Quantum Science and Technology

PERSPECTIVE • OPEN ACCESS

Practical quantum tokens: challenges and perspectives

To cite this article: Nadezhda Kukharchyk *et al* 2026 *Quantum Sci. Technol.* **11** 040501

Quantum Science and Technology

OPEN ACCESS

RECEIVED
11 February 2026

REVISED
20 July 2026

ACCEPTED FOR PUBLICATION
29 July 2026

PUBLISHED
1 September 2026

PERSPECTIVE

Practical quantum tokens: challenges and perspectives

Nadezhda Kukharchyk[1,2,3,*], Holger Boche[3,4], Christian Deppe[3,5], Kirill Fedorov[1,2,3], Martin E Garcia[6], Ilja Gerhardt[7], Rudolf Gross[1,2,3], Thomas Halfmann[8], Hans Huebl[1,2,3], David Hunger[9,10], Wolfgang Kilian[11], Roman Kolesov[12], Juliane Krämer[13], Alexander Kubanek[14,15], Kai Müller[16], Boris Naydenov[17], Janis Nötzel[3,18], Anna P Ovvyan[19], Wolfram H P Pernice[19], Gregor Pieplow[20], Cyril Popov[21], Tim Schroeder[20,22], Kilian Singer[6] and Janik Wolters[23,24,25,26]

[1] Walther-Meißner-Institut, Bayerische Akademie der Wissenschaften, 85748 Garching, Germany
[2] School of Natural Sciences, Technical University of Munich, 85748 Garching, Germany
[3] Munich Center for Quantum Science and Technology (MCQST), 80799 Munich, Germany
[4] Lehrstuhl für Theoretische Informationstechnik, School of Computation, Information and Technology, Technical University of Munich, 80333 Munich, Germany
[5] Institut für Nachrichtentechnik, 38106 Braunschweig, Germany
[6] Institute of Physics, Center for Interdisciplinary Nanostructure Science and Technology (CINSaT), University of Kassel, 34132 Kassel, Germany
[7] Institute for Solid State Physics, Leibniz University Hannover, 30167 Hannover, Germany
[8] Institut für Angewandte Physik, Technische Universtität Darmstadt, 64289 Darmstadt, Germany
[9] Karlsruher Institut für Technologie, Physikalisches Institut, 76131 Karlsruhe, Germany
[10] Karlsruher Institut für Technologie, Institut für QuantenMaterialien und Technologien, 76344 Eggenstein-Leopoldshafen, Germany
[11] Physikalisch-Technische Bundesanstalt (PTB), 10587 Berlin, Germany
[12] 3rd Institute of Physics, University of Stuttgart, 70569 Stuttgart, Germany
[13] Faculty of Informatics and Data Science, University of Regensburg, 93053 Regensburg, Germany
[14] Institute for Quantum Optics, Ulm University, 89081 Ulm, Germany
[15] Center for Integrated Quantum Science and Technology (IQST), Ulm University, Albert-Einstein-Allee 11, 89081 Ulm, Germany
[16] Walter Schottky Institute, Technical University of Munich, 85748 Garching, Germany
[17] Department Spins in Energy Conversion and Quantum Information Science (ASPIN), Helmholtz-Zentrum Berlin für Materialien und Energie GmbH, 14109 Berlin, Germany
[18] Emmy-Noether Group Theoretical Quantum Systems Design, School of Computation, Information and Technology, Technical University of Munich, 80333 Munich, Germany
[19] Kirchhoff-Institute for Physics, Heidelberg University, 69120 Heidelberg, Germany
[20] Department of Physics, Humboldt University of Berlin, 12489 Berlin, Germany
[21] Institute of Nanostructure Technologies and Analytics (INA), Center for Interdisciplinary Nanostructure Science and Technology (CINSaT), University of Kassel, 34132 Kassel, Germany
[22] Ferdinand-Braun-Institute, 12489 Berlin, Germany
[23] Institute of Space Research, German Aerospace Center (DLR e.V.), 12489 Berlin, Germany
[24] Institutes of Physics, Technische Universität Berlin, 10623 Berlin, Germany
[25] Einstein Center Digital Future (ECDF), 10117 Berlin, Germany
[26] AQLS UG (haftungsbeschränkt), 10587 Berlin, Germany
[*] Author to whom any correspondence should be addressed.

E-mail: nadezhda.kukharchyk@wmi.badw.de

Keywords: quantum token, quantum memories, QKD, spin ensembles, infomation security

Abstract

The concept of quantum tokens dates back alongside quantum cryptography to Stephen Wiesner's seminal work in 1983. Already this initial work proposes society-relevant applications such as secure quantum banknotes, which can be exchanged between a bank and a customer. This quantum currency is based on various physical states that can be easily verified but is protected from being copied by the fundamental quantum laws. Four decades later, these ideas have flourished in the field of quantum information, and the concept of quantum banknotes has not only adopted many varying names, such as quantum money, quantum coins, quantum-digital payments, and quantum tokens, but also reached its first experimental demonstrations. In this perspective article, we discuss the current state-of-the-art of quantum tokens in the field of quantum information, as well as their future perspectives. We present a number of physical realizations of quantum tokens with integrated quantum memories and their applicability scenarios in detail. Finally, we discuss

how quantum tokens fit into the information security ecosystem and consider their relationship to post-quantum cryptography.

1. Introduction

Quantum states of light and their interaction with matter have been in the spotlight since the 1970 s. Numerous experiments have confirmed quantum-mechanical properties of light and matter, including but not limited to the observation of quantum entanglement and superposition in individual atomic systems and macroscopic condensates [1–5]. The underlying non-classical effects have catalyzed the development of numerous innovative protocols and technologies for information processing, sensing or quantum applications in general. In addition, quantum communication has been identified as highly relevant for secure information transmission and distributed quantum applications. Also, quantum banknotes were already conceptualized in 1983, which is associated with the advent of quantum tokens nowadays [6]. This quantum currency is based on the idea of an unconditionally secure quantum banknote that can be exchanged between banks and their customers. This concept is intimately linked to an early version of the no-cloning theorem [7, 8] and an initial proposal for a quantum key distribution (QKD) scheme [9]. Nowadays, this quantum-secured exchange is celebrated as the BB84 protocol.

When originally conceived, the idea of quantum tokens was beyond the reach of experimental implementation. In the last decades, one of the main directions of experimental studies with quantum systems has been the controlled creation and manipulation of non-classical states for applications in various quantum technologies [10]. The latter are often classified into the following key pillars: quantum communication, quantum computing, quantum simulation, quantum sensing, and quantum metrology (see figure 1). While these cornerstones of quantum science ask highly relevant intrinsic scientific questions and test quantum mechanics in itself, they also offer opportunities for present-day and future applications. In particular, the question of whether suitable quantum states, protocols, and algorithms can provide an advantage over classical communication, information processing, simulation or sensing schemes is part of active research. Presently, aspects such as task processing times, signal-to-noise ratios, provable security, among others, are investigated. Some quantum advantages have already been experimentally addressed and demonstrated, such as reaching the unconditional security of communication [11, 12], performing classically impossible communication tasks [2, 13], or demonstrating the quantum advantage in computation [14, 15]. The field of quantum communication, which is key to the idea of quantum tokens, has been at the forefront of these developments and has historically been pioneered by experiments in the optical regime. In the field of quantum computing, superconducting circuits operating at microwave frequencies are currently one of the leading candidates for future scalable quantum computers [16]. The combination of these two prominent, but experimentally very different, platforms gives rise to the concept of hybrid quantum communication and computation. This approach allows one to exploit the best of the two worlds' properties to ultimately achieve the goal of quantum advantage in practically relevant tasks. Thanks to significant experimental progress in manipulating quantum states through their preparation, storage, and readout—concepts surrounding quantum tokens can now be realized in proof-of-principle experiments.

The original quantum token ideas by S. Wiesner have received renewed attention over the last decade, in no small part because the rapid advances in quantum computing threaten to undermine the existing classical cryptography protocols which underpin the entire modern communication network. While post-quantum encryption approaches are considered to be a mid-term strategy [17], they may not guarantee the protection of sensitive information in the long term, because of their purely computational security and the corresponding vulnerability to the 'harvest now, decode later' attack, as opposed to the information-theoretic security provided by quantum encryption schemes. Respectively, the field of research on quantum tokens can be defined as a combination of quantum cryptography protocols with quantum memories. Similar to classical keys, verification of quantum tokens can be split into two categories: public and private. In private authentication only selected parties can verify the key [6, 18–20], while public verification can be performed by any party without any knowledge of the originally issued key [21–23].

Combined with their quantum features, these tokens promise to address several security issues, such as eavesdropping detection, privacy, unforgeability, and even contribute to the overarching problem of secure authentication preceding any remote communication between two or more parties. While authentication — the process of verifying one's identity — has been a foundational element of human society for millennia, it has traditionally relied on physical objects that can be generally copied or forged.

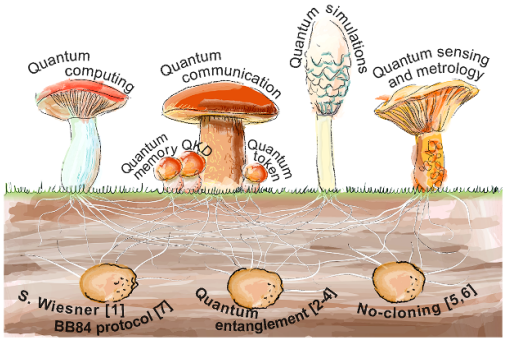

Figure 1. The loose structure of quantum information fields and sub-fields in relation to selected milestone ideas.

Quantum tokens follow these initial verification principles and can strengthen authentication by exploiting quantum features such as no-cloning and measurement theorems. The unconditional security of the authentication process depends additionally on the specifics of the authentication model. In private-key authentication settings, information-theoretic security can be achieved in suitable one-time authentication mechanisms, for example, in the quantum-digital payment scheme [24], and in quantum message authentication schemes [25]. By contrast, public-key authentication schemes are more model-dependent and typically require additional restrictions, such as controlled distribution or a bounded number of quantum public-key copies [26, 27]; standard public-key authentication remains computationally secure.

