the lemma. The inequality in the lemma follows from the fact that $|\langle v_0|v_1\rangle|^2 \le 1$, which gives $(q_0-q_1)^2 + 4q_0q_1|\langle v_0|v_1\rangle|^2 \le (q_0+q_1)^2$.

□

Lemma 2 *Let $\Delta > 0$ be a constant. Let $|\gamma_0\rangle$ and $|\gamma_1\rangle$ be normalized states with $|\langle\gamma_0|\gamma_1\rangle|^2 = \Delta$. Let $|k\rangle$ be an arbitrary orthonormal basis. Then it holds that*

$$\sum_{k\in[n]} \frac{|\langle k|\gamma_0\rangle|^2 \cdot |\langle k|\gamma_1\rangle|^2}{|\langle k|\gamma_0\rangle|^2 + |\langle k|\gamma_1\rangle|^2} \ge \frac{\Delta}{2}.$$

Proof sketch: There are two extreme cases, (A) the overlap between $|\gamma_0\rangle$ and $|\gamma_1\rangle$ is spread out over all directions $|k\rangle$, and (B) it is peaked in a plane, say the plane spanned by $|1\rangle$ and $|2\rangle$. In case A we write without loss of generality $|\gamma_0\rangle = n^{-1/2}\sum_k |k\rangle$ and $|\gamma_1\rangle = n^{-1/2}\sum_k e^{i\alpha_k}|k\rangle$, where the angles α_k satisfy $n^{-1}|\sum_k e^{i\alpha_k}| = \sqrt{\Delta}$. The sum in the lemma evaluates to $\sum_k \frac{(1/n)(1/n)}{1/n+1/n} = 1/2$. In case B we write, without loss of generality, $|\gamma_0\rangle = \cos\varphi|1\rangle + \sin\varphi|2\rangle$ and $|\gamma_1\rangle = \sin\varphi|1\rangle + \cos\varphi|2\rangle$, with $\sin 2\varphi = \sqrt{\Delta}$. The sum evaluates to $2\frac{\sin^2\varphi\cdot\cos^2\varphi}{\cos^2\varphi+\sin^2\varphi} = \frac{1}{2}\sin^2 2\varphi = \Delta/2$. The smallest of the extreme cases is $\Delta/2$. □

Theorem 4 *Let the impostor use $B = T^\dagger T$, $Q_{Bk} = t_k$ as his strategy for the intercept-resend attack. Then his per-round probability of success for the authentication, whenever he decides to send a state to Alice, is bounded by*

$$p \le \frac{1}{2} + \frac{1}{4n}\sum_i\sum_k \sqrt{(|\langle t_k|\psi_{1i}\rangle|^2 - |\langle t_k|\psi_{0i}\rangle|^2)^2 + 4|\langle t_k|\psi_{1i}\rangle|^2 \cdot |\langle t_k|\psi_{0i}\rangle|^2 \cdot |\langle\omega_{0i}|\omega_{1i}\rangle|^2}. \tag{34}$$

Corollary 1 *Let $a, \Delta > 0$ be constants. Let the scattering matrix be such that for all i:*

$$|\langle\psi_{0i}|\psi_{1i}\rangle|^2 \geq \Delta \quad \text{and} \quad |\langle\omega_{0i}|\omega_{1i}\rangle|^2 < 1 - a. \tag{35}$$

Then Theorem 4 implies that

$$p < 1 - \frac{a\Delta}{4}.$$

Proof of Theorem 4: We express the impostor's per-round probability of success for his fake reflected states $|\omega\rangle$ as

$$p = \mathbb{E}_\alpha \mathbb{E}_i \sum_{k\in[n]} |\langle t_k|\psi_{\alpha i}\rangle|^2 \sum_\omega \mathcal{A}[\omega|k]\ |\langle\omega_{\alpha i}|\omega\rangle|^2. \tag{36}$$

