Secure authentication via Quantum Physical Unclonable Functions: a review

Pol Julià Farré[1]*∗*, *Vladlen Galetsky*[2], *Mohamed Belhassen*[3], *Gregor Pieplow*[3], *Kumar Nilesh*[2], *Holger Boche*[2], *Tim Schröder*[3,4], *Janis Nötzel*[2] *& Christian Deppe*[1]

[1]Institute of Communications Engineering, Technische Universität Braunschweig, Braunschweig, Germany
[2]Chair of Theoretical Information Technology, Technical University of Munich, Munich, Germany
[3]Department of Physics, Humboldt-Universität zu Berlin, Berlin, Germany
[4]Ferdinand-Braun-Institut, Berlin, Germany
∗Corresponding author

Email: [1]pol.julia-farre@tu-braunschweig.de, [2]vladlen.galetsky@tum.de, [3]mohamed.belhassen@physik.hu-berlin.de, [3]pieplow@physik.hu-berlin.de, [2]kumar.nilesh@tum.de, [2]boche@tum.de, [4]tim.schroeder@physik.hu-berlin.de, [2]janis.noetzel@tum.de, [1]christian.deppe@tu-braunschweig.de

Keywords: *Survey on QPUFs, QPUF, Authentication, Quantum memories*

Quantum Physical Unclonable Functions (QPUFs) offer a physically grounded approach to secure authentication, extending the capabilities of classical PUFs. This review covers their theoretical foundations and key implementation challenges—such as quantum memories and Haar-randomness—, and distinguishes QPUFs from Quantum Readout PUFs (QR-PUFs), more experimentally accessible yet less robust against quantum-capable adversaries. A co-citation-based selection method is employed to trace the evolution of QPUF architectures, from early QR-PUFs to more recent Hybrid PUFs (HPUFs). This method further supports a discussion on the role of information-theoretic analysis in mitigating inconsistencies in QPUF responses, underscoring the deep connection between secret-key generation and authentication. Despite notable advances, achieving practical and robust QPUF-based authentication remains an open challenge.

1 Introduction

Physical Unclonable Functions (PUFs) are devices characterized by their inherent unclonability and their ability to produce responses that are unpredictable yet consistently reproducible for given inputs. Originally introduced in the classical context [1], PUFs have since found a wide range of applications. These include secret-key generation [2–4], secure storage of cryptographic data [5, 6], and protocols such as oblivious transfer and bit commitment [7, 8]. Central to this article, PUFs are employed in secure authentication schemes [9–11]. In the recent years, a high number of different PUF models have been found to be vulnerable against machine-learning-based attacks [12–16]. As pointed out in [17], this context has motivated to bring the study of PUFs to the quantum realm, giving rise to a still young field of research with the hope and expectation of finding mathematical and robust security guarantees.

Analogous to the classical case, token-based authentication schemes can be designed relying on Quantum PUFs (QPUFs) by exploiting the fingerprint set by the unpredictable outputs (responses) of the considered QPUF when being queried with new, i.e., unqueried, inputs (challenges). However, and distinctly, QPUFs, as formally defined in [18], accept quantum states as challenges, as well as they produce quantum states as responses. The first documented attempt of deriving what one might, at a glance, call a QPUF is found in [19]. Building on this work, [20] also proposes a PUF-based scheme involving quantum systems. We intentionally avoid calling the mentioned proposals QPUFs because, as it will become evident in Section 2, these fail to fall into the definition of a QPUF presented in [18]. A more adequate and accepted label for the schemes proposed in the aforementioned cited works is Quantum Readout PUF (QR-PUF). As we discuss in Section 4, these enjoy a reasonable sense of practicality, as opposed to QPUFs, but require additional ad-hoc assumptions and do not seem to take full advantage of the *quantumness*. That is, essentially, and as already pointed out in [21] for the specific work in [20], the

quantum challenges and responses possible for QR-PUFs are typically mappable to classical information known by the certifier who, as opposed to that of QPUFs, becomes a trusted party.
The work in [18] suggests that QPUFs must be unitary or negligibly non-unitary quantum transformations, and requires the analogous of uniform randomness referred to unitary operators: Haar randomness (we refer readers unfamiliar with this concept to the text book [22] and the tutorials found in [23, 24]). Interestingly, the subsequent work [25] circumvents the requirement of such a costly resource for the challenge selection, while it remains needed, inconveniently, for the QPUF generation. Intimately related to that, the authors in [26] derive two different QPUF models: the Measurement-Based QPUF (MB-QPUF) and the Ideal QPUF, constituting other solutions to circumvent the cost of requiring Haar randomness for challenge selection.
This article aims to provide the reader with a review on QPUFs, going in detail over all the aforementioned aspects within the complex development and evolution of an itself complex field of investigation. In Section 2.1 we revisit the theoretical framework introduced in [18], and we comment on some immediate implications of it when accepting certain assumptions commonly made for PUFs. In Section 2.2, we deliver a discussion on the current incompatibility between requirements and experimental possibilities for QPUF-based tokens, as well as the corresponding near-term perspectives. Later, in Section 3, we present and justify the article selection criteria used in this review, focusing on the most theoretically relevant QPUF proposals. In Section 4, we present our analysis of several articles, providing an underlying historical overview of QPUFs—illustrated as a QPUF timeline—, and a detailed discussion on information-theoretic approaches used for the study and characterization of QPUFs. Finally, Section 5 concludes the article.

2 Theoretical and practical frameworks

In this preliminary section, we present the key theoretical definitions and assumptions underlying the field of QPUFs, and discuss their connections to existing literature. Additionally, we examine the technical implications of this framework to clarify the practical requirements for making QPUFs operational.

2.1 Definitions and common assumptions

We begin by presenting the definition of a QPUF, originally introduced in [18]. It is important to note that this and the subsequent definitions have not been reproduced in an unaltered form. While our aim is not to change the meaning of the established concepts, we present slightly revised formulations that seek to enhance clarity and remain consistent with the original formalism.

Definition 1. $(\{\lambda_i\}, \delta_r, \delta_u, \delta_c)$*-QPUF:*
Quantum channel $\Lambda^{\delta_r,\delta_u,\delta_c}_{\{\lambda_i\}\text{-QPUF}}$*, with* $\delta_r, \delta_u, \delta_c \in [0,1]$*, and with a set of security parameters* $\{\lambda_i \mid \lambda_i \in \mathbb{R}, \forall i\}$ *that serve to adjust the desired level of security within its associated authentication protocol. The channel* $\Lambda^{\delta_r,\delta_u,\delta_c}_{\{\lambda_i\}\text{-QPUF}}$ *must fulfill the following with an overwhelming probability:*

1. δ_u*-uniqueness, ensuring that a sampled channel* $\Lambda^{\delta_r,\delta_u,\delta_c}_{\{\lambda_i\}\text{-QPUF}}$ *is* δ_u*-distinguishable (in the diamond norm [27, 28]) from any other sampled instance.*

2. δ_r*-robustness, ensuring that* $\Lambda^{\delta_r,\delta_u,\delta_c}_{\{\lambda_i\}\text{-QPUF}}$ *maps* δ_r*-indistinguishable (in fidelity [29]) challenges to* δ_r*-indistinguishable responses.*

3. δ_c*-collision resistance, ensuring that* $\Lambda^{\delta_r,\delta_u,\delta_c}_{\{\lambda_i\}\text{-QPUF}}$ *maps* δ_c*-distinguishable (in fidelity) challenges to* δ_c*-distinguishable responses.*

Remark 1. *On the almost-unitaricity requirement and the sampling problem:*
In [18] (its Theorem 3) it is shown how the two last displayed requirements necessarily imply that $\Lambda^{\delta_r,\delta_u,\delta_c}_{\{\lambda_i\}\text{-QPUF}}$ *must be a unitary or a negligibly, with respect to certain security parameters, non-unitary channel. In*

parallel, the uniqueness requirement mandates the existence of a quantum-channel sampling procedure available to the verifier party, and establishing a proper fingerprint.

Having formally defined a QPUF, we now proceed to outline the different schemes used in the literature to leverage the QPUF potential for authentication. These schemes, ultimately aiming to achieve both the completeness and soundness properties as defined in [17], so far include (see Table 1):

1. The prover holds the QPUF and, in the verification phase, is asked to produce the response to a certain number of challenges (QPUF models in [18,30,31] or MB-QPUF in [26]).
2. The prover stores a response and is asked to provide it in the verification phase (Ideal QPUF in [26]).

Table 1: Comparison of the features owned by the two main types of QPUF-based authentication schemes.

Protocol class	Verifier	Prover	Verification type
1. QPUF as a token	Stores a set of responses	Holds the QPUF (token)	Multiple-shot verification
2. Response as a token	Holds the QPUF	Stores a response (token)	1-shot verification

In this context, the two following assumptions, inherited from the framework of classical PUFs, are typically present.

Assumption 1. *Unclonability:*
The manufacturing process yielding $\Lambda^{\delta_r,\delta_u,\delta_c}_{\{\lambda_i\}\text{-QPUF}}$ *is assumed to be uncontrollable, which prevents any adversary from efficiently replicating it. Furthermore, the underlying physical structure of* $\Lambda^{\delta_r,\delta_u,\delta_c}_{\{\lambda_i\}\text{-QPUF}}$ *is too complex to construct a clone of it.*

Assumption 2. *Query-based adversarial model:*
It is assumed that adversaries can interact with the QPUF solely by querying it, i.e., by obtaining valid challenge-response pairs. The number of queries allowed is typically stated as a function of certain security parameters.

Referring to the mentioned query-based adversarial model, the work [18] defines three notions of unforgeability types for QPUF-based authentication protocols.

Definition 2. *Quantum exponential unforgeability:*
Property owned by those QPUF-based authentication protocols that, under any non-previously queried challenge selection, remain unforgeable by any exponential adversary, i.e., any adversary with a number of allowed queries to the QPUF equal to an exponential function of certain security parameters.

Definition 3. *Quantum existential unforgeability:*
Property owned by those QPUF-based authentication protocols that, under any non-previously queried challenge selection, remain unforgeable by any polynomial adversary.

Definition 4. *Quantum selective/universal unforgeability:*
Property owned by those QPUF-based authentication protocols that, under a constrained non-previously queried challenge selection, remain unforgeable by any polynomial adversary.

Remark 2. *On the QPUF dimension and the non-inclusivity of Definition 1:*
As already pointed out in [18], we notice how the assumption made on QPUF unclonability could be violated via process tomography [32] within the, also assumed, query-based adversary model. In this context, exponential unforgeability is unattainable. However, an appropriate choice of security parameters, e.g. the number of qubits targeted by the QPUF channel and the number of responses requested during verification, can potentially lead to achieving the other two notions of unforgeability, which are more realistic and typically sufficient. Importantly, as we discuss in detail in Section 4, we thus notice how Definition 1 denies the quality of being a QPUF for the QR-PUF models [19, 20, 33–35], which target systems of fixed size thus leading to learnable quantum channels unless further assumptions are considered.

Remark 3. *On the Haar-randomness problem:*
As stated in Remark 1, a quantum-channel sampling procedure must be available at the verifier side and, informally, it should not allow for having two too similar instances among different runs of the QPUF-generation scheme. Now, additionally, the unclonability assumption implicitly requires such sampling procedure to be non-reproducible. The security proof (Theorem 6 in [18]) for the weakest form of QPUF unforgeability, i.e., the selective one, motivates the cited authors to model such sampling procedure as being Haar random. That is, Haar randomness paves the way towards having robust security guarantees. Nonetheless, to the best of our knowledge, there is currently no efficient method for mimicking such mathematical construction in real setups. Specifically, one can see how the two prescriptions for Haar-randomly sampling unitary operators given in [24] introduce an exponential overhead in the number of targeted qubits.