Quantum tokens are thus closely tied to the concepts of QKD, but can extend beyond them. In contrast to QKD, whose primary function is to establish shared secret keys between remote parties [9, 28], a quantum token serves as a quantum credential that can be presented and verified at a later time [6, 21]. In private-key token schemes, the verifiers may still require shared secret information, which could, for instance, be distributed using QKD [9, 28]. However, the token aspect provides additional functionality not supplied by QKD alone, such as one-time use, one-time spending, or one-time authentication [6, 24]. This extends the applicability scenarios of quantum tokens beyond those of typical QKD protocols, making quantum tokens more demanding in realization, but more useful in applications. Most importantly, conventional quantum tokens must include a quantum memory element, in one form or another, which can be accessed by request and may also be recycled. Practically, a **quantum token can be understood as a device which stores a codebook of selected quantum states**. These stored quantum states can be retrieved and verified during an authentication or payment procedure. As long as the quantum nature of these states is preserved, it conceptually prevents a duplication of the quantum token, thereby protecting against forgery attacks and guaranteeing validation security. It has also been proposed that probing of an extended reservoir of quantum states can be done selectively in a non-destructive manner, so that this reservoir can be probed and verified again [29]. This approach could potentially allow for multiple uses (recycling) of the single-issued quantum token, while still benefiting from the information-theoretic protection provided by quantum mechanics.

In the existing literature, the concept of quantum tokens appears under different names, such as quantum money [6, 30, 31], quantum payment [24], quantum ticket [18], quantum tokenized signature [32]. All these names address the problem of unforgeability [32–34], which is the central property and requirement for the quantum token.

A somewhat alternative approach to the quantum token ideas is to use a quantum analogue of classical physically unclonable functions (PUFs) [35]. Here, one is supposed to use a classical physical system, the clonability of which is considered practically unrealistic. Then, one can employ quantum states to probe properties of this PUF and protect a corresponding communication channel by quantum laws [36]. Such systems are sometimes referred to as the quantum-read PUFs (QR-PUFs) [37, 38]. Their advantage is that they do not necessarily require a long-living quantum memory [39] and, therefore, are much easier to implement experimentally. The obvious drawback is that the ultimate security of such QR-PUFs relies on the ignorance of their intrinsic PUF structure, which, in theory, can be broken.

Another standalone type of quantum tokens is the so-called S-money protocol, which can be realized without any storage element. In general, S-money relies on short-distance quantum communication and space-time restrictions for the verification of the corresponding classical keys distributed within a network of trusted agents [40, 41]. The S-money thus relies on QKD protocols to exchange a classical key via a short-range quantum channel, which protects this information transfer step by the no-cloning theorem and leaves the task of secure local storage of classical keys to be implemented using classical

or post-quantum protection routines. Finally, the unconditional protection of the classical key between agents stems from space-time restrictions on the classical communication channels between them [42]. A recent realization of the S-money protocol highlights technological advantages of this approach [42].

In this perspective article, we refer to the quantum token as to a device containing a quantum memory element storing a selected codebook of quantum states. Here, it is important to highlight the recent advances in the experimental realization of long-living quantum memories. For instance, it has been demonstrated that one can achieve coherence times of up to 18 h by using an optical quantum memory based on rare-earth elements [43] in combination with its unique temperature stability. Such memories could be made compatible with other experimental requirements in order to encode and validate the quantum token states at optical frequencies [19, 20]. In the gigahertz frequency range—relevant for superconducting quantum circuits and processors—electronic spin ensembles have demonstrated record coherence times, with storage durations reaching up 2 s in nuclear spin denuded silicon [44].

At the same time, recent demonstrations of various quantum communication and cryptography protocols with propagating microwaves [13, 45] demonstrate the experimental feasibility of this approach. In this publication, we present selected experimental realizations and theoretical proposals for quantum tokens, comprising a quantum memory with the corresponding storage and readout routines. Finally, we present our vision for quantum tokens in terms of applications and quantum information science, as well as accounting for the competing field of post-quantum cryptography (PQC) and its place in the overarching information security landscape.

2. Overview of possible physical realizations

Practical realizations of quantum tokens are driven by their use-cases, which embrace their means of transport, storage, and verification routines (see figure 2(a)). One cornerstone is a dedicated vendor that provides quantum tokens. Those can then be exchanged either via a quantum link followed by storing the token in a state-of-the-art long-lived quantum memory, or emitted directly in the form of a physically transportable entity. At a later stage, these tokens can be locally or remotely challenged to ensure their validity, e.g. for authentication purposes. This concept dictates three main ingredients: a storage unit or ***quantum memory***, a ***transmission channel***, and an ***encoding and verification protocol***, as schematically shown in figure 2(b). A unique combination of these three parts forms a specific realization of quantum tokens.

One key and unsolved challenge in realizing quantum tokens is establishing the ***quantum memory***. After identifying a potential candidate, its properties determine the subsequent choice of the transmission channel and the encoding protocol. Quantum memories are physical systems capable of coherently storing a quantum state for a sufficiently long time and returning it on demand. Potential candidates span from natural atoms or ions to artificial atoms and cavities. They come in the form of ensembles of atomic gases, color centers in diamonds, donors in silicon, and rare earth spin ensembles. In applications, which do not require ultra-long storage times, other systems are no less useful, such as 3D microwave cavities [46–48], superconducting artificial atoms [49–51], quantum dots [52], trapped atom and ions [53–56], and even phononic modes [57, 58].

In this article, we focus on a selection of ultra-long coherent spin memories that combine electronic and nuclear spins in the context of quantum tokens. We explore their potential for information encoding, possible transport and communication protocols, and application scenarios. Specifically, we detail spin systems in Cesium-Xenon gas mixtures [59–61], (Si,V, Sn, N)-V centers in diamonds [62–65], Phosphorus donors in silicon [66, 67], and rare earth ions [68–70], all of which have already demonstrated outstanding coherence results and are therefore considered to be the key-systems envisioning accessible quantum memories.

Due to semi-shielding of their 4*f*-electrons, the rare earth ions are an excellent example of spin ensembles exhibiting outstanding quantum coherence of optical and spin degrees of freedom [71], culminating in a recent demonstration of record-long nuclear spin coherence lifetime of up to 18 hours [43]. The color centers in diamonds are a large group of defects, which can couple to the long-coherent nuclear spins of ^{13}C and guarantee fast photon read-out rates [72–76]. For the prototypical system of electron spins, localized phosphorus donors in isotopically pure, nuclear spin-free silicon have demonstrated coherence times up to seconds [77] and, if transferred into a coupled nuclear spin system [78, 79], up to hours [80]. Gas mixtures of alkali metals and noble gases allow for storing optical signals in an electron state in the alkali metal ground state [81–83] and to coherently transfer this state further to more coherent states of nuclear spins of noble gas atomss [84].

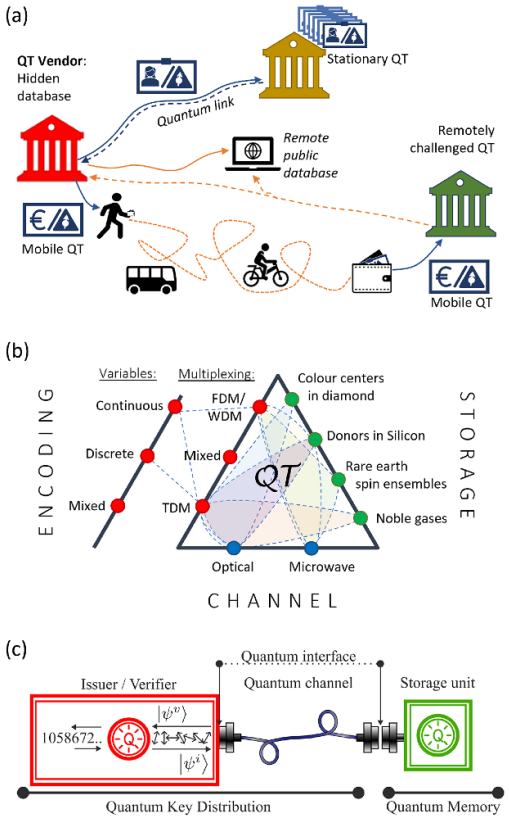

Figure 2. (a) Simplified implementation of quantum token. Here, a flying quantum token is an authentication or transaction key that does not require any intermediate storage. The on-submission quantum token, on the other hand, requires a storage element. The on-submission quantum token can be verified by the holder at the latest by the time of expiry of the quantum storage element. (b) Structural representation of a quantum token, which in a general case requires an encoding protocol, a transmission channel, and a storage element. The encoding protocol is defined by the choice of type of variables (continuous, discrete or mixed) and multiplexing method: TDM (time-division multiplexing), FDM/WDM (frequency- or wavelength-division multiplexing) and mixed. The transmission channel defines the frequency of wavelength at which the respective quantum token is being generated and transmitted; it is bound to the available infrastructure. (c) Key elements of physical realization of quantum token, which include issuing and verifying parties, transmission channel, and storage element.

In these systems, the quantum state is often stored in an excitation of an ensemble of electron and nuclear spins in the form of so-called 'spin-wave excitation' [85] or a collective Dicke state [86]: $|\psi\rangle = \sum_j^N c_j e^{i\delta_i t} e^{-jkz_j} |r_1 \dots e_j \dots g_N\rangle$, which implies deployment of such storage protocols as atomic frequency comb (AFC) [87–89] or off-resonant Raman-type [90, 91]. With techniques initially developed in pulsed spin resonance, the quantum state can be further transferred from the electronic spins into coupled nuclear spins [78, 79], which offers enhanced storage times in the range of hours [80]. To extract information from these systems, refocusing pulses are applied, as implemented in the Hahn echo sequence, and are followed by read-out optical pulses. Other approaches explore the possibility of selectively addressing single ions or atoms to store single quantum states [70]. This would allow the addition of spatial and frequency dimensions to quantum memory multiplexing [92–94].