Here $\mathcal{A}[\omega|k]$ is his strategy: the probability of sending ω given k. The $|\omega_{\alpha i}\rangle$ is the correct return state as defined in (26). By re-arranging the sums we can write

$$\begin{aligned} p &= \frac{1}{2n}\sum_k\sum_\omega \mathcal{A}[\omega|k]\ \langle\omega| \left(\sum_i\sum_\alpha |\langle t_k|\psi_{\alpha i}\rangle|^2 |\omega_{\alpha i}\rangle\langle\omega_{\alpha i}|\right) |\omega\rangle & (37)\\ &\leq \frac{1}{2n}\sum_k \lambda_{\max}\left(\sum_i\sum_\alpha |\langle t_k|\psi_{\alpha i}\rangle|^2 |\omega_{\alpha i}\rangle\langle\omega_{\alpha i}|\right) & (38)\\ &\leq \frac{1}{2n}\sum_i\sum_k \lambda_{\max}\left(\sum_\alpha |\langle t_k|\psi_{\alpha i}\rangle|^2 |\omega_{\alpha i}\rangle\langle\omega_{\alpha i}|\right) & (39)\end{aligned}$$

where $\lambda_{\max}(\cdot)$ denotes the maximum eigenvalue of a matrix. In the last line we have used the convexity of the maximum-eigenvalue function. Finally we apply Lemma 1 (the equality part) with $q_\alpha = |\langle t_k|\psi_{\alpha i}\rangle|^2$ and $|v_\alpha\rangle = |\omega_{\alpha i}\rangle$, and then use $\sum_k |\langle t_k|\cdots\rangle|^2 = 1$. □

Proof of Corollary 1: Substituting $|\langle\omega_{0i}|\omega_{1i}\rangle|^2 < 1 - a$ into (34) and again using the shorthand notation $q_\alpha = |\langle t_k|\psi_{\alpha i}\rangle|^2$, we have

$$\begin{aligned} p &< \frac{1}{2} + \frac{1}{4n}\sum_i\sum_k \sqrt{(q_0+q_1)^2 - 4aq_0q_1} & \\ &= \frac{1}{2} + \frac{1}{4n}\sum_i\sum_k (q_0+q_1)\sqrt{1 - 4a\frac{q_0q_1}{(q_0+q_1)^2}} & (40)\\ &\leq \frac{1}{2} + \frac{1}{4n}\sum_i\sum_k (q_0+q_1)\left[1 - 2a\frac{q_0q_1}{(q_0+q_1)^2}\right] & (41)\\ &= 1 - \frac{a}{2n}\sum_i\sum_k \frac{q_0q_1}{q_0+q_1} & (42)\\ &\leq 1 - \frac{a}{2n}\sum_i \frac{\Delta}{2} = 1 - \frac{a\Delta}{4}. & (43)\end{aligned}$$

In (41) we used $\sqrt{1-x} \leq 1 - \frac{1}{2}x$. In (43) we applied Lemma 2 using the $|t_k\rangle$ basis and $|\gamma_\alpha\rangle = |\psi_{\alpha i}\rangle$. □

In summary, the impostor has no choice but to do a measurement that is essentially equal to $T^\dagger T$; otherwise Alice will notice that the reflection rates are wrong. But the knowledge obtained from measuring $T^\dagger T$ is not sufficient to learn enough about the challenge state $|\psi_{\alpha i}\rangle$, and the result is a success rate p that noticeably differs from 100%.

In principle (34) allows p to come close to 1. However, for that situation to occur the scattering matrix must be quite pathological. The eigenvectors of X_1 are maximally removed from those of X_0. Something special has to happen in order to have $|\omega_{0i}\rangle \propto RT^{-1}|x_{0i}\rangle$ align with $|\omega_{1i}\rangle \propto RT^{-1}|x_{1i}\rangle$ for some i, let alone for *all* i. A randomly created PUF is extremely unlikely to behave like that; and it can be discarded if it is ever created at all.

Note that the bound in Corollary 1 is not tight. Hence in practice the success probability is even lower.