Remark 4. *On the role of the No-cloning theorem:*
Analogous to its classical counterpart, a QPUF is not fundamentally unclonable via brute-force physical inspection. In this regard, the two assumptions stated in the current section become a source exploited in security proofs and rely on a proper QPUF engineering, which we do not discuss in this article, primarily focused on theoretic aspects. However, the No-cloning theorem for unknown quantum states [36] does provide QPUFs with desirable properties not conceivable in the classical setting. Namely, within the swap-test-based [37] verification stage found in [18], the No-cloning theorem eliminates the need for a third trusted party, present in all classical-PUF-based authentication protocols.

2.2 QPUF requirements and today's possibilities

As introduced in Section 2.1, a prover in a QPUF-based authentication scheme holds a QPUF or a set of quantum states that serve as responses. Such token-based authentication can be especially useful in quantum networks, where only a subset of links is authenticated [38]. When a token is delivered once over an authenticated link, the token's holder can subsequently verify their identity on unauthenticated links by sending back quantum states or the QPUF.

If the tokens consist of quantum states, the distribution of these states must meet certain criteria, and the quantum memories used for storage must satisfy their own requirements. First, each state must be encodable in quantum carriers capable of transmitting information. Photons are the most common choice [39,40], as they can propagate through the existing fiber-optic infrastructure. To store the photonic state, a light–to-storage interface must exist.

In the absence of a one-time-authenticated channel within a network, an in-person enrollment phase is required, and quantum state storage must be portable. However, long-lived quantum memories capable of interfacing with unitary quantum operations and storing highly entangled token states [41, 42] have not yet been realized. Currently, the only viable candidates for storing simple, unentangled states are noble-gas memories, which exhibit coherence times ranging from 4 to 100 hours [43, 44], but these still lack a functional interface with flying qubits.

In the more common scenario, the prover holds the QPUF for authentication rather than storing quantum states. Quantum memories, along with interfaces between these memories and the system, are still required to store the responses. The physical implementation of random unitaries remains an active research area [45, 46]. Research focused on designing or analyzing methods to generate specific types of randomness in quantum systems is sometimes discussed within the framework of unitary designs [47]. For example, Nakata et al. [48] conjecture that a physically natural unitary design could utilize geometrically local, time-independent interactions, and propose a physical realization based on cavity Quantum Electrodynamics (QED). If the assumption of time independence is relaxed, a cavity-fed system employing random pairwise interactions on individually emitted photons could also implement a natural-design Hamiltonian [49, 50].

Several platforms can host such devices and distribute their states across quantum networks, provided that interactions between photons and stationary quantum systems are controllable. Candidate platforms include atoms [49, 50], quantum dots [51], ions [52], and color centers [53]. Purely photonic imple-

mentations have also been proposed [45, 54].
Any QPUF platform that does require cryogenic cooling, i.e., all of the above, except for photonic implementations, will for the time being not be portable, and may only be available at fixed nodes in a network.
Next, we provide a brief non-exhaustive overview on quantum memories and the current state of the art in photonic state storage in network applications. A more in-depth overview can be found, for example, in [55].

Working principles of quantum memories

This section focuses on two prevalent methods for storing quantum information via light-matter interfaces: atomic ensemble-based schemes and those that directly transduce photonic qubits into long-lived degrees of freedom within single atom-like systems. Atomic ensemble memories typically utilize three-level atomic systems in a Λ-configuration, allowing for the coherent transfer of quantum states between photons and collective atomic spin excitations. This is achieved through mechanisms such as Electromagnetically Induced Transparency (EIT) or Raman absorption processes [56, 57]. In such setups, an incoming photonic qubit is coherently mapped onto the atomic coherence between the ground state ($|g\rangle$) and a storage state ($|s\rangle$) via interaction with a classical laser field and resonant photon absorption. The stored information is later retrieved through a coherent readout process, again driven by a control laser field [58].
Quantum memories that directly transduce photonic qubits into single atom-like systems similarly utilize a Λ-configuration of a long-lived two-level spin system, coupled via an intermediate optically excited state. Photonic qubits can be encoded in various degrees of freedom, such as time-bin [59], frequency-bin [60], or polarization states [61], and their quantum information is mapped onto long-lived spin states through coherent photon-spin interactions [39].

Quantum memory platforms

A wide variety of quantum-memory platforms exists, each platform with its own strengths and limitations. While we do not aim to provide an exhaustive review, we offer a concise overview of the current state of the art across key platforms (see Table 2).

1. **Atomic ensembles:** Ensembles of cold or warm atoms can be employed for the storage of photonic qubits. A comprehensive overview of the current state of ensemble-based quantum memories can be found in [57] and [55]. These atomic ensembles differ primarily in their operating temperatures and coherence properties. Warm atom systems function at room temperature, eliminating the need for intricate laser cooling setups. In contrast, cold atom memories offer longer coherence times, attributed to reduced atomic collisions and narrower spectral lines.

2. **Trapped Atoms:** Hyperfine states of atoms serve as reliable qubit candidates [62] [63]. A key advantage of trapped atoms is their strong isolation from the environment, which significantly minimizes decoherence. Various trapping techniques are employed depending on the type of atom: ions are typically confined using oscillating radio-frequency electric fields, while neutral atoms are held using optical tweezers.

3. **Color centers:** In materials like diamond, defects in the crystal lattice, such as vacancies or the presence of foreign atoms, can give rise to color centers. These defects form energy-level structures that are optically addressable and suitable for qubit implementation. Unlike trapped atoms, color centers are inherently confined within the solid-state lattice, eliminating the need for external trapping mechanisms. This simplifies the system design and allows for the integration of nanostructures around the qubit. However, the solid-state environment introduces decoherence, primarily due to interactions with other lattice defects and background noise.

Table 2: This table presents the state-of-the-art performance metrics for each platform. The values shown are the best reported figures and may not be directly comparable as they are not necessarily achieved under the same conditions. Superscripts denote: $*$ — T_2^* coherence time measured via Ramsey interferometry, $\dagger$ — T_2 coherence time measured via Hahn echo or dynamical decoupling. Abbreviations: RT — Room Temperature, TW — Telecom Wavelength, NA - Not available.

Platform	Storage time	Operating temperature	Wavelength	Efficiency	Bandwidth
Warm Atomic Ensemble	1.1 μs^* [65]	RT [65]	780 nm [65]	82% [65]	170 MHz [65]
Cold atom	4.7 ms [66]	100 μK [67]	780 nm [67]	87% [67]	29 Hz [66]
Trapped ions	1 hour* [68]	RT [68]	369.5 nm [68]	98.6% [68]	NA
Trapped neutral atoms	40 s† [69]	1 μK [70]	852 nm [71]	84% [72]	10 kHz [71]
Rare-Earth Ensemble	1 hour† [64]	1.7 K [64]	580 nm [64]	69% [73]	10 kHz [64]
Color Center	40 ms† [74]	RT [74]	619 nm [75]	42.3% [76]	NA
Fiber Loops	52 μs [77]	RT [77]	TW [77]	54% [78]	78 kHz [77]

4. **Rare-Earth Ensemble:** In these systems, the electron spin serves as the qubit. A key advantage is that the electron resides in the atom's inner shell [57], providing enhanced shielding from environmental disturbances and thus improving coherence, which can be further extended up to one hour by incorporating the state-of the-art atomic frequency-comb technique [64]. However, this shielding also poses a challenge, as it makes the electron more difficult to manipulate, resulting in slower gate operations and more complex control requirements.

5. **Fiber loops:** This approach represents a fundamentally different type of quantum memory, where the photon is stored by circulating it through a long optical fiber loop. The primary advantage is its simplicity, no quantum operations or auxiliary quantum systems are required to store the information. However, this method has notable limitations: photon loss accumulates over time as the photon travels through the fiber, and retrieval is not on-demand but strictly determined by the fixed length of the loop.

Quantum Error Correction

Quantum error correction (QEC) [79, 80] was developed to make inherently noisy quantum hardware fault-tolerant, enabling reliable quantum computation. The same principles can be extended to quantum memories to protect stored quantum information. Here, we provide a brief overview on key concepts of active QEC as applied to quantum memories, and highlight recent developments in the field. For a more detailed treatment, refer to [81, 82].

A common approach in active QEC combines multiple physical qubits (e.g., superconducting [83, 84], spin [85], or photonic qubits [86]) into a single logical qubit, typically within the stabilizer-code framework [81]. Below, we provide a brief overview on state-of-the-art implementations of active QEC in quantum memories.

State of the art: Google recently demonstrated a significant experimental milestone by implementing a distance-7 quantum error-correcting code using 101 qubits, achieving break-even error correction by doubling memory lifetime to 291 ± 6 μs compared to the longest-lived physical qubit used in the experiment [84]. In related experimental advances, the Tesseract code demonstrated distance-four encoding using just 16 physical qubits, successfully performing up to five rounds of error correction [87], while Debry *et al.* encoded an error-corrected qubit in a single ion, achieving a coherence time extension factor of 1.5 [88]. Complementing these experiments, recent theoretical research has emphasized the design of local error-correction circuits aimed at significantly extending quantum memory lifetimes [89]; notably, Park *et al.* proposed a low-resource code capable of preserving 12 logical qubits for nearly one million syndrome cycles using only 288 physical qubits [89].

Overall, the storage times and logical error rates, even with the error correction achieved to date, do not approach those of the unencoded case with conventional memories [90]. This limitation leaves only a narrow set of specialized authentication scenarios, namely those permitting very short communication distances. Near-future applications may still arise, for example, blind quantum communication with identity authentication, in which users can authenticate only when in close proximity to the computing resource [91].

3 Methodology

The procedure for identifying articles that extend QPUF research involves measuring the similarity between their reference lists, based on the assumption that articles building upon QPUFs tend to share common citations. To select the relevant articles for our study, we employed a modified version of the Jaccard similarity for sets [92], following these steps:

1. Select m baseline articles B_i that are known to contribute significantly to the development of QPUFs (in our case, $m = 4$).

2. Construct the reference space $\mathcal{B}$ by taking the union of the reference sets from the baseline articles:

$$\mathcal{B} := \bigcup_{i=1}^{m} T(B_i), \tag{1}$$

   where $T(B_i)$ denotes the set of references cited by the baseline article B_i.

3. Extract metadata and reference information from candidate articles using web Application Programming Interfaces (APIs) and/or ethical web scraping methods.

4. Compare each candidate article's reference set with the baseline reference space by matching Digital Object Identifiers (DOIs), using a cross-referencing API such as Crossref [93]. We define the modified Jaccard similarity as:

$$Sim(A_i) = \frac{|T(A_i) \cap \mathcal{B}|}{|T(A_i)|}, \tag{2}$$

   where $T(A_i)$ is the reference set of article A_i.

5. An article A_i is selected for further study if it satisfies the similarity threshold condition: $Sim(A_i) \geq l$, where l is the predefined acceptance threshold.

In this review, we have selected the works of QR-QPUF [94], QPUF [18, 26], and Hybrid PUFs (HPUFs) [17] as our baseline articles, as they introduce novel theoretical perspectives related to the QPUF topic. It is important to note a selection bias in our choice of baselines, as we primarily focus on approaches that emphasize theoretical protocol innovation. Furthermore, for our analysis, we have set the acceptance threshold value to $l = 0.1$. The outcome of the article selection is presented in Table 4 within the Appendix, where baseline articles are highlighted in yellow, and accepted articles for review are shaded in light gray. To better illustrate the relationships between articles, Figure 1 shows the co-citation network, with the article [18] on the left and [94] on the right, each serving as a baseline reference.