The properties of the selected quantum memory impose requirements regarding the implementation of the ***channel*** used for the transmission, which we attribute to either the optical or the microwave domain. Some of the specific systems discussed later can also be addressed via both optical and microwave excitations, thus enabling control via either channel. However, motivated by optical quantum communication technologies, many of them have been primarily researched for the storage of optical photons. Particular optical interest lies in the compatibility with the existing infrastructure of fiber networks, which could be used for quantum communication, thereby reducing construction efforts.

While communication between very distant quantum nodes is best ensured by optical fiber technologies, local direct (wireless) communication can alternatively be implemented using microwave and GHz technologies. In particular, when considering the integration with superconducting microwave quantum circuits, this approach allows for circumventing the necessity of transducing the quantum signal between the gigahertz and optical frequencies. [95, 96]. The development of quantum microwaves and the associated technologies began more than ten years ago as a pioneering scientific achievement [97–99]. Demonstration that quantum properties (such as path entanglement) can be observed

in propagating microwave signals is one of the crucial achievements [100–102]. Due to the low signal energy of quantum microwaves, suitable measurement methods had to be developed first, with which propagating squeezed states could then be detected [13, 103–105]. Combining spin systems with quantum microwaves allows one to close the technology gap in the generation and storage of purely microwave quantum tokens, as these play a central role in the realization of quantum networks in the GHz frequency range.

The third pillar of basic quantum token representation is the ***encoding*** routine, which is also researched in the QKD field. One quantum token is a combination of generated single quantum states, which can be distributed in time (time domain multiplexing or TDM) or in frequency/ wavelength (frequency/wavelength domain multiplexing or TDM/WDM), the choice of which is limited by the chosen quantum memory system. As a basic example, microwave quantum memory based on ensembles of donors in silicon has a very narrow available frequency bandwidth and thus facilitates only TDM [67]. Optical quantum memories based on rare earth spin ensembles, on the other hand, are nicely compatible with either TDM, or FDM, or a combination of both due to their inhomogeneously broadened optical transitions and developed storage routines [106].

Additionally, the encoding relies on the type of variables used to generate the key, with two standard types: discrete and continuous-variables (CVs). The discrete-variable (DV) protocols use individual photons and their properties, such as polarization, to encode information, whereas CV protocols rely on the quadratures of light, like amplitude and phase. The aforementioned BB84 protocol [9, 107] is a textbook example of a DV protocol, which uses strictly defined combinations of photon polarizations. It typically achieves longer transmission distances than CV schemes but requires expensive single-photon detectors. There are other DV protocols, such as 10^{91} [108], BBM92 [11] or SARG04 [109], which aim to mitigate the weaknesses and pitfalls of the BB84 protocol. The CV protocols can operate with standard telecommunication components and offer higher key rates over short distances. However, CV systems are more sensitive to noise and loss, making them more challenging over long distances [110–112]. Both approaches have unique advantages and are actively developed for different use cases in quantum communication [113].

The basic representation of the quantum token outlined in figure 2(b) does not capture key **performance metrics** that go well beyond the coherence time of the chosen quantum memory system. These metrics, such as *fidelity, write-read efficiency, qubit count parameter, bit-rate, etc*, are essential for evaluating the practical applicability of quantum token solutions [114]. Some of these parameters are highly dependent on the quality of individual devices, while others are intrinsically linked to the internal properties of the selected spin systems and the encoding protocols employed. Nearly the most important quantity characterizing the applicability of the QT device is the ***fidelity*** F, which measures how close the verified quantum state $|\psi^v\rangle$ is to the issued quantum state $|\psi^i\rangle$, in the general case:

$$F\left(\rho\left(|\psi^v\rangle\right),\rho\left(|\psi^i\rangle\right)\right)=\left(\mathrm{tr}\sqrt{\sqrt{\rho\left(|\psi^v\rangle\right)}\rho\left(|\psi^i\rangle\right)\sqrt{\rho\left(|\psi^v\rangle\right)}}\right)^2.$$

Here, $\rho(|\psi^{v,i}\rangle)$ are the density matrices of the verified and issued quantum states, respectively. The fidelity can be specified for separate elements of quantum tokens: quantum channel, quantum memory, and the interface between them (see figure 2(c)). However, the overall fidelity of the quantum token device is of utmost importance, as it quantifies the total loss of quantum information. The ***write-read efficiency*** η is the quantitative characteristic of the quantum memory. It is defined as the ratio of retrieved (verified) photons to the issued ones. However, it lacks information on whether the quantum state is preserved. The complexity of the token key depends on its size, which is described by the ***qubit count parameter***. This parameter is limited by the storage and control capabilities of the quantum memory and by the ***bit-rate*** of the channel-memory combination. The robustness of a quantum token against transmission noise is quantified by a total verification ***error rate***, including errors from the transmission channel, memory, interfaces, and measurement. While in each specific case the tolerable error rate is protocol dependent, it is possible to identify its highest bound, which is inversely proportional to the asymptotic no-cloning fidelity setting lowest possible bound for transmitted fidelity when the protocol is still secure. This is particularly relevant for all deterministic protocols. For Wiesner-type encodings, explicit security analyses show that the probability of producing two valid noiseless copies decreases exponentially with the number of encoded states, scaling as $(3/4)^n$. Noisy implementations require a threshold version of this bound, where the accepted error fraction is chosen between the honest noise level and the best achievable counterfeiting error rate [115]. In addition, the error rate can be reduced

by ***quantum error correction*** postprocessing routines, such as the BBBSS protocol [11], the Cascade protocol [116], the Winnow protocol [117], or low-density parity-check codes optimized for QKD postprocessing [118, 119]. The additional metrics for quantum tokens are related to the previously mentioned main ones. They can be derived first with respect to the QKD and memory parts independently, and then combined to achieve the overall device performance.

To determine a single quantity characterizing the total quantum token reliability, we can define an ***effective lifetime of a quantum token*** as the maximum time interval between the token issuance and verification for which an honestly stored token is accepted with probability above the protocol threshold, while the probability of successful forgery remains below the required security bound. This lifetime is therefore not identical to the intrinsic coherence time of the memory, but is a protocol quantity determined by the combined effects of storage time, write-read efficiency, state fidelity, loss, noise, qubit count, and the chosen verification threshold. The realistic storage time required is consequently application dependent. Flying-token or quantum-digital-payment schemes may require only short-lived quantum states during the transaction or issuance stage and can avoid long-term quantum storage [24, 42]. In contrast, on-submission or Wiesner-type quantum tokens require the quantum state itself to remain verifiable until later presentation, so their useful lifetime must exceed the expected delay between issuance and verification [6]. Thus, seconds-to-minutes storage can already be relevant for online authentication or payment scenarios, whereas portable offline tokens would require substantially longer, potentially hours-to-days, storage times.

Most of the quantum memories discussed here are solid-state-based, thus suffering significantly from interactions with lattice vibrations (phonons). To reduce the impact of phonons, one has to freeze them out by cooling down such memories to liquid helium temperatures or even below. Moreover, one has to decouple the remaining phononic excitations from the frequencies of the utilized spin states. This leads to a significant overhead of operational infrastructure, consisting of a cryostat, often requiring the supply of liquid ^{4}He or a ^{4}He/^{3}He mixture. For spin-based systems, in addition, a magnet system is required, providing magnetic fields from hundreds to thousands of mT. Quantum tokens integrating such memories can be demonstrated soon. However, they require substantial running costs and maintenance resources, which large institutions can afford but are out of reach for the average private user. Nevertheless, such tokens could be deployed by larger stakeholders, such as banks or governments, as stationary units, see figure 2(a).

One of the most fascinating aspects is certainly the idea of a mobile quantum token, which can be carried by any single user as easily as in a pocket and can be used to securely validate any transaction or prove identity. This is the holy grail of quantum memories, requiring the preservation of a quantum state in ambient conditions when being exposed to mechanical shocks, electromagnetic radiation, and other noise sources. Thermalized to room temperatures and about the size of a finger, quantum memories based on mixtures of alkali metal and noble gas atoms in atomic vapor cells address the problem of storing photonic quantum states for several minutes, hours, or even up to days under ambient conditions [84, 120, 121].

Once ensuring the required robustness and technological simplicity of the overall system, they are expected to outperform solid-state quantum memories and pioneer the mobile version of quantum tokens. On the other hand, solid-state quantum memories are making rapid progress and are meanwhile addressing the possibility of preserving a quantum state at natural thermal conditions. This has been experimentally demonstrated recently with an ensemble of donors in isotopically engineered silicon, where a quantum bit has been stored for 39 min [80]. The possibility of room-temperature storage is also being actively pursued for devices based on nitrogen-vacancy centers in silicon, where the quantum state is transferred into a nuclear spin state with long coherence time.

As discussed in more detail in the following sections, the key emphasis of this publication is to review the current status and perspectives of a variety of experimentally explored quantum memory systems, including their potential to enable a wide range of promising applications and use cases. In the following sections, we discuss each system in detail, along with the appropriate protocols and implementation scenarios.