4.4.2 Quantum computer attack on the authentication

Again, the authentication is vulnerable to an attack by Quantum Computer (QC). The attack is an extension of the one in Section 3.3.2. It needs [i] fast quantum teleportation, [ii] fast quantum computation and [iii] fast measurement of the state of the QC. The third requirement is new.
The QC's memory consists of two parts: Mem1 for the transmission and Mem2 for the reflection degrees of freedom. The challenge state $|\psi_{\alpha i}\rangle$ is moved into Mem1 by teleportation. Mem2 is initialized to zero. Then a unitary operation is applied that is equivalent to scattering by the QR-PUF, i.e. an operation is done equivalent to applying the scattering matrix S to $\begin{pmatrix} |\psi_{\alpha i}\rangle \\ 0 \end{pmatrix}$. The result is a superposition $T|\psi_{\alpha i}\rangle \otimes 0 + 0 \otimes R|\psi_{\alpha i}\rangle$. (The tensor product refers to Mem1 and Mem2.) Then a measurement is done that only detects 'in which memory the particle is'. If the outcome is '2', then the state of the QC is $0 \otimes R|\psi_{\alpha i}\rangle$; The state of Mem2 is teleported onto a response state and sent to Alice. If the outcome is '1', then the state in Mem1 is used for QKE (either by applying an equivalent of X_0 or X_1 directly in the QC, or by teleporting the state of Mem1 out and then measuring $X_{0/1}$).
This attack correctly reproduces all reflection rates, reflected states and transmitted states. It allows an impostor to pass authentication without possessing Bob's QR-PUF and to generate a shared secret key with Alice.
However, the attack requires two fast teleportations, a powerful QC and a fast QC state measurement, which together will present a serious technological hurdle for quite some time to come.

4.4.3 Security of the key

If there is no 'quantum' attack and if Bob's QR-PUF is successfully authenticated, then form Alice's point of view the key is secure. The argument is straightforward. The authentication can be spoofed only by a quantum attack. Given that there is no quantum attack, successful authentication implies that Bob really controls the QR-PUF. Hence Alice is truly generating a key with Bob. With impostors having been excluded, we only have to worry about eavesdropping. The transmitted states travel through the QR-PUF in a 'transparent' way,[6] i.e. Alice's T^{-1} in the challenge states $T^{-1}|x_{\alpha i}\rangle$ undoes the effect of transmission through the QR-PUF, and effectively she sends eigenstates of X_0 or X_1 to Bob. Thus, the protocol rounds in which transmission occurs are completely equivalent to an ordinary QKE scheme, and all the standard security proofs for QKE apply.

4.4.4 Security trade-offs for authenticated QKE

Below we list the security properties of three authentication methods for QKE. We find it interesting that the QR-PUF authentication achieves an unusual type of trade-off: it has no need for the a priori sharing of a secret, but the security depends on physical assumptions.

Auth. method	**Security assumption**	**Remarks**
MAC	unconditional	needs a priori shared secret
entangled state	unconditional	needs a priori shared secret state; unpractical because of decoherence.
QR-PUF	physical unclonability; no quantum emulation	needs trusted enrollment data (allowed to be public)

5 Summary and future work

We have introduced a new security primitive, the Quantum Readout PUF (QR-PUF), which is a classical PUF that can be read out using quantum states. We have shown how QR-PUFs can be used to achieve remote authentication without a trusted remote reader device. The security is

[6] The presence of the QR-PUF may introduce some additional noise. It is well known how to deal with noise.

based on two well known physical assumptions, physical unclonability and uniqueness, and one new physical assumption, quantum-computational unclonability. The no-cloning theorem guarantees that intercept-resend attacks will be detected. Our authentication scheme is vulnerable to a three-step attack employing quantum teleportation and a quantum computer. For this reason we need the assumption of quantum-computational unclonability, which states that this kind of attack, while possible in theory, is infeasible in practice because of technical or financial issues. What makes a 'quantum' attack especially difficult is the fact that our protocol doubles as a distance bounding scheme; all three steps of the attack have to be extremely fast.