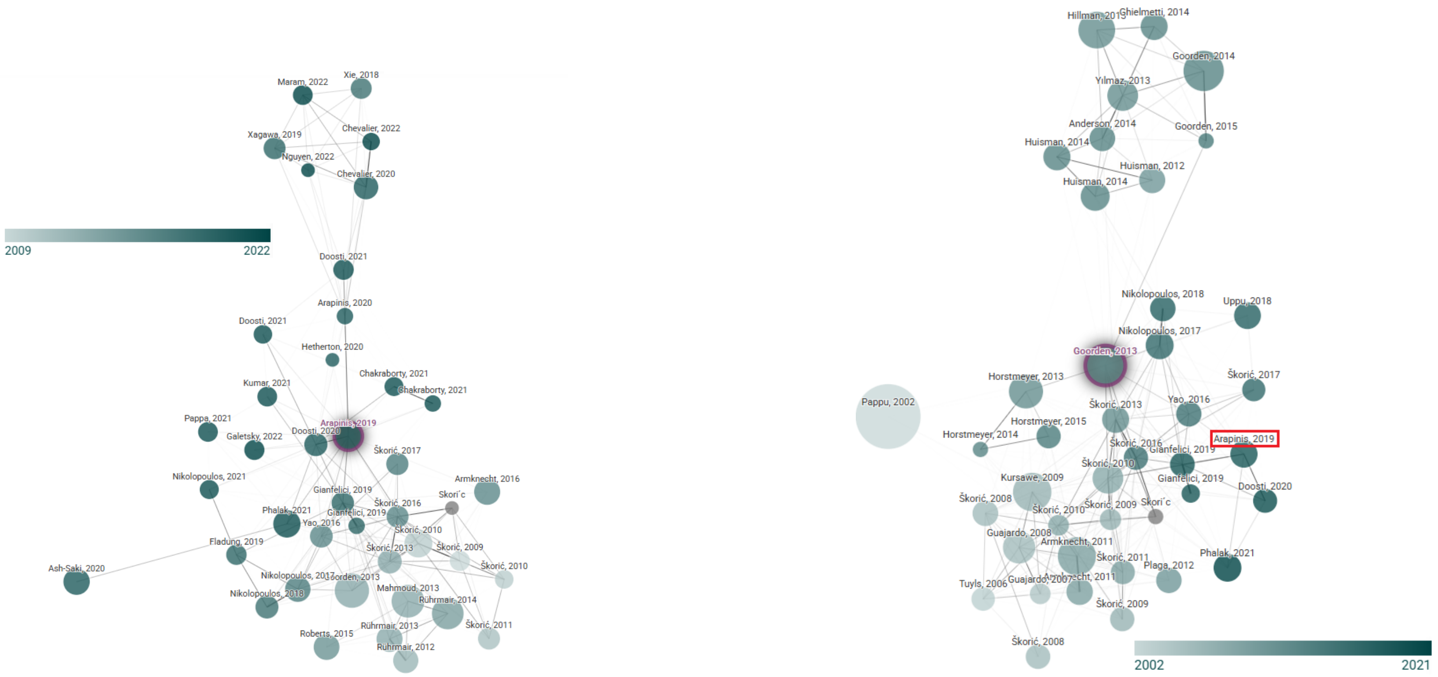
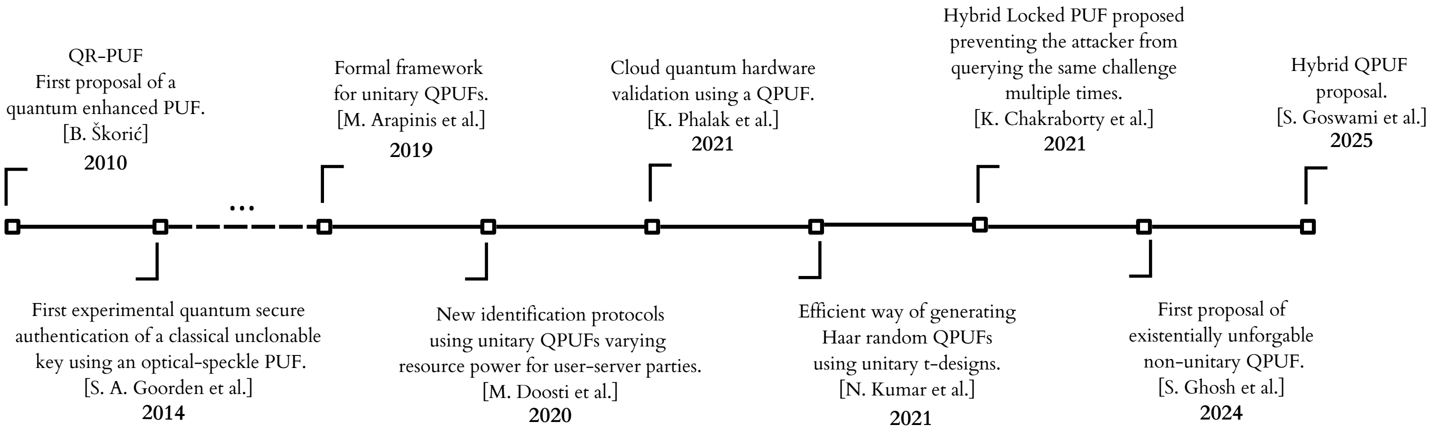


Figure 1: Graph relation to [18] (left) and to [94] (right). We observe the collision of co-citations from the right graph into the left one (highlighted in red). The years of the co-related papers are specified.

4 Review

In this section, we review the development of Quantum Physical Unclonable Functions (QPUFs), with a timeline of key milestones illustrated in Figure 2. We begin with Quantum-Readout PUFs (QR-PUFs), which are foundational to the field and noteworthy for their relatively modest hardware requirements compared to QPUFs. We introduce the initial QR-PUF proposals and highlight the first significant experimental demonstration. We also identify recurring features across various implementations, such as reliance on a trusted third party. With regard to QPUFs, our focus is on the body of work that builds upon the framework introduced in [18], examining the key enhancements and new directions proposed. A central point of discussion is whether these follow-up models satisfy the criteria established in Definition 1. In instances where they do not, we analyze the implications for the associated security properties. Moreover, we introduce another class of PUF models—known as Hybrid PUFs (HPUFs)—which offer an alternative approach by incorporating classical PUF architectures at their core. Finally, one of the articles selected for review ultimately inspired a comprehensive overview of QPUF analyses based on information-theoretic approaches and tools.



QR-PUF
First proposal of a
quantum enhanced PUF.
[B. Škorić]
2010

First experimental quantum secure
authentication of a classical unclonable
key using an optical-speckle PUF.
[S. A. Goorden et al.]
2014

Formal framework
for unitary QPUFs.
[M. Arapinis et al.]
2019

New identification protocols
using unitary QPUFs varying
resource power for user-server parties.
[M. Doosti et al.]
2020

Cloud quantum hardware
validation using a QPUF.
[K. Phalak et al.]
2021

Efficient way of generating
Haar random QPUFs
using unitary t-designs.
[N. Kumar et al.]
2021

Hybrid Locked PUF proposed
preventing the attacker from
querying the same challenge
multiple times.
[K. Chakraborty et al.]
2021

First proposal of
existentially unforgable
non-unitary QPUF.
[S. Ghosh et al.]
2024

Hybrid QPUF
proposal.
[S. Goswami et al.]
2025

Figure 2: Timeline with some of the major theoretical and hardware developments in the field of QPUFs.

4.1 QR-PUFs

Birth and development of QR-PUFs

The first QR-PUF was coined in [19]. In this work, the author assumes the existence of a physically unclonable device capable of performing quantum unitary evolutions. Two further assumptions are, first, that distinct sampled unitaries are unique and distinguishable, and second, that attackers cannot emulate such unitary evolution with a sufficiently small time delay. Under these assumptions, two protocols are derived for remote authentication, each assuming different measurement capabilities at the verifier side. Moreover, another protocol achieving both unidirectional and mutual authentication for a Quantum Key Distribution (QKD) scheme is proposed.

The author of [19] highlights, as one of their main strengths, that the presented QR-PUF protocols do not rely on trusted remote readers. This makes them secure against emulation attacks, but, however, it comes at the price of the strong assumptions made. Specifically, and as discussed in the cited article itself, assuming the impossibility of efficiently building a quantum emulator of the QR-PUF plays a paramount role and it is unclear whether it is a plausible premise. Intimately related to that, the work in [95] presents a cloning-based attack, further outlining the importance of the critical assumptions present within the discussed model.

Readers interested in security analyses concerning the first QR-PUF prototypes are referred to [96, 97]. The former study examines the security of the models introduced in [19], specifically against challenge estimation attacks. The latter presents a notable experimental implementation of a QR-PUF in a practical setup [94]. In particular, it evaluates the performance of a QR-PUF authentication protocol in an optical setting, accounting for quadrature-based attack strategies. The authors introduce quantitative metrics to effectively distinguish between legitimate clients and potential attackers.

Finally, we note that in an extension of the original model proposed in [19], the work in [20] presents a scheme that leverages a QR-PUF to authenticate the transmission of both classical and quantum information.

The QR-PUF theoretical framework

Within the formal aspect of QR-PUFs, the authors of [98] propose a theoretical framework in order to establish common quantifiable notions of security for distinct instances of either classical PUFs or QR-PUFs. We notice that under the considerations of the cited work, the set of challenges and responses for a QR-PUF can be fully characterized by classical information owned by the certifier, who becomes a trusted party. This trait, as pointed out in [21] for the already introduced work in [20], seems to encompass all QR-PUF models, and sets them apart from QPUFs. Moreover, [98] establishes the notions of robustness and unclonability, which resemble, respectively, the security notions of completeness and soundness [17]. The authors further distinguish between two kinds of unclonability. The first kind refers to physical unclonability, while the second kind, under the label of mathematical unclonability, formalizes the feature of non-learnability of a QR-PUF via query-based attacks. Importantly, quantifying the latter requires no reference to quantum properties, since it is done with respect to the classical characterization of the QR-PUF.

4.2 QPUFs

Polysemy of the term QPUF in the literature

The introduced theoretical framework on QR-PUFs, together with the one presented for QPUFs in Section 2.1, raises the question of whether the models presented in [33, 34] should be regarded as QR-PUF proposals, even though they are presented as QPUFs. That is, while the challenge-response mapping of the PUFs presented in the two cited articles stems from a quantum state preparation and measurement, such mapping is known by the certifier, and encoded as classical information. Both works propose a model that defines 1-qubit random rotations as challenges and monitors the output measurement histograms, which become the responses. Notably, these proposed schemes introduce the concept of using

variational circuits constrained to a specific architecture, capable of handling an arbitrary number of input qubits. Such number loosely functions as a security parameter, because the circuit complexity, and thus the learnability overhead, only scales polynomially with the number of input qubits.
Also labeled as a QPUF, the model proposed by the authors in [35] introduces the idea of associating a unique fingerprint to quantum hardware devices due to the uncontrollable variations in their qubit frequency, defined by its excited-to-ground-state energy difference. Remarkably, the authors display a desirable hamming weight within the keys generated via their fuzzy extraction [99] scheme, as well as a desirable hamming distance exhibited by different generated keys. Arguably, this contribution can also be seen as a QR-PUF model because the proposed set of challenges and responses is mappable to classical information owned by the certifier.

QPUF schemes building on [18]

With regard to QPUF models that adjust to the definitions provided in [18], we find three relevant works (see Table 3 for a schematic comparative):

1. Firstly, the article [30] proposes using a QPUF device for client-server authentication. This work includes two authentication protocols with distinct hardware requirements: one being suitable for server authentication, with a Low Resources Verifier (LRV), and the other being suitable for client authentication, with a High Resources Verfier (HRV). The former protocol introduces major variations to the initial scheme found in [18], owning extra steps that include QPUF-device exchange and quantum state shuffling. At the verifier side, no quantum measurements are needed to be carried out, but quantum memories are still required. As for the latter defined protocol, the main novelty introduced is that it allows to choose between two different testing algorithms, one relying on the ordinary swap test, as originally conceived, and the other one relying on the so-called generalized swap (gswap) test.

   In the two mentioned types of test, exponential security is achieved in the following sense: the probability of having a successful forgery for a polynomial adversary, in the number of targeted qubits, decreases exponentially with the security parameter N, i.e., the number of different challenges tested per round. Nevertheless, it is worth stressing that the completeness property, i.e., the assurance that legitimate provers are accepted, is highly dependent on the quantum noiseless assumption. That is, for the swap-test-based verification algorithm, a tiny amount of quantum noise brings the probability of true acceptance to an exponentially, in the number of responses M tested per each different challenge, low value. If gswap test is chosen instead, such problem is mitigated, but remains a concern to be addressed in real scenarios.