3. Microwave quantum tokens for superconducting quantum networks

Recent advances in generating quantum states in the microwave domain, coupled with the progress in superconducting circuit–based quantum information processing and the persistent challenge of efficient microwave-to-optical transduction, underscore the importance of developing quantum tokens and their

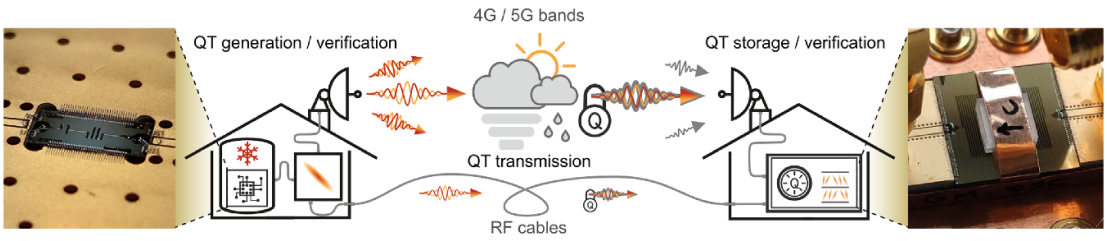

Figure 3. Microwave quantum tokens show strong potential for the advancement of secure short-range quantum communication. Beyond traditional cable-based connections, wireless links in the 2–12GHz frequency range are feasible due to the exceptionally low absorption losses in open air. These links also exhibit strong resilience to weather-related disturbances, such as fog and rain. Recent studies [45] report high fidelities for the wireless transmission of microwave quantum states. Taken together, these findings indicate that secure information transmission via quantum tokens can be seamlessly integrated into existing classical microwave communication infrastructures.

storage directly within the gigahertz frequency range. In this section, we follow a holistic experimental approach operating in the microwave frequency domain. We address both the generation of quantum tokens as well as strategies for their storage and retrieval in solid-state spin ensembles. The key generation is based on CV quantum communication representing an established concept in QKD [28], quantum teleportation [122], dense coding [123], and Q-tokens [18], which has been successfully translated to the field of gigahertz communications using superconducting quantum circuits [13, 45, 103, 124, 125], as conceptually shown in figure 3. Notably, the latter concepts are directly compatible with the superconducting quantum processors. In particular, they discuss the generation of Q-tokens assembled from displaced squeezed states corresponding to the CV regime of quantum communication. Especially for small-scale local networks with characteristic ranges of up to about 100m, direct communication between quantum nodes using GHz signals is expected to offer clear advantages over approaches based on the frequency conversion (FC) to optical frequency bands [126, 127]. Such microwave quantum networks can be complemented further by using ultra-long-lived quantum memories based on spin ensembles, which can be directly interfaced with microwave quantum states. Specifically, we discuss here phosphorus dopants in isotopically engineered, nuclear-spin-diluted, silicon host crystals as well as erbium-based spin ensembles in $LiYF_4$ and $CaWO_4$ matrices. Both systems have demonstrated electron spin coherence times exceeding seconds [44, 80] and are considered as prime candidates for quantum memory applications [128].

We implement the generation of a microwave Q-token in the gigahertz frequency band using concepts inspired by a well-known CV QKD protocol [129]. This scheme is based on two central operations: (i) squeezing and (ii) displacement of propagating microwave states. The latter imprints the secret token information and encodes the classical key as a quantum state, while the squeezing operation ensures the unconditional security of the protocol. A corresponding microwave CV-QKD protocol with finite-size codebooks of displaced squeezed microwaves has recently been implemented with superconducting circuits and demonstrated the information-theoretic security [45]. Respectively, such codebooks or ensembles of displaced squeezed states represent the Q-token, which can be stored in a quantum memory. This type of Q-token guarantees the information security against copying attempts via the no-cloning theorem. Evaluating the fidelity of retrieved quantum states enables verification of whether a duplicate has been made. For instance, if the state fidelity F_{nc} exceeds the threshold of $2/3$, assuming an infinite Gaussian Q-token codebook in the measurement device independence (MDI) regime [130], one can assert that the state has not been copied, thereby confirming the authenticity of information therein. In real systems, one has to rely on finite-energy codebooks which lead to somewhat increased no-cloning threshold values, $F_{\mathrm{nc}} > 2/3$ [131, 132].

In our particular experiments, we generate microwave squeezed states using superconducting Josephson parametric amplifiers (JPAs) [133], which typically consist of a $\lambda/4$ coplanar waveguide resonator shorted to ground via a direct-current superconducting quantum interference device (dc-SQUID). The dc-SQUID provides a nonlinear inductance, enabling a flux-tunable JPA resonance frequency. The periodic modulation of the magnetic flux through the dc-SQUID with a strong coherent tone at twice the JPA resonance frequency enables a parametric amplification process, which leads to squeezing of the JPA's input signals. These squeezed states are subsequently emitted by the JPA and can be guided to spin ensembles, as sketched in figure 4.

One approach to realizing a quantum memory relies on resonantly converting microwave signals into spin excitations via an intermediate microwave resonator inductively coupled to the spin ensemble [85].

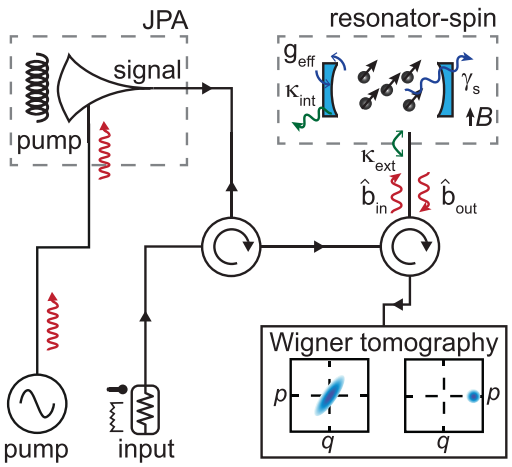

Figure 4. Conceptual experimental setup for the coupling of propagating squeezed microwaves and quantum tokens to a spin ensemble. A Josephson parametric amplifier (JPA), controlled by a microwave pump signal, generates squeezed microwave states, which are subsequently displaced to form a quantum token. This signal is then transferred to a spin-resonator system engineered to transduce microwave excitations into spin excitations. The quantum properties of the emitted signal from the spin-resonator are assessed using Wigner tomography.

The initial information from the input signal can be stored in the spin memory for the duration of its coherence time and recovered by using a spin echo sequence [128, 134]. Donor states in nuclear spin-depleted ^{28}Si crystals have been extensively studied in this context and possess long relaxation and coherence times at cryogenic temperatures [44, 67, 128, 135]. One of the spin systems considered here is an electron spin ensemble constituted by phosphorus donors. This spin ensemble is hosted by an isotopically purified ^{28}Si host crystal, and has a donor concentration of $[P] = 10^{17}\mathrm{cm}^{-3}$. It is inductively coupled to a planar lumped element superconducting microwave resonator [67, 136]. When the transition frequency of one of the electron spin resonance transitions becomes resonant with the microwave resonator, the corresponding modes can hybridize, resulting in a hybrid resonator-spin system. The Hamiltonian of this system is typically described using the Tavis–Cummings Hamiltonian [67, 137, 138].

Since a Q-token is supposed to consist of multiple individual quantum states drawn from the corresponding codebook, it is important to realize the storage of multiple of those states in the quantum memory. In particular, time-domain multiplexing for the sequential storage of Q-token states using a single spin transition is a suitable approach for its implementation.

Alternatively, spin systems, such as ^{167}Er, offer a rich structure of transitions in the microwave range available already at and close to zero magnetic fields [139, 140]. Often these systems show inhomogeneous broadening, which can be used for storage protocols based on a frequency division multiplexing approach. This scheme allows for the simultaneous storage of individual quantum states and Q-tokens. While the protocol naturally differs from the time-domain storage concept above, the availability of multiple transitions offers access to multi-frequency storage concepts, which necessitate the development of Q-token generation at multiple frequencies.

Recently, we have demonstrated a high-precision microwave spectroscopy of such ensembles [140], proving the possibility of simultaneous access to several spin transitions. First experiments of coherent storage in this broadband regime have already demonstrated a retrieved echo efficiency on the order of 0.1%. While this number is insufficient for practical Q-token storage, it demonstrates the feasibility of this approach.

The successful verification of quantum token storage requires the realization of state estimation or tomography protocols. We perform Wigner tomography of the output microwave signals using a heterodyne detection setup, which is based on the calculation of statistical quadrature moments up to the fourth order and their application for the Gaussian state reconstruction [101, 141]. For signal calibration, we perform Planck spectroscopy [104, 142]. Analyzing the signals with respect to their moments then allow to estimate the output signal variance $\sigma^2_{\mathrm{s,out}}$, which can be translated to a squeezing level of the emitted output signal via $S = -10\log_{10}(\sigma^2_{\mathrm{s,out}}/0.25)$ referenced to the vacuum level. For the Tavis–Cummings system, we can derive that the output variance $\sigma^2_{\mathrm{s,out}}$ is related to the variance $\sigma^2_{\mathrm{s,in}}$ at the input of the resonator-spin system by

$$\sigma^2_{\mathrm{s,out}} = r^2\,\sigma^2_{\mathrm{s,in}} + l^2\,\sigma^2_{\mathrm{l}} + t^2\,\sigma^2_{\mathrm{spin}}, \tag{1}$$

where the complex coefficients r, l, and t describe terms of the Langevin noise operator associated with the reflection from the cavity, the resonator internal losses, and coupling to the spin ensemble, respectively. Here, the variance σ_{I}^2 originates from a thermal bath coupled to the resonator via its internal losses. Similarly, σ_{spin}^2 is associated with a thermal bath formed by the spin ensemble. Initial experiments show coupling rates up to $t = 0.6$, indicating that quantum signals prevail in spin excitations.

The storage of microwave quantum tokens in solid-state spin ensembles will represents an important milestone in quantum technologies in general and for quantum communication and Q-tokens in particular. The combination of tunable Zeeman spin transitions with very long coherence times at GHz frequencies makes these systems a very promising choice for future microwave quantum memories. Experimentally, we have already shown a successful coupling of propagating microwave squeezed states to an ensemble of phosphorus donor atoms embedded in nuclear spin-depleted ^{28}Si crystals [143]. Additionally, we have demonstrated the broadband spectroscopy of rare earth spin ensembles which paves the way toward multi frequency multi-mode Q-token storage using frequency domain multiplexing protocols [140].

It is worth to note that the generation of microwave Q-tokens as well as operation of spin quantum memories typically demands millikelvin temperatures. While this puts boundaries on consumer applications, the use in quantum information processing or the implementation of quantum-LANs connecting multiple superconducting quantum processors is evident due to its technical compatibility. The distribution and storage of unconditional secure Q-tokens is essential for many important concepts such as distributed information processing and for the blind computing paradigm.

4. Long-lived quantum tokens based on rare earth ions

Rare-earth ions (REI) doped in dielectric solids constitute optically addressable spins systems with exceptionally long coherence times for both optical and spin transitions [71]. The spin states can be directly addressed and controlled via narrow optical transitions, enabling deterministic initialization, manipulation, and readout of qubit states. Integration of REI into photonic devices such as cavities has enabled the enhancement of light–matter interactions and gives access also to single ions [70, 144–146] as qubits. Consequently, REI are promising candidates for the core tasks of quantum token protocols: Efficient generation of memory-compatible photonic qubits, their long-lived storage, and efficient state retrieval [147].