We have sketched how QR-PUF authentication can be intertwined with Quantum Key Exchange. Reflected states are used for authentication, transmitted states for QKE. This combination achieves authenticated QKE without the need for an initial shared secret (such as a short MAC key or an entangled state). The sketched protocol has the unusual property that the quantum channel is authenticated, allowing for an un-authenticated classical channel. This reversal necessitates the use of KMS-MACs.

In our schemes Alice waits for a returning state before sending her next challenge state; this simplifies the security proofs considerably, since in this setting it suffices to look at the security of an isolated round without having to worry about (entanglement) attacks on multiple challenge states. We leave more general protocols and their security proof as a subject for future work.

We have not discussed the issue of implementation. The biggest question is how to construct a QR-PUF in the first place. The most practical option seems to be a partially transmissive optical PUF that is challengeable by single photon states or coherent states through an optical fiber. The main difficulty is to make sure that the uniqueness and physical unclonability properties hold, in spite of the limited number of challenges that can be passed through a fiber. Fibers carry a limited number of transversal modes, while such modes are the main way of challenging an ordinary speckle-producing optical PUF [20, 21]. We are perhaps aided by the fact that multiple wavelengths are available as a challenge.

Another question is how to quantify the difficulty of the 'quantum' attack (Section 3.3.2), which is the most serious threat to QR-PUFs. Here too the availability of different wavelengths seems to help us, since it increases the required size of the quantum computer.

Our protocols can be extended in a number of obvious ways. For instance, EPR pairs can be used, as well as anti-eavesdropping countermeasures like 'decoy states' [14]. The QR-PUF can be used for Quantum Oblivious Transfer. Another option is transmitting states through more than one QR-PUF. It would also be interesting to see if one can construct a 'quantum PUF', i.e. a PUF that has actual quantum behaviour, resulting in nontrivial (even nonlinear) interaction between the challenge state and the PUF.

Acknowledgements

We kindly thank Pim Tuyls, Berry Schoenmakers, Allard Mosk and Andrea Fiore for useful discussions. We thank the anonymous reviewers for pointing out the unfinished state of a previous version.

References

[1] C.H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179, 1984.

[2] C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W.K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Phys. Rev. Lett.*, 70:1895–1899, 1993.

[3] J.D.R. Buchanan, R.P. Cowburn, A. Jausovec, D. Petit, P. Seem, G. Xiong, D. Atkinson, K. Fenton, D.A. Allwood, and M.T. Bryan. Forgery: 'fingerprinting' documents and packaging. *Nature, Brief Communications*, 436:475, July 2005.

[4] J.L. Carter and M.N. Wegman. Universal classes of hash functions. *Journal of Computer and System Sciences*, 18(2):143–154, 1979.

[5] C.N. Chong, D. Jiang, J. Zhang, and L. Guo. Anti-counterfeiting with a random pattern. In *SECURWARE*, pages 146–153. IEEE, 2008.

[6] R. Cramer, Y. Dodis, S. Fehr, C. Padró, and D. Wichs. Detection of algebraic manipulation with applications to robust secret sharing and fuzzy extractors. In N.P. Smart, editor, *EUROCRYPT*, volume 4965 of *Lecture Notes in Computer Science*, pages 471–488. Springer, 2008.

[7] G. DeJean and D. Kirovski. Radio frequency certificates of authenticity. In *IEEE Antenna and Propagation Symposium – URSI*, 2006.

[8] D. Dieks. *Phys. Lett. A*, 92:271, 1982.

[9] L.M. Duan, M. Lukin, J.I. Cirac, and P. Zoller. Long-distance quantum communication with atomic ensembles and linear optics. *Nature*, 414:413–418, 2001.

[10] A.K. Ekert. Quantum cryptography based on Bells theorem. *Phys. Rev. Lett.*, 67:661 – 663, 1991.