   More specifically, let us fix $N = 1$ challenges per verfication-decision round, and let us assume that the fidelities $\{F_i\}_{i=1}^{M}$ between the responses to the fixed challenge generated by a legitimate prover and those stored by the verifier fulfill

   $$1 - \mu \leq F_i \leq 1 - \epsilon \quad \forall i, \tag{3}$$

   for some $0 < \epsilon < \mu < 1$.

   Then, the swap-test-based verification algorithm leads to a probability p_{TA} of true acceptance fulfilling the condition

   $$\left(\frac{2-\mu}{2}\right)^{M} \leq p_{\text{TA}} \leq \left(\frac{2-\epsilon}{2}\right)^{M}, \tag{4}$$

   having that M also constrains the probability p_{TR} of true rejection, as

$$p_{\mathrm{TR}} \geq 1 - \left(\frac{1 + \frac{d+1}{D}}{2} \right)^M , \tag{5}$$

where D is the dimension of the underlying Hilbert space, and d is the dimension of the largest subspace spanned by the set of challenges queried by an adversary.

For the gswap-test-based verification algorithm, instead, we find

$$\frac{1}{M+1} + \frac{M}{M+1}(1-\mu) \leq p_{\mathrm{TA}} \leq \frac{1}{M+1} + \frac{M}{M+1}(1-\epsilon). \tag{6}$$

That is, in this case, p_{TA} is not upper-bounded by a quantity that approaches zero exponentially in M, as in Equation (4) and, moreover, we observe an informative lower bound for it. However, for p_{TR}, we find

$$p_{\mathrm{TR}} \geq 1 - \frac{1}{M+1} - \frac{M}{M+1} \frac{d+1}{D}. \tag{7}$$

Hence, we only find it to be lower-bounded by a quantity that approaches 1 at a slower pace than the one shown in Equation (5).

Finally, notice that if larger values of N are set, in order to enhance soundness, completeness is exponentially affected. That is, p_{TA} approaches zero exponentially fast in N for both types of tests considered.

2. Secondly, the work in [31] makes different relevant contributions to the field. On the one hand, the cited authors note that [18] lacks a uniqueness proof for their QPUF theoretical construction. Nevertheless, they show that uniqueness is guaranteed by the Haar-randomness hypothesis. Notably, they additionally prove that other sampling strategies can also deliver uniqueness. Furthermore this article comments on the inconvenience of the Haar-randomness requirement, and proposes an alternative relying on the well-known properties of t-designs, delivering the first application of this concept for a general value of t. The proper functioning of this alternative, however, comes at the price of restricting the number of queries by the adversary to t, instead of it being any polynomial amount of certain security parameters. As a final remark, this work does not omit a discussion on the effect of quantum noise, but they restrict it to the case of unitary noise channels. In such case the proposed scheme remains functional.

3. As the third and last proposal building on [18], the authors of [26] develop different schemes that further explore the potential of QPUFs, actively exploiting the Haar-randomness assumption. The contributions of this work are two-fold: on the one hand, the introduction of the Ideal QPUF model achieves the strongest kind of unforgeability against polynomial adversaries, i.e., quantum existential unforgeability, by harnessing the randomness provided by quantum measurements. Moreover, for this proposal, multiple swap tests are no longer required for the verification algorithm. The new acceptance procedure, instead, benefits from a one-shot scheme that owns similar desirable properties as those of the gswap verification. Nonetheless, the proposed implementations of such Ideal PUF suffer from serious practical drawbacks including exponential circuit depth and the requirement of inverting an unknown unitary evolution. On the other hand, the derived Measurement-Based PUF (MB-QPUF) takes advantage of the properties of maximally entangled states of arbitrary dimension in order to achieve selective unforgeability, while avoiding the costly resource of Haar randomness for the challenge selection. In such case, desirably, the two entangled system parties can be kept close to each other, avoiding the need of sustaining entanglement over large distances.

As a final observation before concluding this section, we aim to stress how, as pointed out by the last cited authors, QPUF models require further investigation when considering noisy environments.

Table 3: Comparison between proposals of novel schemes building on [18].

Article	Proposal name	Introduced improvement/s w.r.t. [18]	Drawback/s
M. Doosti et al. [30] (a)	HRV	gswap & Remote authentication	Haar randomness still required for challenge selection
M. Doosti et al. [30] (b)	LRV	Low-resources verifier & Remote autehentication	Haar randomness still required for challenge ´ selection
N. Kumar et al. [31]	QPUF from unitary t-designs	Haar randomness not required & Robust against unitary noise	Vulnerable against polynomial adversaries
S. Ghosh et al. [26] (a)	Ideal QPUF	Existentially unforgeable & Haar randomness not required for challenge selection & One-shot verification	Haar randomness still required for QPUF generation & Exponential circuit complexity/ unknown unitary inversion
S. Ghosh et al. [26] (b)	MB-QPUF	Haar randomness not required for challenge selection	Haar randomness still required for QPUF generation

It remains an open question whether there exist error correction procedures able to maintain the desirable security features of the introduced QPUF schemes while rendering them robust under realistic conditions, given the current and near-term hardware limitations.

4.3 Hybrid PUFs

In an attempt to gain practicality, the authors in [100] introduce the idea of combining classical and weak classical PUFs with a quantum encoding exploiting non-orthogonal states. Such construction, which they label as *quantum lock*, allows for having a Hybrid PUF (HPUF) that supports challenge reusability and is secure against attackers that have fully characterized the underlying classical PUF. On the other hand, both the *offline* and *online protocols* presented in [17] constitute two other HPUF models that, instead of relying on non-orthogonal state preparation, exploit the properties of maximally entangled states.
The above proposals represent a step towards requiring more realistic resources. For instance, they neither require quantum memories nor Haar randomness. Nevertheless, neither of the two articles discusses the effect of quantum noise or the threat posed by phishing-attack schemes, which can presumably compromise their security with the following strategy: the attacker impersonates the client first, in order to receive a challenge, and the server later, in order to obtain a valid response from the client and redirect it to the server.

4.4 Information-theoretic analysis of QPUFs

The security analysis of QPUFs is predominantly grounded in information-theoretic frameworks. Unlike computational security, which relies on hardness assumptions, information-theoretic approaches provide unconditional guarantees on critical properties such as unpredictability, unclonability, and entropy. Such an analysis establishes performance and security limits that are independent of implementation and adversarial capabilities, including those of quantum-capable adversaries.
Our article-selection criteria include the work in [101], which introduces an information-theoretic framework for QPUFs based on bipartite Discrete Memoryless Multiple Sources (DMMS), an abstraction derived from biometric source models [102]. Within this framework, QPUFs are modeled as stochastic sources, where a challenge is mapped to a response via a probabilistic transformation influenced by quantum or device-specific noise, and the challenge (input), response (output), and internal randomness are modeled as random variables. Unlike spatially distributed DMMS models, here the observations occur sequentially (in time) under varying physical conditions. This abstraction, which treats the QPUF as a black-box oracle, decouples the analysis from specific physical implementations, thereby enabling general, device-agnostic evaluations of uncertainty, noise, and information flow. It accommodates both classical and quantum challenge schemes while assuming quantum responses, encompassing a broad class of

QPUF protocols [103]. This analysis relies on two key bounds: the achievability bound, which ensures the existence of coding or challenge–response schemes that attain a target performance with vanishing error probability, and the converse bound, which defines the theoretical maximum that no scheme can exceed. Together, these bounds tightly determine the capacity and ultimate limits of QPUF-based cryptographic systems.

Within this framework, authentication performance is characterized via standard security metrics such as the False Acceptance Rate (FAR), representing the probability of an adversary being falsely accepted, and the False Rejection Rate (FRR), representing the likelihood of a legitimate prover being rejected. It has been shown that QPUF-based systems can be designed to achieve asymptotically vanishing FRR and exponentially decaying FAR, ensuring robust security guarantees even in the presence of quantum-capable adversaries [104].

Information-theoretic methods also underpin secure key generation and data storage using QPUFs [105, 106]. The core insight is that QPUFs' intrinsic randomness supplies high entropy that can be harvested into secret keys with provable secrecy. These high-entropy outputs can be processed (e.g., via privacy amplification) to yield secret keys. Information-theoretic analysis precisely quantifies how many secret bits can be extracted and how much information an adversary can learn. The secret key rate was shown to be related to the FAR, thereby establishing that a higher secret key rate extracted from a QPUF corresponds to a tighter bound on the adversarial success probability [104]. In [101, 107] secret key capacities extractable from QPUF outputs under privacy leakage have been bounded via mutual-information expressions. Extensions to secure data storage and message identification (detecting if a specific message is present instead of full decoding) via QPUFs were further characterized in [108] and [109], wherein identification capacity was shown to scale double-exponentially with the QPUF output length under idealized conditions. Importantly, these entropy-based bounds hold regardless of adversarial computational power. An information-theoretic argument guarantees that even a quantum-enabled adversary cannot reduce the QPUF's inherent entropy below its limit. In turn, the QPUF's intrinsic randomness is tied directly to provable secrecy: for example, any key derived from the QPUF can be made statistically independent of public helper data. These security guarantees rely on the concept of privacy leakage, which requires that public helper data reveal negligible information about the QPUF's output. This requirement is especially critical in quantum settings, as compromise of QPUF output could lead to irreversible identity theft.

All of these results rely on idealizations, i.i.d. noise, perfect challenge-response correlations, and unbounded blocklength, that abstract away practical limitations such as hardware imperfections, correlated errors, and finite-length effects. The necessity of bridging the gap between theoretical information-theoretic security proofs and realistic implementations has been emphasized in recent discussions [110, 111], and remains an important direction for future work. Despite these caveats, the information-theoretic framework provides a rigorous, implementation-independent foundation for the analysis of QPUF-based cryptographic protocols, ensuring robustness even against adversaries endowed with quantum capabilities.

5 Conclusions

In this review article, we explore the concept of Quantum Physical Unclonable Functions (QPUFs) from both theoretical and practical perspectives. The initial theoretical framework serves as a crucial starting point for formalizing the essential criteria a QPUF must satisfy. However, while conceptually well defined, this model faces substantial experimental limitations that currently hinder its practical deployment. Among the most pressing challenges are the handling of quantum noise and the development of an effective and reliable QPUF sampler. However, a range of studies have emerged that build upon this foundational framework, either by strengthening its security properties or by relaxing some of its more demanding practical constraints. These contributions offer valuable insights into how theoretical models might evolve towards implementable forms.

Our review also considers Quantum Readout PUFs (QR-PUFs), which represent a more practical and experimentally demonstrated class of devices. Although promising, these implementations rely on certain strong assumptions, and their security may be compromised when those assumptions do not hold. We also note that many models identified as QR-PUFs are frequently labeled as QPUFs in the literature. This blending of definitions reveals a notable polysemy, highlighting the need for clearer terminology and classification within the field.

Furthermore, we examine a novel solution found in recent contributions to the field: Hybrid PUFs (HPUFs). These aim to extend the capabilities of classical PUFs by integrating quantum features. These models show potential for supporting authentication protocols and represent a step towards practical applications grounded in classical-quantum hybrid systems.

Finally, we review the main works in the state of the art of studying QPUFs via information-theoretic analyses, which typically focus on both achievability and converse bounds, and exploit the interconnection between secret-key generation and authentication. We further acknowledge the idealizations that are typically present in approaches of this nature, and comment on how these affect the actual implications of the outcomes implied by such studies.

Acknowledgements

The authors gratefully acknowledge financial support from the Federal Ministry of Research, Technology and Space of Germany (BMFTR) within the program Souverän. Digital. Vernetzt. This work was supported by the joint project 6G-life, project identification numbers 16KISK002 and 16KISK263. Furthermore, VG and JN acknowledge additional support from BMFTR through projects 16KISQ039, 16KISQ077, and 16KISQ168, as well as from the German Research Foundation (DFG) under project NO 1129/2-1. CD and PJF received further funding from BMFTR projects 16KISQ169, 16KIS2196, 16KISQ038, 16KISR038, 16KISQ170, and 16KIS2234. HB and KN were supported by BMFTR projects 16KISQ037K, 16KISQ077, 16KISQ093, 16KISR026, 16KIS2195, and 16KIS1598K. TS, GP, and MB acknowledge support from the BMBF projects QPIS (No. 16KISQ032K) and DINOQUANT (No. 13N14921), as well as from the European Commission through the ERC Starting Grant project QUREP (No. 851810).