REI have been widely used to store photonic qubits in macroscopic ensembles of ions with demonstrations of the longest storage times to date. Storage protocols for ensembles are mostly based on electromagnetically induced transparency (EIT) [148, 149] and AFC [106]. With this, weak coherent pulses have been stored for up to 1 h [88]. One of the key challenges is the combination of long storage time with high storage efficiency and low noise. In this respect, using EIT storage with narrow-band spectral filtering, single photons could be stored for up to 1.3 s [149] with an efficiency of 12.5%. To increase storage capacity, spectral, temporal, and spatial multiplexing has been implemented, and demonstrations have achieved storage in 250 spatio-temporal modes [150], and in 1650 spectro-temporal modes [151]. Figure 6(a) depicts a bulk-doped crystal that typically serves as the platform for such experiments.

Scaling to deterministic, multi-qubit token generation benefits from addressing individual ions. Due to the dipole-forbidden character of the coherent $4f-4f$ transitions in REI, a key requirement is a significant enhancement of light–matter interactions with an optical microcavity. The enhancement is quantified by the coherent cooperativity

$$C = F_{\mathrm{P}}\frac{\gamma_0}{2\gamma}, \tag{2}$$

where $F_{\mathrm{P}} = 3/(4\pi^2) \times Q/V \times \lambda^3$ is the Purcell factor determined by the quality factor Q and the mode volume V of the cavity, γ_0 is the natural excited-state decay rate, and γ the homogeneous linewidth. Nanophotonic and open-access microcavities have achieved Purcell factors up to $F_{\mathrm{P}} = 700$ [144, 152], enabling single-ion detection, state read-out and coherent control [70, 145, 146]. Figure 5(a) shows the cavity-enhanced absorption (or reflection) used to map a photonic qubit onto a single REI, while figure 5(b) details the three-level Λ-system employed for storage and retrieval. Spectral addressing of a chosen ion within an inhomogeneously broadened ensemble is illustrated in figure 5(c). A range of experiments has achieved efficient single ion detection, state readout, and coherent control [70, 144–146]. Single-ion quantum coherence has reached up to 30 ms lifetime [145], and also multi-qubit registers based on spectral multiplexing have been demonstrated [146, 153]. Furthermore, single REI can serve as single photon sources to produce a photon-based quantum token in a memory-compatible

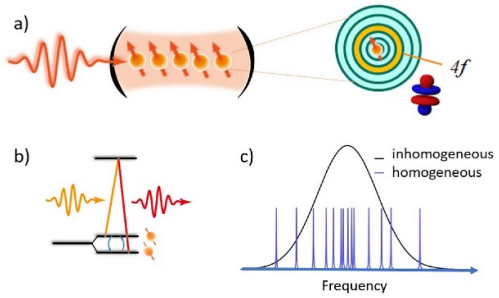

Figure 5. (a) A photonic qubit is stored in a single REI qubit by cavity-enhanced absorption or cavity reflection. (b) Schematic level scheme for the spin-photon interface. (c) Inhomogeneously broadened optical transition (black) with narrow homogeneous linewidths (blue), enabling single- and multi-qubit addressing within a single cavity.

way [144, 146, 154]. Quantum tokens may require transmission over large distance, and, for example, Erbium ions offer suitable telecom transitions coupled to coherent spins [153, 155, 156].

For quantum token storage, it is advantageous to choose long-lived nuclear spin states as qubit levels. Non-Kramers ions with zero effective electron spin have so far shown the longest coherence times. For example, with Pr^{3+}:YSO, coherent storage of up to 1 min was demonstrated [148], and the longest nuclear spin coherence was observed for Eu^{3+}:YSO to date, yielding a hyperfine coherence of up to 18 hours [43], and coherent storage for up to one hour [88]. For these examples, specific magnetic fields are used that lead to a zero first order Zeeman transition (ZEFOZ), which improves coherence by $\sim 10^3-$fold. Additionally, carefully optimized dynamical decoupling sequences are harnessed [157], which can prolong coherence by another factor of $\sim 10^4$. Recent developments on Er^{3+}:$CaWO_4$ [158] and $^{171}Yb^{3+}$:$CaWO_4$ [159] and earlier work on $^{167}Er^{3+}$:YSO [160] show that Kramers ions can achieve second-long coherence.

Efficient coupling of REI to guided or resonant optical modes is essential for both ensemble and single-ion approaches. Nanophotonic waveguides provide strong transverse confinement, and the on-chip geometry offers more possibilities for spatial multiplexing, increase of optical depth, and combination with additional structures such as RF electrodes for spin control. Figure 6(b) shows an example geometry designed by R. Kolesov (unpublished) that optimizes light–matter interaction by an extended waveguide length through a meandering shape. Earlier work has used laser-written waveguides in Y_2SiO_5 crystals [161] or titanium-doped lithium niobate waveguides [162] to demonstrate efficient quantum storage. Integration of REI into micro- and nanophotonic cavities and use of the Purcell effect has enabled enhanced light–matter interactions for small ensembles and single ions, which offer better scaling potential. Figure 6(c) shows an open-access Fabry–Perot microcavity with a REI-doped membrane, which achieves full tunability together with high quality factors and moderately small mode volumes. This approach has enabled Purcell-enhanced spectroscopy of few ions in nanoparticles [69, 163, 164] and single ion detection in nanoparticles and membranes [70, 146]. Even stronger light–matter coupling can be achieved with nanophotonic cavities. Harnessing nanobeam geometries, smallest mode volumes with high quality factors have led to exceptionally large Purcell factors mentioned above [144, 145]. Figure 6(d) shows a design by R. Kolesov [165] that harnesses nanopatterned lithium niobate in a nanobeam photonic crystal geometry with side-wall modulation to realize a cavity. The additional electrodes allow one to tune the cavity resonance frequency, similarly to earlier work on microdisc cavities [154], which allowed single ion detection and fast dynamic resonance frequency tuning.

Coupling REI to cavities is a key aspect for achieving efficient and thus near-deterministic single photon generation in a memory compatible way. The Purcell effect leads to a dominant emission into a cavity mode that can be collected with $> 90\%$ efficiency. Enhancement of the emission furthermore leads to a broadening of the optical transition and can mask spectral diffusion. This has enabled the generation of Fourier-limited photons [166, 167] and the entanglement of quantum memories [168]. Cavity-coupled REI are thus promising to achieve efficient quantum token generation, efficient writing into the memory, and efficient readout.

The quantum token protocol suitable for REI is largely following the original proposal of quantum money [6], and one variant is analyzed in detail in [169]: The issuer of the quantum token produces random photonic quantum states, e.g. time-bin or polarization qubits, and sends the photons—possibly via an optical fiber link—to the customer. The customer receives the photon qubits and stores them in a multi-mode REI quantum memory or a single-ion quantum register coupled to a cavity. For verification,

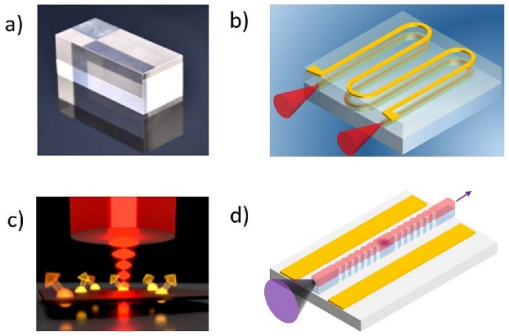

Figure 6. Examples of photonic structures for REI quantum token storage. (a) A doped bulk crystal enabling multiplexed and long-lived storage. (b) Waveguide with integrated RF waveguide (yellow) for spin control. (c) Fiber-based Fabry–Perot microcavity with integrated REI-doped membrane. (d) Nanophotonic cavity based on a Lithium Niobate nanobeam with tuning electrodes and RF waveguide (yellow).

the stored photons are released and measured, and the issuer compares the measurement outcomes with the expected result.

Although REI experiments currently require cryogenic environments (∼1.5 K), highly stabilized lasers, vector magnets and RF control, recent engineering advances have yielded compact rack-mounted platforms that integrate cryogenics, laser locking and microwave electronics. Combined with the photonic integration strategies outlined above, these systems open the way for field-deployable quantum-token nodes that can operate autonomously over long periods.

The confluence of record-breaking nuclear-spin coherence, near-deterministic single-photon generation via Purcell-enhanced cavities, and versatile photonic integration positions REI as a uniquely powerful platform for deterministic, long-lived, and efficiently transmittable quantum tokens. Future work will focus on achieving cooperativities well above unity for single-ion memories, integrating fast electro-optic tuning of cavity and emitter resonances, and demonstrating full end-to-end token protocols—including long-distance verification over deployed fiber networks.

5. Diamond based quantum tokens

The realization of quantum tokens pursued here is an innovative approach based on quantum projection noise of ensembles of nitrogen-vacancy (NV) color centers in diamond [170]. The envisioned device is schematically shown in figure 7(a). The previously developed ensemble-based quantum token protocol enables the implementation of non-copyable tokens containing an ensemble of identically prepared qubits [171, 172]. It can replace, especially in case of ensembles, the conventional copy protection guaranteed by the quantum no-cloning theorem by a protection ensured by quantum projection noise. In the ensemble approach, the quantum projection noise can reveal an undesirable copy operation, since it increases if a hacker tries to make an illegal measurement of the token on a basis different than the one prepared and issued by a bank [171]. In addition, the realization of a quantum token based on single NVs is technologically rather challenging, as high precision in magnetic field alignment is required. The overall security of the protocol has been verified by parallelized brute-force simulations in order to make accurate predictions about the number of ensembles and qubits required on a quantum coin. Advanced attacks on the protocol can assume that measurements can be performed on partial ensembles and that even individual qubits can be measured. Even though such an attack could be considered technically unfeasible, the security of the ensemble-based protocol under these advanced attacks has been proven [172]. Following this approach, we have developed a protocol for designing a specific quantum coin with desired security requirements, as sketched in figure 7(b).

An ensemble-based quantum coin can be realized by fabrication of nanopillars in diamond which will correspond to the individual quantum tokens, each containing an ensemble of NV centers with the same alignment within it, see figure 7(a) [171, 172] .