[11] B. Gassend, D.E. Clarke, M. van Dijk, and S. Devadas. Silicon physical unknown functions. In V. Atluri, editor, *ACM Conference on Computer and Communications Security — CCS 2002*, pages 148–160. ACM, November 2002.

[12] D. Gottesman and J. Preskill. Secure quantum key exchange using squeezed states, 2000. arXiv:quant-ph/0008046v2.

[13] J. Guajardo, S.S. Kumar, G.J. Schrijen, and P. Tuyls. FPGA intrinsic PUFs and their use for IP protection. In P. Paillier and I. Verbauwhede, editors, *CHES*, volume 4727 of *LNCS*, pages 63–80. Springer, 2007.

[14] W.-Y. Hwang. Quantum key distribution with high loss: Toward global secure communication. *Phys.Rev.Lett.*, 91:057901, 2003.

[15] K. Inoue, E. Waks, and Y. Yamamoto. Differential phase shift quantum key distribution. *Phys. Rev. Lett.*, 89:037902, 2002.

[16] D. Kirovski. Toward an automated verification of certificates of authenticity. In J.S. Breese, J. Feigenbaum, and M.I. Seltzer, editors, *ACM Conference on Electronic Commerce*, pages 160–169. ACM, 2004.

[17] S.S. Kumar, J. Guajardo, R. Maes, G.J. Schrijen, and P. Tuyls. The Butterfly PUF: Protecting IP on every FPGA. In M. Tehranipoor and J. Plusquellic, editors, *HOST*, pages 67–70. IEEE Computer Society, 2008.

[18] K. Kursawe, A.-R. Sadeghi, D. Schellekens, B. Škorić, and P. Tuyls. Reconfigurable physical unclonable functions. In *HOST*, 2009.

[19] D.N. Matsukevich and A. Kuzmich. Quantum state transfer between matter and light. *Science*, 306(5696):663–666, 2004.

[20] R. Pappu. *Physical One-Way Functions.* PhD thesis, MIT, 2001.

[21] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld. Physical One-Way Functions. *Science*, 297:2026–2030, Sept. 2002.

[22] B.S. Shi, J. Li, J.M. Liu, X.F. Fan, and G.C. Guo. Quantum key distribution and quantum authentication based on entangled state. *Phys.Lett.A*, 281:83–87, 2001.

[23] D.R. Stinson. Universal hashing and authentication codes. *Designs, Codes, and Cryptography*, 4:369–380, 1994.

[24] P. Tuyls, G.J. Schrijen, B. Škorić, J. van Geloven, R. Verhaegh, and R. Wolters. Read-proof hardware from protective coatings. In L. Goubin and M. Matsui, editors, *Cryptographic Hardware and Embedded Systems — CHES 2006*, volume 4249 of *LNCS*, pages 369–383. Springer-Verlag, 2006.

[25] P. Tuyls, B. Škorić, and T. Kevenaar. *Security with Noisy Data: Private Biometrics, Secure Key Storage and Anti-Counterfeiting.* Springer, London, 2007.

[26] P. Tuyls, B. Škorić, S. Stallinga, A.H.M. Akkermans, and W. Ophey. Information-theoretic security analysis of physical uncloneable functions. In A.S. Patrick and M. Yung, editors, *9th Conf. on Financial Cryptography and Data Security*, volume 3570 of *LNCS*, pages 141–155. Springer, 2005.

[27] B. Škorić. On the entropy of keys derived from laser speckle; statistical properties of Gabor-transformed speckle. *Journal of Optics A: Pure and Applied Optics*, 10(5):055304–055316, 2008.

[28] B. Škorić, T. Bel, A.H.M. Blom, B.R. de Jong, H. Kretschman, and A.J.M. Nellissen. Randomized resonators as uniquely identifiable anti-counterfeiting tags. *Secure Component and System Identification Workshop*, Berlin, March 2008.

[29] W.K. Wootters and W.H. Zurek. A single quantum cannot be cloned. *Nature*, 299:802–803, 1982.