Appendix: Article-selection table for the review

Table 4 shows the list of articles considered in the review, including: title, authors, year, citation count, reference count and similarity score.

Title	Authors	Year	Citations	References	Similarity
[17] Hybrid Authentication Protocols for Advanced Quantum Networks	Suchetana Goswami et al.	2025	0	76	1.00
[112] QPUF Based on Multidimensional Fingerprint Features of Single Photon Emitters..	Qian Li et al.	2025	3	49	0.00
[113] Near-Infrared Circularly Polarized Luminescent Physical Unclonable Functions	Jiang Huang et al.	2024	13	14	0.00
[114] QPUF 2.0: Exploring Quantum Physical Unclonable Functions ...	Venkata K. V. V. B. et al.	2024	0	55	0.07
[115] QS-Auth: A Quantum-secure mutual authentication...	Mahima Mary Mathews et al.	2024	1	81	0.05
[116] Soteria: A Quantum-Based Device Attestation Technique...	Mansoor Ali Khan et al.	2024	10	46	0.05
[26] Existential unforgeability in quantum authentication...	Soham Ghosh et al.	2024	4	41	1.00
[101] Information Theoretic Analysis of a Quantum PUF	Kumar Nilesh et al.	2024	1	28	0.29
[34] QPUF: Quantum Physical Unclonable Functions for Security-by-Design...	Venkata K. V. V. B. et al.	2023	3	23	0.13
[117] Physical Realization...	Sara Nocentini et al.	2023	1	41	0.05
[118] Quantum Logic Locking for Security	Rasit Onur Topaloglu	2023	6	16	0.13
[119] Quantum Crosstalk as a Physically Unclonable Characteristic...	Christopher Z. Chwa et al.	2023	2	18	0.06
[35] Trustworthy Quantum Computation through...	Kaitlin N. Smith et al.	2023	0	28	0.18
[21] Comparison of Quantum PUF models	Vladlen Galetsky et al.	2022	9	29	0.13
[120] On Security Notions for Encryption in a Quantum World	C. Chevalier et al.	2022	40	38	0.05
[121] Dual-color dynamic anti-counterfeiting labels with persistent...	Ngei Katumo et al.	2022	33	49	0.02
[122] On the Quantum Security of OCB	Varun Maram et al.	2022	7	45	0.02
[33] Quantum PUF for Security and Trust...	Koustubh Phalak et al.	2021	73	18	0.28
[25] On the connection between quantum pseudorandomness...	Mina Doosti et al.	2021	5	48	0.08
[123] A Unified Framework For Quantum Unforgeability	Mina Doosti et al.	2021	12	34	0.15
[100] Quantum Lock: A Provable Quantum Communication Advantage	Kaushik Chakraborty et al.	2021	8	70	0.34
[31] Efficient Construction of Quantum Physical Unclonable Functions...	N. Kumar et al.	2021	14	41	0.10
[124] Learning classical readout quantum PUFs based on single-qubit gates	Anna Pappa et al.	2021	8	21	0.24
[11] Remote quantum-safe authentication of entities...	G. Nikolopoulos	2021	6	32	0.19
[30] Client-server Identification Protocols with Quantum PUF	Mina Doosti et al.	2020	24	58	0.16
[125] Gap-enhanced Raman tags for physically unclonable anticounterfeiting labels	Yuqing Gu et al.	2020	227	64	0.02
[126] Security Analysis of Identification Protocols...	Frederick Hetherton	2020	0	30	0.20
[127] Analysis of crosstalk in NISQ devices...	Abdullah Ash-Saki et al.	2020	64	14	0.00
[18] Quantum Physical Unclonable Functions: Possibilities and Impossibilities	Myrto Arapinis et al.	2019	55	55	1.00
[128] PbS Quantum Dots Based on PUFs for Ultra High-Density Key Generation	Yuejun Zhang et al.	2019	5	29	0.00
[98] Theoretical framework for physical unclonable...	Giulio Gianfelici et al.	2019	24	41	0.20
[129] Optical scheme for cryptographic commitments with physical unclonable keys	Georgios M. Nikolopoulos	2019	5	33	0.06
[130] Intercept-Resend Emulation Attacks Against a Continuous-Variable...	L. Fladung et al.	2019	14	35	0.09
[131] (Tightly) QCCA-Secure Key-Encapsulation...	Keita Xagawa et al.	2019	1	24	0.04
[132] A quantum related-key attack based...	H. Xie, L. Yang	2018	16	52	0.00
[133] Continuous-variable quantum authentication of...	G. Nikolopoulos	2018	47	37	0.03
[134] Asymmetric cryptography with physical unclonable keys	R. Uppu et al.	2018	34	38	0.05
[135] A Retrospective and a Look Forward: Fifteen Years of...	Chip-Hong Chang et al.	2017	177	132	0.05
[20] Authenticated communication from quantum readout of PUFs	B. Škorić et al.	2017	22	12	0.25
[136] Towards a Unified Security Model for...	F. Armknecht et al.	2016	63	32	0.16
[95] Quantum cloning attacks against PUF-based...	Y. Yao et al.	2016	22	34	0.18
[96] Security analysis of Quantum-Readout PUFs in the...	B. Škorić	2016	14	19	0.37
[137] Using Quantum Confinement to...	J. Roberts et al.	2015	54	38	0.13
[16] PUF modeling attacks: An introduction and overview	U. Rührmair, J. Sölter	2014	112	51	0.18
[97] Security of Quantum-Readout PUFs against quadrature-based...	B. Škorić et al.	2013	32	26	0.23
[94] Quantum-secure authentication of a physical...	S. A. Goorden et al.	2013	222	23	0.17
[8] On the practical use of physical unclonable functions in...	U. Rührmair, M. van Dijk	2013	52	37	0.22
[4] Sharp lower bounds on the extractable randomness from non-uniform sources	B. Škorić et al.	2011	15	23	0.17
[19] Quantum Readout of Physical Unclonable Functions	B. Škorić	2010	74	31	1.00

Table 4: QPUF papers are sorted by publication date (as of May 12th, 2025). Baseline articles are marked in yellow; accepted ones (with threshold $l = 0.1$) appear in light gray.

References

[1] R. Pappu, B. Recht, J. Taylor, and N. Gershenfeld, "Physical One-Way functions," *Science*, vol. 297, no. 5589, pp. 2026–2030, 2002, DOI: https://doi.org/10.1126/science.1074376.

[2] B. Chen and F. M. J. Willems, "Secret key generation over biased physical unclonable functions with polar codes," *IEEE Internet of Things Journal*, vol. 6, no. 1, pp. 435–445, 2019, DOI: https://doi.org/10.1109/JIOT.2018.2864594.

[3] R. Maes, V. van der Leest, E. van der Sluis, and F. Willems, "Secure key generation from biased PUFs: extended version," *Journal of Cryptographic Engineering*, vol. 6, no. 2, pp. 121–137, 2016, DOI: https://doi.org/10.1007/s13389-016-0125-6.

[4] B. Škorić, C. Obi, E. Verbitskiy, and B. Schoenmakers, "Sharp lower bounds on the extractable randomness from non-uniform sources," *Inf. Comput.*, vol. 209, pp. 1184–1196, 2011, DOI: https://doi.org/10.1016/j.ic.2011.06.001.

[5] I. Eichhorn, P. Koeberl, and V. van der Leest, "Logically reconfigurable pufs: Memory-based secure key storage," in *Proceedings of the Sixth ACM Workshop on Scalable Trusted Computing*, ser. STC '11. New York, NY, USA: Association for Computing Machinery, 2011, pp. 59–64, DOI: https://doi.org/10.1145/2046582.2046594.

[6] M. Cortez, G. Roelofs, S. Hamdioui, and G. di Natale, "Testing PUF-based secure key storage circuits," in *2014 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, 2014, pp. 1–6, DOI: https://doi.org/10.7873/DATE.2014.207.

[7] M. B. Santos, P. Mateus, and A. N. Pinto, "Quantum oblivious transfer: A short review," *Entropy*, vol. 24, no. 7, p. 945, 2022, DOI: https://doi.org/10.3390/e24070945.

[8] U. Rührmair and M. van Dijk, "On the practical use of physical unclonable functions in oblivious transfer and bit commitment protocols," *Journal of Cryptographic Engineering*, vol. 3, pp. 17–28, 2013, DOI: https://doi.org/10.1007/s13389-013-0052-8.

[9] M. Asim, J. Guajardo, S. S. Kumar, and P. Tuyls, "Physical unclonable functions and their applications to vehicle system security," in *VTC Spring 2009 - IEEE 69th Vehicular Technology Conference*, 2009, pp. 1–5, DOI: https://doi.org/10.1109/VETECS.2009.5073800.

[10] C. Herder, M.-D. Yu, F. Koushanfar, and S. Devadas, "Physical unclonable functions and applications: A tutorial," *Proceedings of the IEEE*, vol. 102, no. 8, pp. 1126–1141, 2014, DOI: https://doi.org/10.1109/JPROC.2014.2320516.

[11] G. M. Nikolopoulos, "Remote quantum-safe authentication of entities with physical unclonable functions," *Photonics*, vol. 8, no. 7, 2021, DOI: https://doi.org/10.3390/photonics8070289.

[12] G. T. Becker, "On the pitfalls of using arbiter-PUFs as building blocks," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 34, no. 8, pp. 1295–1307, 2015, DOI: https://doi.org/10.1109/TCAD.2015.2427259.

[13] J. Delvaux, "Machine-learning attacks on PolyPUFs, OB-PUFs, RPUFs, LHS-PUFs, and PUF–FSMs," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 8, pp. 2043–2058, 2019, DOI: https://doi.org/10.1109/TIFS.2019.2891223.

[14] U. Rührmair, F. Sehnke, J. Sölter, G. Dror, S. Devadas, and J. Schmidhuber, "Modeling attacks on physical unclonable functions," in *Proceedings of the ACM Conference on Computer and Communications Security.* ACM, 2010, pp. 237–249, DOI: https://doi.org/10.1145/1866307.1866335.

[15] U. Rührmair, J. Sölter, F. Sehnke, X. Xu, A. Mahmoud, V. Stoyanova, G. Dror, J. Schmidhuber, W. Burleson, and S. Devadas, "PUF modeling attacks on simulated and silicon data," Cryptology ePrint Archive, Paper 2013/112, 2013, DOI: https://doi.org/10.1109/TIFS.2013.2279798.

[16] U. Rührmair and J. Sölter, "PUF modeling attacks: An introduction and overview," *2014 Design, Automation & Test in Europe Conference & Exhibition (DATE)*, pp. 1–6, 2014, DOI: https://doi.org/10.7873/DATE.2014.361.

[17] S. Goswami, M. Doosti, and E. Kashefi, "Hybrid authentication protocols for advanced quantum networks," 2025, DOI: https://doi.org/10.48550/arXiv.2504.11552.

[18] M. Arapinis, M. Delavar, M. Doosti, and E. Kashefi, "Quantum Physical Unclonable Functions: Possibilities and Impossibilities," *Quantum*, vol. 5, p. 475, Jun. 2021, DOI: https://doi.org/10.22331/q-2021-06-15-475.

[19] B. Škorić, "Quantum readout of physical unclonable functions: Remote authentication without trusted readers and authenticated quantum key exchange without initial shared secrets," 2009, DOI: not available.

[20] B. Škorić, P. W. H. Pinkse, and A. P. Mosk, "Authenticated communication from quantum readout of PUFs," *Quantum Information Processing*, vol. 16, no. 7, p. 200, 2017, DOI: https://doi.org/10.1007/s11128-017-1649-0.