The electronic spins of the NVs are used as auxiliary qubits, while the nitrogen nuclear spins serve as memory qubits. The number of NV centers in each ensemble should be small enough such that the quantum projection noise is still measurable [171] and can be determined by the diameter of the nanopillars as well as by the density of the created NVs. Ion implantation or delta-doping during diamond growth can be implemented for the creation of NVs with desired density and electron beam

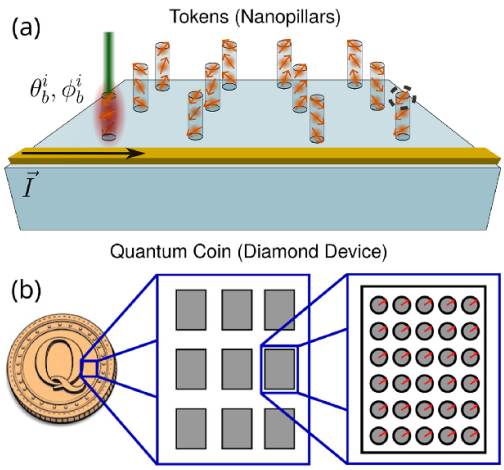

Figure 7. (a) Schematic representation of the diamond-based quantum token. Small ensembles of NVs represent the token and are fabricated in the nano-pillars in order to increase the optical readout efficiency (green line). The NVs electron spins are used for initialization and readout of the quantum information presented by the angles θ_b^i and ϕ_b^i of the spin magnetization on the Bloch sphere. This is realized using radio and microwave pulses and the information is then stored in the nitrogen nuclear spins. The wire is used to apply RF and MW for spin control. (b) The final quantum coin (left) consists of many quantum tokens, where each one has a certain number of nanopillars.

Figure 8. Scheme of the ensemble-based quantum token protocol. A bank generates many quantum tokens with angles θ_b^i and ϕ_b^i in a quantum coin device. The latter is then physically handed to the user, who stores it until authentication by the bank is required, which consists in measuring the tokens in the coin and comparing them with the previously generated angles. The coin is accepted if a minimum number of tokens in the coin above a certain security threshold is measured in the right state. See [171, 172] for more details.

lithography followed by inductively coupled plasma reactive ion etching for fabrication of nanopillars with various diameters [65, 173]. Such photonic nanostructures enhance photon collection efficiency. The NV ensemble in each nanopillar is initialized by a confocal microscope and laser illumination, and the electron spins manipulated by microwave fields in conjunction with static electric fields for addressing and for controlling the charge state of the NV centers. On the other hand, the number of quantum tokens (i.e. of the nanopillars) within a quantum coin should be chosen high enough such that the probability of a hacker to generate accidentally a copy of the quantum coin is arbitrarily small [172], as captured in figure 7(b).

The proposed protocol is schematically presented in figure 8. First, the bank optically initializes the electronic spins of a token and prepares a quantum state by applying resonant microwave pulses. The state is then transferred to the nuclear spins, which have a longer coherence time that can be further extended by dynamic decoupling and charge state control of the NVs. To authenticate the token angles, the bank performs a single-shot readout of the nuclear spin, using the electronic spin as an ancillary qubit. The same protocol, but with different angles, is then applied to all tokens in the coin. This protocol is benchmarked on five IBM quantum processors and a general attack scenario is analyzed, in which the hacker attempts to read the bank token and forge a fake one, based on the information gained from this measurement. It has been experimentally demonstrated that the probability for the bank to erroneously accept a forged coin composed of multiple tokens can reach values below 10^{-22} , while the probability that the bank accepts its own coin is above 0.999 [171].

The main idea behind this practical realization of QT is to store quantum coherence for a certain period of time and then reactivate it so that it can be used in a verification routine. First, coherence is generated on the electron spins in NV centers because they can be easily optically polarized and read out. There the electron spin coherence T_{2e} in this system has a maximum lifetime of 2.4 ms [174] (in

isotopically pure ^{13}C diamond) and cannot be extended due to the strong coupling of the electron spins to magnetic and electrical environmental noise. However, it is possible to transfer the coherent state to neighboring nuclear spins, where it can be stored for several seconds or even minutes. The reason for this is that the magnetic moment of the nuclear spins is three orders of magnitude smaller than that of the electron spins. This quantum memory can be realized in diamond with the intrinsic nuclear spins to NV centers ^{14}N ($I = 1$) or ^{15}N ($I = 1/2$) or using carbon nuclei with ^{13}C ($I = 1/2$). The main challenge here is to develop a method that allows for fast coherence transfer, compared to the electron spin coherence time and without losses to the quantum memory. Coherence can also be generated directly on the nuclear spins using radio frequency pulses and transferred to the electron spins via a (back) swap gate and later read out optically. For this purpose, the nuclear spins are first initialized (polarized) via the NV centers.

The nuclear spin coherence time T_{2n} is limited by magnetic interaction with spins of the same type and also by coupling to different electron spins (NV centers, P1 centers, other paramagnetic defects) in the diamond crystal. In order to extend the lifetime of the stored coherence state, which would lead to a longer storage time for the quantum tokens, the nuclear spins must be decoupled from the environment. The goal of decoupling protocols (also known as dynamical decoupling [175]) is to suppress certain terms in the magnetic dipole-dipole interaction and, depending on the application, they can suppress the coupling between the same spins (homogeneous decoupling, e.g. MREV [73]) or the coupling to other spins (heterogeneous decoupling, e.g. CPMG [176] or XY8 [175]).

The application scenario we are envisioning is a diamond-based portable quantum token that can be miniaturized and equipped with integrated photonic structures and microwave electronics. This can generate dynamic decoupling pulses during transport, which allows nuclear spins to be optimally decoupled from electron spins. The current state of the art with integrated photonic chips in combination with the microwave electronics found in mobile phones would allow in the near future an ensemble-based quantum token to be integrated into an ID card, for example. The bank would then be a system at border control. This would allow transit at the airport to be checked with a built-in expiration date. By transmitting secretly the alignment parameters of the quantum tokens (the angles θ_b^i and ϕ_b^i), it would also be possible to check the token at another local position.

The main limitation currently are the coherence times of the nuclear spins in diamond. Although they can reach values of several seconds even at room temperature [73], this is still orders of magnitude shorter compared to what would be required for a practical implementation. However, since the ensemble based quantum token protocol is hardware agnostic, it could be easily adapted to other promising physical systems like trapped ions with coherence times exceeding 1 hour [53] and cold atoms with coherence times up to 20 s [177]. However, the miniaturization of the physical devices is still a challenge due to the required complex experimental setups, like vacuum chambers.

6. Quantum token architecture based on hybrid quantum photonics

^{13}C nuclear spins in diamond are excellent candidates for quantum memories due to their good isolation from the environment. The weak interaction with the environment results in long storage times, known to be capable of storing information on the timescale of seconds [73]. At the same time, the quantum memory needs to be accessed and, ideally, interfaced with photons to enable the information exchange over long distance. Strongly coupled spins, including ^{13}C nuclear spins, have been detected with sub-megahertz resolution in nanodiamonds (ND) [178]. The control of strongly-coupled ^{13}C has been demonstrated via a nearby SiV center [72], with further improved sensitivity due to modified electron-phonon coupling in NDs [179], as well as due to large strain [72]. Thereby, three coherent processes are established, which enable the exchange of quantum information between long-lived quantum memories and information transmission over long distances. As depicted in figure 9 the electronic spin of the SiV center connects to photons via the optical dipole moment (here transition C). Hyperfine coupling between the SiV centers electron spin and ^{13}C nuclear spin states enables to mediate coherent interactions to the memory unit. All three qubits, the optical dipole (qubit 1), the electron spin (qubit 2) and the nuclear spin (qubit 3) are coherently controlled. The coherent control rates of the optical dipole was realized with a Rabi-frequency of about 1 GHz, see figure 9(b). The coherent control of the SiV's electron spin was realized at microwave frequencies with a Rabi frequency of about 10 MHz, see figure 9(c). The hyperfine coupling to the nuclear spin environment was investigated for a large variation of coupling strengths depending on the relative position and orientation of the spins [178]. For the three qubit system discussed above, the hyperfine coupling strength of $A_{\|}/2\pi = 621.8\,\mathrm{kHz}$ was resolved by means of electron Ramsey measurements, see figure 9(d) to a nearby ^{13}C nuclear spin.

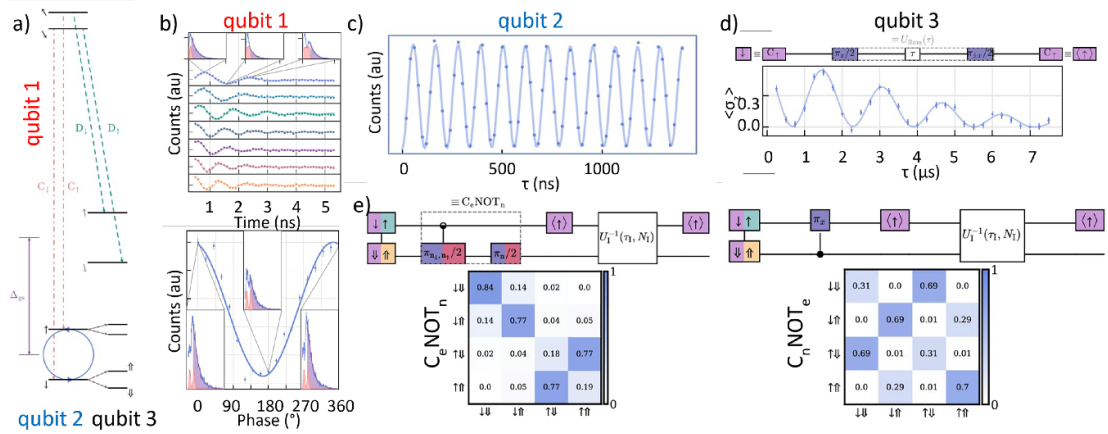

Figure 9. Coherent control of the three qubits[*]. (a) Schematic of the level scheme. The optical dipole of transition C is connected to the SiV's electron spin state. Hyperfine-coupling to nearby nuclear spins splits the electron spin level. (b) Coherent amplitude and phase control of the optical dipole with Rabi-frequencies of about 1 GHz. (c) Coherent, microwave-based electron spin control is demonstrated with a Rabi frequency of about 10 MHz. (d) The coupling to nearby nuclear spins is revealed by electron Ramsey measurement, here with a coupling strength of $A_{\|}/2\pi = 621.8$ kHz. (e) Electron-mediated nuclear spin control. Amplitude transfer matrix of a C_eNOT_n and C_nNOT_e gate with the corresponding fidelities.

[*] (a)–(e) Reproduced from [178]. CC BY 4.0.

For the exchange of quantum information respective gatter-operations need to be constructed, between the different qubit systems. As an example, the amplitudes of the gatter's transfer matrix for the two CNOT-gates between electron spin and nuclear spin, C_eNOT_n and C_nNOT_e, with the respective fidelities are depicted in figure 9(e).

The three-qubit unit is realized in a ND with sizes typically below 100 nm. Since the spatial expansion is small compared to the optical wavelength the NDs can be integrated into photonic platforms by means of AFM-based nanomanipulation, realizing efficient coupling between the optical dipole and an optical mode, which is defined by the photonic structure. The quantum unit can be incorporated in a variety of photonic platforms. As a promising material platform, we developed Si_3N_4 chip technology with predefined interaction zones and optimized it for its use in the quantum regime [180]. An example is the strong background fluorescence in Si_3N_4, originating from green laser illumination, which was a known limitation for the use of quantum signals in Si_3N_4 devices. The developed pump-probe design in a crossed-waveguide architecture enabled a suppression of background signal by 20 dB [181]. Integrated, 1D photonic crystal cavities (PCC) enable an efficient interface between the optical dipole of the SiV center and a single waveguide mode by means of Purcell enhancement [181, 182]. 3D-printed coupler build an efficient optical interface to Gaussian, free-space optics and electrodes, microawave- and RF-structures as well as microheaters enable the complete on-chip control of the spin system, as illustrated in figure 10(a).

The quantum post-processing is based on AFM-nanomanipulation and, besides the positioning with nanometer accuracy, enables the control of all degrees of freedom of the optical coupling to individual PCC modes [183]. As depicted in figure 10(b), the quantum post-processing enables the optimization of the hybrid device directly by evaluating the optical Rabi oscillations, while the position and the dipole orientation of selected SiV centers is repeatedly optimized with respect to the overlap with the optical mode. Here, the optical Rabi frequency was increased to about 2.7 GHz. As a result of the enhanced light–matter interaction the corresponding optical transition spectrally broadens. For such spectrally broadened transition, optical access to the electron spin states becomes more efficient [184] and the integrated quantum memory units can be accessed on-chip. The resulting hybrid devices combine advantages of an industry-relevant photonics platform, such as Si_3N_4, with individually optimized quantum systems enabling full on-chip control under relaxed experimental conditions.

Quantum token protocols involve entanglement distribution based on time- or frequency-binned spin-photon entangled states [185]. The optical dipole of a single SiV center is the interface to single photons at a wavelength of about 737 nm. These single photons have shown to be indistinguishable, even for SiV center in seperate NDs [186]. A low-noise yet highly efficient quantum FC into the telecom frequency band, such as the telecom C-band, can be adapted in a modular way [187] and is required for long-distance information exchange via established fiber networks [188]. The electron spin coherence needs to be long enough to exchange quantum information with the ^{13}C nuclear spin quantum

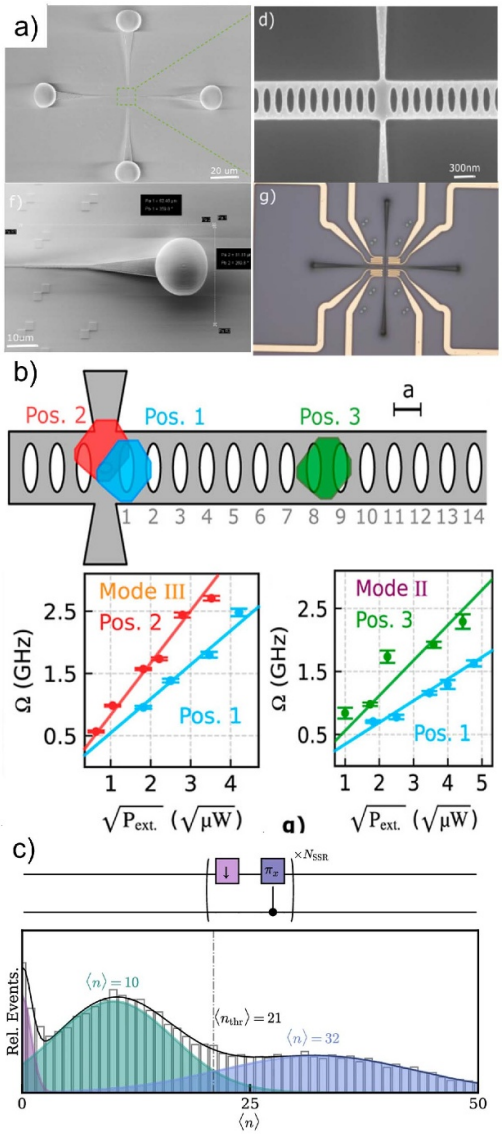

Figure 10. Hybrid Quantum Photonics. (a) Si_3N_4-photonics was optimized for its use in the quantum regime including waveguides, photonic crystal cavities with predefined interaction zones, 3D couplers and electronic infrastructure. (b)* AFM-based quantum postprocessing enables the optimization of all degrees of freedom of the optical coupling while in-situ monitoring the hybrid systems' performance by means of maximizing the optical Rabi frequency (here shown depending on the ND's position within the photonic crystal cavities mode). Reproduced from [187]. CC BY 4.0. (c)** Photon statistics obtained from a 3 ms long single-shot readout sequence with a separation in the mean photon number between the bright state $n = 32$ and dark state $n = 10$, enables to compensate limitations in the initialization process.
* (b) Reproduced from [183]. CC BY 4.0.
** (c) Reproduced from [178]. CC BY 4.0.

memory, which has been demonstrated in above mentioned references. The demonstrated realization established nuclear spin initialization and readout as well as relevant gatter operations via the SiV's electron spin in a ND. The electron spin coherence time is extended to 273 μs at 4 K by applying dynamical decoupling sequences [72]. A large ground-state splitting reduces phonon-induced electron spin decoherence. The prolonged electron spin coherence enables to address individual ^{13}C nuclear spins via indirect electron spin control. The protocols are implemented starting with the initialization of the electron spin state. Using rotations on the electron spin in conjunction with electron-mediated nuclear rotations enables to construct initialization gates, which transfers the electron spin's population onto the target nuclear spin. A target nuclear spin initialization between 0.647 and 0.682 was achieved, which is limited by the imperfections of the electron spin initialization fidelity. Based on the spin initialization together with conditional and unconditional rotations C_eNOT_n gates as well as C_nNOT_e gates were implemented, as depicted in figure 9(e). Again, the electron initialization fidelity of about 0.84 limits the gate fidelity which itself is well above 0.9. Imperfect nuclear spin initialization can be overcome by implementing single shot readout of the nuclear spin state. A clear separation of the mean photon

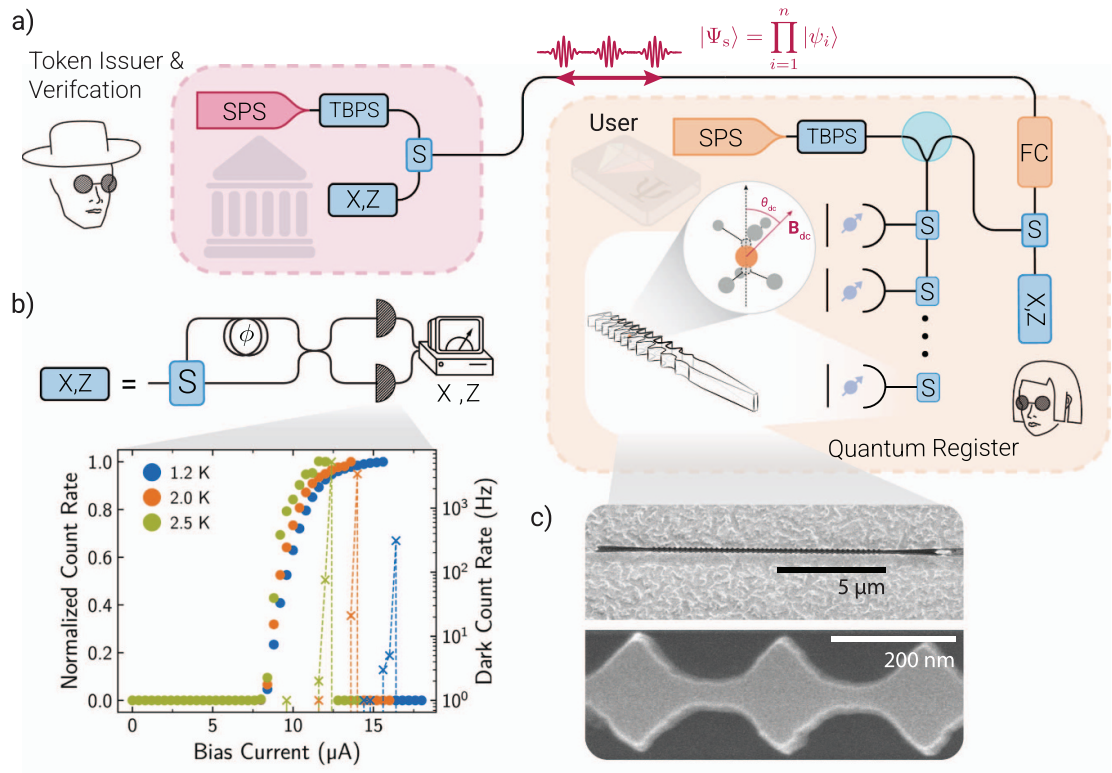

Figure 11. (a) The SnV enabled quantum token scheme encompasses token creation, storage, retrieval, and verification. The issuer generates a quantum token $|\psi_s\rangle$ with a unique serial number s, composed of photonic qubits $|\psi_i\rangle$ prepared via a single-photon source (SPS) and time-bin qubit preparation stage (TBPS) [202–204]. Photons are encoded in the desired states and transmitted in the infrared, requiring frequency conversion (FC) only at the user end for G4V interaction. Users store the token in a high-efficiency sawfish spin-photon interface array [191, 192], using electronic or nuclear ^{13}C spin. Fast switches (S) enable efficient routing and X/Z-basis measurements, with the X-basis implemented via a switch-integrated imbalanced Mach–Zehnder interferometer with controllable phase ϕ. Storage completes after sequential X-basis measurements. For retrieval, the spin state is entangled with an SPS photon sent to the verifier; a Z-basis spin measurement follows. (a) Reproduced from [169]. CC BY 4.0. (b) Normalized count rates of a SNSPD illuminated with 780 nm laser light operated at different temperatures. The count rate is saturating toward unity with the bias current approaching the critical current of for lower operating temperatures. Reproduced from [193]. CC BY 4.0. (c) Fabricated sawfish resonator in diamond. Reproduced from [192]. CC BY 4.0.

number between both nuclear spin state of $n = 32$ for the bright state and $n = 10$ for the dark state, as shown in figure 10(c), results in a discrimination between both nuclear spin states with fidelities of $F_{\text{bright}} = 0.935$ and $F_{\text{dark}} = 0.824$.