[21] V. Galetsky, S. Ghosh, C. Deppe, and R. Ferrara, "Comparison of quantum puf models," in *2022 IEEE Globecom Workshops*. IEEE, dec 2022, pp. 820–825, DOI: https://doi.org/10.1109/GCWkshps56602.2022.10008722.

[22] E. S. Meckes, *The Random Matrix Theory of the Classical Compact Groups.* Cambridge University Press, 2020, DOI: https://doi.org/10.1017/9781108303453.

[23] A. A. Mele, "Introduction to Haar Measure Tools in Quantum Information: A Beginner's Tutorial," *Quantum*, vol. 8, p. 1340, May 2024, DOI: https://doi.org/10.22331/q-2024-05-08-1340.

[24] O. D. Matteo, "Understanding the Haar measure," Mar. 2021, https://pennylane.ai/qml/demos/tutorial˙haar˙measure (accessed 2025-06-23).

[25] M. Doosti, N. Kumar, E. Kashefi, and K. Chakraborty, "On the connection between quantum pseudorandomness and quantum hardware assumptions," *Quantum Science and Technology*, vol. 7, no. 3, p. 035004, Apr. 2022, DOI: https://doi.org/10.1088/2058-9565/ac66fb.

[26] S. Ghosh, V. Galetsky, P. Julià Farré, C. Deppe, R. Ferrara, and H. Boche, "Existential unforgeability in quantum authentication from quantum physical unclonable functions based on random von neumann measurement," *Phys. Rev. Res.*, vol. 6, no. 4, p. 043306, Dec. 2024, DOI: https://doi.org/10.1103/PhysRevResearch.6.043306.

[27] A. Y. Kitaev, "Quantum computations: algorithms and error correction," *Russian Mathematical Surveys*, vol. 52, no. 6, pp. 1191–1249, 1997, DOI: https://doi.org/10.1070/RM1997v052n06ABEH002155.

[28] B. Regula, R. Takagi, and M. Gu, "Operational applications of the diamond norm and related measures in quantifying the non-physicality of quantum maps," *Quantum*, vol. 5, p. 522, Aug. 2021, DOI: https://doi.org/10.22331/q-2021-08-09-522.

[29] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition.* Cambridge University Press, 2010, DOI: https://doi.org/10.1017/CBO9780511976667.

[30] M. Doosti, N. Kumar, M. Delavar, and E. Kashefi, "Client-server identification protocols with quantum puf," *ACM Transactions on Quantum Computing*, vol. 2, pp. 1–40, 2020, DOI: https://doi.org/10.1145/3484197.

[31] N. Kumar, R. Mezher, and E. Kashefi, "Efficient construction of quantum physical unclonable functions with unitary t-designs," 2021, DOI: https://doi.org/10.48550/arXiv.2101.05692.

[32] L. F. Gladden, “Process tomography: Principles, techniques and applications,” *Measurement Science and Technology*, vol. 8, no. 4, p. 021, apr 1997, DOI: https://doi.org/10.1088/0957-0233/8/4/021.

[33] K. Phalak, A. A. Saki, M. Alam, R. O. Topaloglu, and S. Ghosh, “Quantum PUF for security and trust in quantum computing,” *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 11, no. 2, pp. 333–342, Jun. 2021, DOI: https://doi.org/10.1109/JETCAS.2021.3077024.

[34] V. K. V. V. Bathalapalli, S. P. Mohanty, C. Pan, and E. Kougianos, “QPUF: Quantum Physical Unclonable Functions for Security-by-Design of Industrial Internet-of-Things,” in *2023 IEEE International Symposium on Smart Electronic Systems (iSES)*, 12 2023, pp. 296–301, DOI: https://doi.org/10.1109/iSES58672.2023.00067.

[35] K. N. Smith and P. Gokhale, “Trustworthy quantum computation through quantum physical unclonable functions,” 2023, DOI: https://doi.org/10.48550/arXiv.2311.07094.

[36] W. K. Wootters and W. H. Zurek, “A single quantum cannot be cloned,” *Nature*, vol. 299, no. 5886, pp. 802–803, 1982, DOI: https://doi.org/10.1038/299802a0.

[37] H. Nishimura, *A Survey: SWAP Test and Its Applications to Quantum Complexity Theory.* Singapore: Springer Nature Singapore, 2025, pp. 243–261, DOI: https://doi.org/10.1007/978-981-96-0668-9_16.

[38] H. Chen, H. Jia, X. Wu, X. Wang, and M. Wang, “Quantum token for network authentication,” in *2021 IEEE International Conference on Web Services (ICWS)*, Sep. 2021, pp. 688–692, DOI: https://doi.org/10.1109/ICWS53863.2021.00095.

[39] A. Reiserer and G. Rempe, “Cavity-based quantum networks with single atoms and optical photons,” *Reviews of Modern Physics*, vol. 87, no. 4, pp. 1379–1418, Dec. 2015, DOI: https://doi.org/10.1103/RevModPhys.87.1379.

[40] W. Luo, L. Cao, Y. Shi, L. Wan, H. Zhang, S. Li, G. Chen, Y. Li, S. Li, Y. Wang, S. Sun, M. F. Karim, H. Cai, L. C. Kwek, and A. Q. Liu, “Recent progress in quantum photonic chips for quantum communication and internet,” *Light: Science & Applications*, vol. 12, no. 1, p. 175, Jul. 2023, DOI: https://doi.org/10.1038/s41377-023-01173-8.

[41] M.-H. Jiang, W. Xue, Q. He, Y.-Y. An, X. Zheng, W.-J. Xu, Y.-B. Xie, Y. Lu, S. Zhu, and X.-S. Ma, “Quantum storage of entangled photons at telecom wavelengths in a crystal,” *Nature Communications*, vol. 14, no. 1, p. 6995, Nov 2023, DOI: https://doi.org/10.1038/s41467-023-42741-1.

[42] R. Lockhart, “Low-rank separable states are a set of measure zero within the set of low-rank states,” *Physical Review A*, vol. 65, no. 6, 2002, DOI: https://doi.org/10.1103/PhysRevA.65.064304.

[43] F. Allmendinger, P. Blümler, M. Doll, O. Grasdijk, W. Heil, K. Jungmann, S. Karpuk, H.-J. Krause, A. Offenhäusser, M. Repetto, U. Schmidt, Y. Sobolev, K. Tullney, L. Willmann, and S. Zimmer, “Precise measurement of magnetic field gradients from free spin precession signals of 3He and 129Xe magnetometers,” *The European Physical Journal D*, vol. 71, no. 4, p. 98, Apr. 2017, DOI: https://doi.org/10.1140/epjd/e2017-70505-4.

[44] M. E. Limes, N. Dural, M. V. Romalis, E. L. Foley, T. W. Kornack, A. Nelson, and L. R. Grisham, “Long spin-1/2 noble gas coherence times in mm-sized anodically bonded batch-fabricated 3He-129Xe-87Rb cells,” *Applied Physics Letters*, vol. 126, no. 13, p. 134001, Mar. 2025, DOI: https://doi.org/10.1063/5.0245061.

[45] H. Tang, L. Banchi, T.-Y. Wang, X.-W. Shang, X. Tan, W.-H. Zhou, Z. Feng, A. Pal, H. Li, C.-Q. Hu, M. Kim, and X.-M. Jin, “Generating Haar-Uniform Randomness Using Stochastic Quantum

Walks on a Photonic Chip," *Physical Review Letters*, vol. 128, no. 5, p. 050503, Feb. 2022, DOI: https://doi.org/10.1103/PhysRevLett.128.050503.

[46] K. Kumaran, M. Sajjan, S. Oh, and S. Kais, "Random projection using random quantum circuits," *Physical Review Research*, vol. 6, no. 1, p. 013010, Jan. 2024, DOI: https://doi.org/10.1103/PhysRevResearch.6.013010.

[47] A. Roy and A. J. Scott, "Unitary designs and codes," *Designs, Codes and Cryptography*, vol. 53, no. 1, pp. 13–31, Oct. 2009, DOI: https://doi.org/10.48550/arXiv.0809.3813.

[48] Y. Nakata, C. Hirche, M. Koashi, and A. Winter, "Efficient Quantum Pseudorandomness with Nearly Time-Independent Hamiltonian Dynamics," *Physical Review X*, vol. 7, no. 2, p. 021006, Apr. 2017, DOI: https://doi.org/10.1103/PhysRevX.7.021006.

[49] P. Thomas, L. Ruscio, O. Morin, and G. Rempe, "Efficient generation of entangled multiphoton graph states from a single atom," *Nature*, vol. 608, no. 7924, pp. 677–681, Aug. 2022, DOI: https://doi.org/10.1038/s41586-022-04987-5.

[50] P. Thomas, L. Ruscio, O. Morin, and G. Rempe, "Fusion of deterministically generated photonic graph states," *Nature*, vol. 629, no. 8012, pp. 567–572, May 2024, DOI: https://doi.org/10.1038/s41586-024-07357-5.

[51] A. Russo, E. Barnes, and S. E. Economou, "Photonic graph state generation from quantum dots and color centers for quantum communications," *Physical Review B*, vol. 98, no. 8, p. 085303, Aug. 2018, DOI: https://doi.org/10.1103/PhysRevB.98.085303.

[52] J. Schupp, V. Krcmarsky, V. Krutyanskiy, M. Meraner, T. Northup, and B. Lanyon, "Interface between Trapped-Ion Qubits and Traveling Photons with Close-to-Optimal Efficiency," *PRX Quantum*, vol. 2, no. 2, p. 020331, Jun. 2021, DOI: https://doi.org/10.1103/PRXQuantum.2.020331.

[53] G. Pieplow, Y. Strocka, M. Isaza-Monsalve, J. H. D. Munns, and T. Schröder, "Deterministic Creation of Large Photonic Multipartite Entangled States with Group-IV Color Centers in Diamond," Dec. 2023, DOI: https://doi.org/10.48550/arXiv.2312.03952.

[54] K. Zelaya, M. Honari-Latifpour, and M.-A. Miri, "Integrated photonic programmable random matrix generator with minimal active components," *npj Nanophotonics*, vol. 2, no. 1, pp. 1–11, Feb. 2025, DOI: https://doi.org/10.1038/s44310-025-00054-9.

[55] L. E. Rodríguez, "A warm atomic vapour quantum memory in the context of space research," Doctoral Thesis, Technische Universität Berlin, Berlin, Germany, 2024, DOI: https://doi.org/10.14279/depositonce-21368.

[56] M. Fleischhauer, A. Imamoglu, and J. P. Marangos, "Electromagnetically induced transparency: Optics in coherent media," *Reviews of Modern Physics*, vol. 77, no. 2, pp. 633–673, Jul. 2005, DOI: https://doi.org/10.1103/RevModPhys.77.633.

[57] K. Shinbrough, D. R. Pearson, B. Fang, E. A. Goldschmidt, and V. O. Lorenz, "Broadband quantum memory in atomic ensembles," in *Advances In Atomic, Molecular, and Optical Physics*, ser. Advances in Atomic, Molecular, and Optical Physics, L. F. DiMauro, H. Perrin, and S. F. Yelin, Eds. Academic Press, Jan. 2023, vol. 72, pp. 297–360, DOI: https://doi.org/10.1016/bs.aamop.2023.04.001.

[58] A. I. Lvovsky, B. C. Sanders, and W. Tittel, "Optical quantum memory," *Nature Photonics*, vol. 3, no. 12, pp. 706–714, Dec. 2009, DOI: https://doi.org/10.1038/nphoton.2009.231.

[59] I. Marcikic, H. de Riedmatten, W. Tittel, V. Scarani, H. Zbinden, and N. Gisin, "Time-bin entangled qubits for quantum communication created by femtosecond pulses," *Physical Review A*, vol. 66, no. 6, p. 062308, Dec. 2002, DOI: https://doi.org/10.1103/PhysRevA.66.062308.

[60] J. M. Lukens and P. Lougovski, “Frequency-encoded photonic qubits for scalable quantum information processing,” *Optica*, vol. 4, no. 1, pp. 8–16, Jan. 2017, DOI: https://doi.org/10.1364/OPTICA.4.000008.

[61] K. C. Chen, E. Bersin, and D. Englund, “A polarization encoded photon-to-spin interface,” *npj Quantum Information*, vol. 7, no. 1, pp. 1–6, Jan. 2021, DOI: https://doi.org/10.1038/s41534-020-00337-3.

[62] C. D. Bruzewicz, J. Chiaverini, R. McConnell, and J. M. Sage, “Trapped-ion quantum computing: Progress and challenges,” *Applied Physics Reviews*, vol. 6, no. 2, May 2019, DOI: https://doi.org/10.1063/1.5088164.

[63] D.-I. D. Cho, S. Hong, M. Lee, and T. Kim, “A review of silicon microfabricated ion traps for quantum information processing,” *Micro and Nano Systems Letters*, vol. 3, no. 1, p. 2, Apr. 2015, DOI: https://doi.org/10.1186/s40486-015-0013-3.

[64] Y. Ma, Y.-Z. Ma, Z.-Q. Zhou, C.-F. Li, and G.-C. Guo, “One-hour coherent optical storage in an atomic frequency comb memory,” *Nature Communications*, vol. 12, no. 1, p. 2381, Apr. 2021, DOI: https://doi.org/10.1038/s41467-021-22706-y.

[65] J. Guo, X. Feng, P. Yang, Z. Yu, L. Q. Chen, C.-H. Yuan, and W. Zhang, “High-performance Raman quantum memory with optimal control in room temperature atoms,” *Nature Communications*, vol. 10, no. 1, Jan. 2019, DOI: https://doi.org/10.1038/s41467-018-08118-5.

[66] X.-H. Bao, A. Reingruber, P. Dietrich, J. Rui, A. Dück, T. Strassel, L. Li, N.-L. Liu, B. Zhao, and J.-W. Pan, “Efficient and long-lived quantum memory with cold atoms inside a ring cavity,” *Nature Physics*, vol. 8, no. 7, pp. 517–521, May 2012, DOI: https://doi.org/10.1038/nphys2324.

[67] Y.-W. Cho, G. T. Campbell, J. L. Everett, J. Bernu, D. B. Higginbottom, M. T. Cao, J. Geng, N. P. Robins, P. K. Lam, and B. C. Buchler, “Highly efficient optical quantum memory with long coherence time in cold atoms,” *Optica*, vol. 3, no. 1, p. 100, Jan. 2016, DOI: https://doi.org/10.1364/OPTICA.3.000100.

[68] P. Wang, C.-Y. Luan, M. Qiao, M. Um, J. Zhang, Y. Wang, X. Yuan, M. Gu, J. Zhang, and K. Kim, “Single ion qubit with estimated coherence time exceeding one hour,” *Nature Communications*, vol. 12, no. 1, Jan. 2021, DOI: https://doi.org/10.1038/s41467-020-20330-w.

[69] K. Barnes, P. Battaglino, B. J. Bloom, K. Cassella, R. Coxe, N. Crisosto, J. P. King, S. S. Kondov, K. Kotru, S. C. Larsen, J. Lauigan, B. J. Lester, M. McDonald, E. Megidish, S. Narayanaswami, C. Nishiguchi, R. Notermans, L. S. Peng, A. Ryou, T.-Y. Wu, and M. Yarwood, “Assembly and coherent control of a register of nuclear spin qubits,” *Nature Communications*, vol. 13, no. 1, p. 2779, May 2022, DOI: https://doi.org/10.1038/s41467-022-29977-z.

[70] M. Saffman, “Quantum computing with atomic qubits and Rydberg interactions: progress and challenges,” *Journal of Physics B: Atomic, Molecular and Optical Physics*, vol. 49, no. 20, p. 202001, Oct. 2016, DOI: https://doi.org/10.1088/0953-4075/49/20/202001.

[71] J. P. Covey, H. Weinfurter, and H. Bernien, “Quantum networks with neutral atom processing nodes,” *npj Quantum Information*, vol. 9, no. 1, Sep. 2023, DOI: https://doi.org/10.1038/s41534-023-00759-9.

[72] J. Simon, H. Tanji, J. K. Thompson, and V. Vuletić, “Interfacing collective atomic excitations and single photons,” *Phys. Rev. Lett.*, vol. 98, no. 18, p. 183601, May 2007, DOI: https://doi.org/10.1103/PhysRevLett.98.183601.

[73] M. P. Hedges, J. J. Longdell, Y. Li, and M. J. Sellars, “Efficient quantum memory for light,” *Nature*, vol. 465, no. 7301, pp. 1052–1056, Jun. 2010, DOI: https://doi.org/10.1038/nature09081.

[74] N. Bar-Gill, L. M. Pham, A. Jarmola, D. Budker, and R. L. Walsworth, “Solid-state electronic spin coherence time approaching one second,” *Nature Communications*, vol. 4, no. 1, p. 1743, Apr. 2013, DOI: https://doi.org/10.1038/ncomms2771.

[75] M. E. Trusheim, B. Pingault, N. H. Wan, M. Gündoğan, L. De Santis, R. Debroux, D. Gangloff, C. Purser, K. C. Chen, M. Walsh, J. J. Rose, J. N. Becker, B. Lienhard, E. Bersin, I. Paradeisanos, G. Wang, D. Lyzwa, A. R.-P. Montblanch, G. Malladi, H. Bakhru, A. C. Ferrari, I. A. Walmsley, M. Atatüre, and D. Englund, “Transform-limited photons from a coherent tin-vacancy spin in diamond,” *Phys. Rev. Lett.*, vol. 124, no. 2, p. 023602, Jan. 2020, DOI: https://doi.org/10.1103/PhysRevLett.124.023602.

[76] M. K. Bhaskar, R. Riedinger, B. Machielse, D. S. Levonian, C. T. Nguyen, E. N. Knall, H. Park, D. Englund, M. Lončar, D. D. Sukachev, and M. D. Lukin, “Experimental demonstration of memory-enhanced quantum communication,” *Nature*, vol. 580, no. 7801, pp. 60–64, Apr 2020, DOI: https://doi.org/10.1038/s41586-020-2103-5.

[77] K. Fook Lee, G. Gül, Z. Jim, and P. Kumar, “Fiber loop quantum buffer for photonic qubits,” *New Journal of Physics*, vol. 26, no. 8, p. 083011, aug 2024, DOI: https://doi.org/10.1088/1367-2630/ad6703.

[78] S. Cheng, C. Evans, and T. Pittman, “Fiber-coupled broadband quantum memory for polarization-encoded photonic qubits,” May 2025, DOI: https://doi.org/10.48550/arXiv.2505.10638.

[79] P. W. Shor, “Scheme for reducing decoherence in quantum computer memory,” *Physical Review A*, vol. 52, no. 4, pp. R2493–R2496, Oct. 1995, DOI: https://doi.org/10.1103/PhysRevA.52.R2493.

[80] D. Gottesman, “An Introduction to Quantum Error Correction and Fault-Tolerant Quantum Computation,” Apr. 2009, DOI: https://doi.org/10.48550/arXiv.0904.2557.

[81] B. M. Terhal, “Quantum error correction for quantum memories,” *Reviews of Modern Physics*, vol. 87, no. 2, pp. 307–346, Apr. 2015, DOI: https://doi.org/10.1103/RevModPhys.87.307.

[82] S. Heußen, D. F. Locher, and M. Müller, “Measurement-Free Fault-Tolerant Quantum Error Correction in Near-Term Devices,” *PRX Quantum*, vol. 5, no. 1, p. 010333, Feb. 2024, DOI: https://doi.org/10.1103/PRXQuantum.5.010333.

[83] N. Ofek, A. Petrenko, R. Heeres, P. Reinhold, Z. Leghtas, B. Vlastakis, Y. Liu, L. Frunzio, S. M. Girvin, L. Jiang, M. Mirrahimi, M. H. Devoret, and R. J. Schoelkopf, “Extending the lifetime of a quantum bit with error correction in superconducting circuits,” *Nature*, vol. 536, no. 7617, pp. 441–445, Aug. 2016, DOI: https://doi.org/10.1038/nature18949.

[84] R. Acharya, D. A. Abanin, L. Aghababaie-Beni *et al.*, “Quantum error correction below the surface code threshold,” *Nature*, vol. 638, no. 8052, pp. 920–926, feb 2025, DOI: https://doi.org/10.1038/s41586-024-08449-y.

[85] M. H. Abobeih, Y. Wang, J. Randall, S. J. H. Loenen, C. E. Bradley, M. Markham, D. J. Twitchen, B. M. Terhal, and T. H. Taminiau, “Fault-tolerant operation of a logical qubit in a diamond quantum processor,” *Nature*, vol. 606, no. 7916, pp. 884–889, Jun. 2022, DOI: https://doi.org/10.1038/s41586-022-04819-6.

[86] H. Zhang, L. Wan, S. Paesani, A. Laing, Y. Shi, H. Cai, X. Luo, G.-Q. Lo, L. C. Kwek, and A. Q. Liu, “Encoding Error Correction in an Integrated Photonic Chip,” *PRX Quantum*, vol. 4, no. 3, p. 030340, Sep. 2023, DOI: https://doi.org/10.1103/PRXQuantum.4.030340.

[87] B. W. Reichardt, D. Aasen, R. Chao, A. Chernoguzov, W. v. Dam, J. P. Gaebler, D. Gresh, D. Lucchetti, M. Mills, S. A. Moses, B. Neyenhuis, A. Paetznick, A. Paz, P. E. Siegfried, M. P. d. Silva, K. M. Svore, Z. Wang, and M. Zanner, “Demonstration of quantum computation and error correction with a tesseract code,” Dec. 2024, DOI: https://doi.org/10.48550/arXiv.2409.04628.

[88] K. DeBry, N. Meister, A. V. Martinez, C. D. Bruzewicz, X. Shi, D. Reens, R. McConnell, I. L. Chuang, and J. Chiaverini, “Error correction of a logical qubit encoded in a single atomic ion,” Mar. 2025, DOI: https://doi.org/10.48550/arXiv.2503.13908.

[89] M. Park, N. Maskara, M. Kalinowski, and M. D. Lukin, “Enhancing quantum memory lifetime with measurement-free local error correction and reinforcement learning,” *Physical Review A*, vol. 111, no. 1, p. 012419, Jan. 2025, DOI: https://doi.org/10.1103/PhysRevA.111.012419.

[90] V. Galetsky, N. Vyas, A. Comin, and J. Nötzel, “Feasibility of logical bell state generation in memory assisted quantum networks,” 2025, DOI: https://doi.org/10.48550/arXiv.2412.01434.

[91] J. Quan, Q. Li, and L. Li, “Verifiable blind quantum computation with identity authentication for different types of clients,” Oct. 2022, DOI: https://doi.org/10.1109/TIFS.2023.3340859.

[92] L. da F. Costa, “Further generalizations of the Jaccard index,” 2021, DOI: https://doi.org/10.48550/arXiv.2110.09619.

[93] Patrick Polischuk. rest-api-doc. https://github.com/CrossRef/rest-api-doc (accessed 2025-06-23).

[94] S. A. Goorden, M. Horstmann, A. P. Mosk, B. Škorić, and P. W. H. Pinkse, “Quantum-secure authentication of a physical unclonable key,” *Optica*, vol. 1, no. 6, pp. 421–424, Dec 2014, DOI: https://doi.org/10.1364/OPTICA.1.000421.

[95] Y. Yao, M. Gao, M. Li, and J. Zhang, “Quantum cloning attacks against puf-based quantum authentication systems,” *Quantum Information Processing*, vol. 15, pp. 3311–3325, 2016, DOI: https://doi.org/10.1007/s11128-016-1316-x.

[96] B. Škorić, “Security analysis of quantum-readout pufs in the case of challenge-estimation attacks,” *Quant. Inf. Comput.*, vol. 16, no. 1-2, pp. 0050–0060, 2016, DOI: https://doi.org/10.26421/QIC16.1-2-4.

[97] B. Škorić, A. Mosk, and P. Pinkse, “Security of quantum-readout pufs against quadrature based challenge estimation attacks,” *IACR Cryptol. ePrint Arch.*, vol. 2013, p. 84, 2013, https://eprint.iacr.org/2013/084 (accessed 2025-06-23).

[98] G. Gianfelici, H. Kampermann, and D. Bruß, “Theoretical framework for physical unclonable functions, including quantum readout,” *Physical Review A*, 2019, DOI: https://doi.org/10.1103/PhysRevA.101.042337.

[99] Y. Dodis, R. Ostrovsky, L. Reyzin, and A. Smith, “Fuzzy extractors: How to generate strong keys from biometrics and other noisy data,” *SIAM Journal on Computing*, vol. 38, no. 1, pp. 97–139, Jan. 2008, DOI: https://doi.org/10.1137/060651380.

[100] K. Chakraborty, M. Doosti, Y. Ma, C. Wadhwa, M. Arapinis, and E. Kashefi, “Quantum lock: A provable quantum communication advantage,” *Quantum*, vol. 7, p. 1014, May 2023, DOI: https://doi.org/10.22331/q-2023-05-23-1014.

[101] K. Nilesh, C. Deppe, and H. Boche, “Information theoretic analysis of a Quantum PUF,” in *2024 IEEE International Symposium on Information Theory (ISIT)*, 2024, pp. 3320–3325, DOI: https://doi.org/10.1109/ISIT57864.2024.10619408.

[102] T. Ignatenko, F. M. Willems *et al.*, “Biometric security from an information-theoretical perspective,” *Foundations and Trends® in Communications and Information Theory*, vol. 7, no. 2–3, pp. 135–316, 2012, DOI: http://dx.doi.org/10.1561/0100000051.

[103] K. Nilesh, C. Deppe, and H. Boche, “Quantum PUF and its applications with information theoretic analysis,” in *2024 IEEE 10th World Forum on Internet of Things (WF-IoT)*. IEEE, 2024, pp. 1–6, DOI: https://doi.org/10.1109/WF-IoT62078.2024.10811185.

[104] K. Nilesh, C. Deppe, and H. Boche, "Authentication based on quantum PUF," IEEE, 2025, International Conference on Communications (IEEE ICC), DOI: not available.

[105] K. Nilesh, M. Geitz, C. Deppe, and H. Boche, "Method and apparatus for enrolling a data message for identification in a data storage, and method and apparatus for identifying the presence of one or more query data messages," Filed: 2025-06-07, Application No.: EP25181530.4, Publisher: European Patent Office, DOI: not available.

[106] K. Nilesh, M. Geitz, C. Deppe, and H. Boche, "Method and apparatus for storing a data message in a data storage, and method and apparatus for retrieving a data message from a data storage," Filed: 2025-06-07, Application No.: EP25181531.2, Publisher: European Patent Office, DOI: not available.

[107] K. Nilesh, C. Deppe, and H. Boche, "Quantum PUF based secret key generation and secure storage with side information," IEEE, 2025, International Symposium on Information Theory (ISIT), DOI: not available.

[108] K. Nilesh, C. Deppe, and H. Boche, "Secret key generation and storage based on QPUF," IEEE, 2025, Information Theory Workshop (ITW), DOI: not available.

[109] K. Nilesh, C. Deppe, and H. Boche, "Secure storage and identification using quantum PUF," IEEE, 2025, International Conference on Communications (IEEE ICC), DOI: not available.

[110] Z. Amiri, R. Bassoli, H. Boche, S. Charania, J. Czarske, S. Das, C. Deppe, D. L. Calsi, S. Maheshwari, S. Nande, K. Nilesh, J. Nötzel, and Q. Zhang, "Quantum technology applications for 6G networks," in *6G-life: Unveiling the Future of Technological Sovereignty, Sustainability and Trustworthiness*. Academic Press, 2025, DOI: not available.

[111] Z. Amiri, R. Bassoli, H. Boche, S. Charania, J. Czarske, S. Das, C. Deppe, S. Dev, F. Fitzek, M. Habibie, J. Hawellek, M. He, K. Jamshidi, D. L. Calsi, S. Nande, K. Nilesh, J. Nötzel, D. Plettemeier, A. Shetewy, C. Upadhyay, and Q. Zhang, "Quantum technology concepts for 6G networks," in *6G-life: Unveiling the Future of Technological Sovereignty, Sustainability and Trustworthiness*. Academic Press, 2025, DOI: not available.

[112] Li, Qian, Chen, Feiliang, Su, Juan, Yao, Yao, Kang, Jianbin, Xie, Feng, Li, Mo, and Zhang, Jian, "Quantum physical unclonable function based on multidimensional fingerprint features of single photon emitters in random aln nanocrystals," *Advanced Functional Materials*, vol. 35, no. 9, p. 2416216, 2025, DOI: https://doi.org/10.1002/adfm.202416216.

[113] Huang, Jiang, Jin, Xue, Yang, Xuefeng, Zhao, Tonghan, Xie, Helou, and Duan, Pengfei, "Near-infrared circularly polarized luminescent physical unclonable functions," *ACS Nano*, vol. 18, no. 24, pp. 15 888–15 897, Jun. 2024, DOI: https://doi.org/10.1021/acsnano.4c03136.

[114] Bathalapalli, Venkata K. V. V., Mohanty, Saraju P., Pan, Chenyun, and Kougianos, Elias, "QPUF 2.0: Exploring quantum physical unclonable functions for security-by-design of energy cyber-physical systems," 2024, DOI: https://doi.org/10.48550/arXiv.2410.12702.

[115] M. M. Mathews and P. V., "QS-auth: A quantum-secure mutual authentication protocol based on puf and post-quantum signature for heterogeneous delay-tolerant networks," *Journal of Information Security and Applications*, vol. 83, p. 103787, 2024, DOI: https://doi.org/10.1016/j.jisa.2024.103787.

[116] M. A. Khan, M. N. Aman, and B. Sikdar, "Soteria: A quantum-based device attestation technique for internet of things," *IEEE Internet of Things Journal*, vol. 11, no. 9, pp. 15 320–15 333, 2024, DOI: https://doi.org/10.1109/JIOT.2023.3346397.

[117] S. Nocentini, U. Rührmair, M. Barni, D. S. Wiersma, and F. Riboli, "Physical realization of a hyper unclonable function," 2023, DOI: https://doi.org/10.48550/arXiv.2301.02147.

[118] R. O. Topaloglu, "Quantum logic locking for security," *J*, vol. 6, no. 3, pp. 411–420, 2023, DOI: https://doi.org/10.3390/j6030027.

[119] C. Z. Chwa, L. A. Hsia, and L. D. Merkle, "Quantum crosstalk as a physically unclonable characteristic for quantum hardware verification," in *NAECON 2023 - IEEE National Aerospace and Electronics Conference*, 2023, pp. 309–313, DOI: https://doi.org/10.1109/NAECON58068.2023.10365761.

[120] C. Chevalier, E. Ebrahimi, and Q.-H. Vu, "On security notions for encryption in a quantum world," Cryptology ePrint Archive, Paper 2020/237, 2020, https://eprint.iacr.org/2020/237 (accessed 2025-06-23).

[121] N. Katumo, K. Li, B. S. Richards, and I. A. Howard, "Dual-color dynamic anti-counterfeiting labels with persistent emission after visible excitation allowing smartphone authentication," *Scientific Reports*, vol. 12, no. 1, p. 2100, Feb. 2022, DOI: https://doi.org/10.1038/s41598-022-05885-6.

[122] V. Maram, D. Masny, S. Patranabis, and S. Raghuraman, "On the quantum security of OCB," Cryptology ePrint Archive, Paper 2022/699, 2022, https://eprint.iacr.org/2022/699 (accessed 2025-06-23).

[123] M. Doosti, M. Delavar, E. Kashefi, and M. Arapinis, "A unified framework for quantum unforgeability," 2021, DOI: https://doi.org/10.48550/arXiv.2103.13994.

[124] N. Pirnay, A. Pappa, and J.-P. Seifert, "Learning classical readout quantum pufs based on single-qubit gates," *Quantum Machine Intelligence*, vol. 4, no. 2, p. 14, Jun. 2022, DOI: https://doi.org/10.1007/s42484-022-00073-1.

[125] Y. Gu, C. He, Y. Zhang, L. Lin, B. D. Thackray, and J. Ye, "Gap-enhanced raman tags for physically unclonable anticounterfeiting labels," *Nature Communications*, vol. 11, no. 1, p. 516, Jan. 2020, DOI: https://doi.org/10.1038/s41467-019-14070-9.

[126] F. Hetherton, "Security analysis of identification protocols based on quantum physical unclonable functions," MSc Dissertation, School of Informatics, University of Edinburgh, Edinburgh, UK, 2020, DOI: not available.

[127] A. Ash-Saki, M. Alam, and S. Ghosh, "Analysis of crosstalk in NISQ devices and security implications in multi-programming regime," *Proceedings of the ACM/IEEE International Symposium on Low Power Electronics and Design*, 2020, DOI: https://doi.org/10.1145/3370748.3406570.

[128] Y. Zhang, Z. Luan, X. Zhang, J. Shu, and P. Wang, "PbS quantum dots based on physically unclonable function for ultra high-density key generation," *Journal of Electronic Materials*, vol. 48, no. 12, pp. 7603–7607, Dec 2019, DOI: https://doi.org/10.1007/s11664-019-07660-2.

[129] G. M. Nikolopoulos, "Optical scheme for cryptographic commitments with physical unclonable keys," *Optics Express*, vol. 27, no. 20, p. 29367, Sep. 2019, DOI: https://doi.org/10.1364/OE.27.029367.

[130] L. Fladung, G. M. Nikolopoulos, G. Alber, and M. Fischlin, "Intercept-resend emulation attacks against a continuous-variable quantum authentication protocol with physical unclonable keys," *Cryptography*, vol. 3, no. 4, p. 25, Oct. 2019, DOI: https://doi.org/10.3390/cryptography3040025.

[131] K. Xagawa and T. Yamakawa, "(Tightly) QCCA-secure key-encapsulation mechanism in the quantum random oracle model," *IACR Cryptol. ePrint Arch.*, vol. 2018, p. 838, 2019, https://eprint.iacr.org/2018/838 (accessed 2025-06-23).

[132] H. Xie and L. Yang, "A quantum related-key attack based on bernstein-vazirani algorithm," *ArXiv*, vol. abs/1808.03266, 2018, DOI: https://doi.org/10.1007/s11128-020-02741-2.

[133] G. M. Nikolopoulos and E. Diamanti, “Continuous-variable quantum authentication of physical unclonable keys,” *Scientific Reports*, vol. 7, no. 1, p. 46047, 2017, DOI: https://doi.org/10.1038/srep46047.

[134] R. Uppu, T. A. W. Wolterink, S. A. Goorden, B. Chen, B. Škorić, A. P. Mosk, and P. W. H. Pinkse, “Asymmetric cryptography with physical unclonable keys,” *Quantum Science and Technology*, vol. 4, no. 4, p. 045011, oct 2019, DOI: https://doi.org/10.48550/arXiv.1802.07573.

[135] C.-H. Chang, Y. Zheng, and L. Zhang, “A retrospective and a look forward: Fifteen years of physical unclonable function advancement,” *IEEE Circuits and Systems Magazine*, vol. 17, no. 3, pp. 32–62, 2017, DOI: https://doi.org/10.1109/MCAS.2017.2713305.

[136] F. Armknecht, D. Moriyama, A. Sadeghi, and M. Yung, “Towards a unified security model for physically unclonable functions,” *IACR Cryptol. ePrint Arch.*, vol. 2016, p. 33, 2016, https://eprint.iacr.org/2016/033 (accessed 2025-06-23).

[137] J. Roberts, I. E. Bagci, M. A. M. Zawawi, J. Sexton, N. Hulbert, Y. J. Noori, M. Young, C. Woodhead, M. Missous, M. Migliorato, U. Roedig, and R. Young, “Using quantum confinement to uniquely identify devices,” *Scientific Reports*, vol. 5, 2015, DOI: https://doi.org/10.1038/srep16456.