Since the ND host can be integrated in conventional photonics, a potentially higher photon-collection efficiency enables single-shot readout on the electron spin, which circumvents remaining limitations of the electron spin initialization fidelity. Increasing the cooperativity of the hybrid quantum photonics systems makes spin-dependent reflectivity accessible which can be utilized for further protocol development [189] . Additionally, combining an ancillary nuclear spin with single-shot readout and a subsequent SWAP gatter operation can also improve electron spin initialization. An extension to quantum register consisting of multiple ^{13}C nuclear spins [190] enables fault-tolerance in the storage of quantum information. Extending the system to more than one nuclear spin further increase the complexity of applicable protocols. Finally, it is worth mentioning that these results neither required a vector magnet nor a dilution refrigerator, which enables to realize a simpler version table-top experiment with lower technical overhead and thus positively affects scalability concerns.

7. Quantum tokens based on color centers in diamonds

The token implementation we pursue is based on Wiesner's seminal quantum money protocol [6]. Specifically, we studied the generation, storage, and retrieval of Wiesner quantum money states, where storage and retrieval are accomplished through an integrated and highly efficient spin-photon interface [191, 192], as well as integrated superconducting nanowire single-photon detectors (SNSPDs) [193–198]. The token scheme was explained in detail by Strocka *et al* [169], from which we adapted figure 11. To date, a full implementation of such a message and retrieve token scheme has not yet been achieved with

solid state quantum memories, with a recent demonstration [199] implemented with cold atoms. In this work, we consider the SnV as a quantum memory, which is a group-IV vacancy center (G4V) in diamond. G4Vs include the silicon vacancy (SiV), germanium vacancy (GeV), tin vacancy (SnV), and lead vacancy (PbV). G4Vs in diamond form inversion-symmetric defects with D_3d symmetry, where the dopant atom occupies an interstitial site between two vacancies. This high symmetry strongly suppresses sensitivity to electric-field noise compared to the NV center, making G4Vs ideal for integration into nanostructures where surface charge fluctuations can be significant [62, 200, 201].

The token protocol we adapted begins with the creation of a Wiesner quantum money state by a token issuer, as depicted in figure 11. With the aid of a SPS and a time-bin qubit preparation stage [202–204], the token state $|\Psi_s\rangle = \prod_{i=1}^{n} |\psi_i\rangle$ is produced through the successive emission of single photons, thus utilizing TDM. Here, n denotes the number of photonic qubits, and each $|\psi_i\rangle$ is selected uniformly at random from the set of time-bin qubits $|E\rangle, |L\rangle, (|E\rangle + |L\rangle)/\sqrt{2}, (|E\rangle - |L\rangle)/\sqrt{2}$, where $|E\rangle$ ($|L\rangle$) represents the early (late) time-bin state. Each token state is uniquely identified by a serial number s. Time-bin encoding is chosen for this project because it is particularly well-suited to the storage and retrieval protocols developed for G4Vs [189, 206–208]. When single photons are generated directly in the telecom band [209–211], only a single FC stage is needed at the quantum memory node to translate them to a frequency compatible with the G4Vs. Conversion from the visible and near infrared to the telecom spectral range can be readily achieved with quantum FC systems [187, 212–216]. Through a series of routing operations, spin-photon cavity reflections, control operations, and photon detection events, the photons of the token state that survive transmission are stored in the memory register with high fidelity [169]. During storage, the token can be processed using the noise-tolerant quantum retrieval game approach [18] to verify and spend it. Alternatively, the state can be returned to the issuer or sent to a trusted verifier. In Strocka *et al* [169], we investigated the latter to demonstrate the versatility of the quantum register. The retrieval of the state is performed using an inverse protocol that requires another SPS, which creates single photons that are reflected off the spin-cavity systems. Notably, through heralded storage, more complex quantum states [217] can, in principle, be both stored and generated [218], such that this memory architecture is not limited to product states.

We focus on the SnV as a quantum memory, exploiting both its electronic spin and nearby ^{13}C nuclear spins. More generally, the negatively charged G4Vs are optically active, effective spin-1/2 systems with zero-phonon-line transitions at 520 nm (PbV) [219], 619 nm (SnV) [220], 602 nm (GeV) [221], and 737 nm (SiV) [221]. When coupled to a nanophotonic crystal cavity, their optically accessible spins provide an efficient and integrable quantum-memory platform [191, 192]. Photons can be stored in such a memory using two main approaches. The first is approach uses amplitude gates [189, 206, 208], which generate intermittent entanglement through spin-dependent reflection of incident time-bin photons combined with a spin control operation. The second approach involves controlled-phase gates [207, 218], which rely on a spin coupled to a one-sided open cavity, a single control operation, and a spin-dependent phase shift upon reflection. In the QPIS project we target the second method because it is not limited to 50% efficiency. Such a limit would break the token schemes security threshold for noise tolerance [18, 222]. For both methods the storage of a state is heralded by detecting the reflected time-bin qubits with a measurement device. Such a device also has to operate at near unity efficiency to guarantee a successful implementation of the protocol. Once the storage of a qubit is heralded, the electronic spin state can be swapped onto a nearby nuclear ^{13}C spin [74, 75] for storage exceeding 17 ms [74]. The color centers that had the highest priority for us were SnVs [76, 223], which have the additional benefit of being sufficiently spin-coherent in the Kelvin range, due to their comparatively large spin–orbit splitting [63, 224].

For control of the memory and the creation of time-bin qubits, all-optical approaches have been analyzed both experimentally and theoretically [169, 225–227]. In particular, a highly efficient microwave control scheme was developed and analyzed, exploiting the orientation of the magnetic control field [228]. Theoretical analysis revealed that, for both microwave and optical control, the fidelity of the spin gates can exceed 99% [169, 228].

For the integrated routing of photons, which is required for scaling the G4V platform to multiple spin-coupled cavities, a new platform was developed [205] (figure 12(c)). The detection that concludes the heralding requires highly efficient detectors, which in QPIS are based on integratable SNSPDs [193–198](figure 12(a)).

Finally, the most central component of the scheme is the spin-photon interface. In QPIS, we base this interface on the sawfish nanophotonic crystal resonator, which, through its amplitude-modulated external corrugations, overcomes a fabrication challenge related to the adiabatic coupling of a resonator mode to a waveguide [191, 192] (figures 12(b) and (c)).

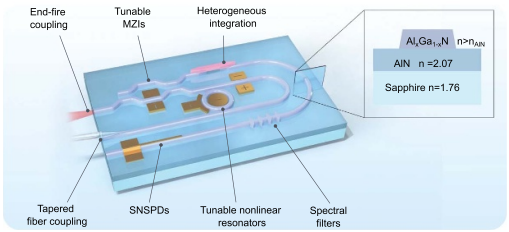

Figure 12. AlGaN/AlN heterostructures for all the functionalities required for routing and switching photons. Reproduced from [205]. CC BY 4.0.

All these components are critical for the functioning of the scheme and were specifically developed and chosen for the QPIS project to aim at the most efficient nanophotonic operation of the targeted quantum memory.

As of now, G4Vs have demonstrated storage times ranging from 20 ms for the electronic spin of a germanium vacancy (GeV) [229] to up to 18 s for a nuclear ^{13}C spin coupled to the defect [230]. Achieving long coherence times with the GeV required millikelvin temperatures, which is a constraint expected to be less stringent for heavier G4Vs, such as tin and lead vacancies [224]. Although these are record storage times for optically accessible solid-state spins, such storage times are too short for a realistic quantum money scheme, which would ideally hold token states indefinitely. However, signature schemes that allow an issuer to send a limited number of tokens, which an autonomous agent can use to sign a restricted set of instructions, for example steering commands in a satellite between base stations, could still be enabled by such short storage times [231].

8. Room-temperature quantum token based on alkali metals and noble gases

Storing photonic quantum states for several minutes, hours, or even up to days under ambient conditions is hardly addressed in science, but a central challenge for the realization of practical quantum tokens. Quantum memories based on mixtures of alkali metal and noble gas atoms in atomic vapor cells can address this challenge with the aim of ideally extending the storage time into the hour range. At the same time, this approach implements a robust and technological simple overall system. The solution discussed here consists of storing optical signals into an electron spin wave in the alkali metal ground state and the subsequent coherent transfer of the spin wave to nuclear spins of noble gas atoms with very long coherence times. This allows us to profit from the efficient quantum optical interface of alkali metal atoms and at the same time the exceptionally long coherence time of noble gas spins, as they are well protected from the environment.

Using the optical interface of alkali metal atoms, single photons or weak coherent states can be stored in a phase coherent fashion [81, 82]. Naturally, this can be extended to the storage of polarization states in a quantum superposition [83], which renders these memory systems very flexibly in terms of encoding basis and continuous as well as discrete variable protocols can potentially be implemented. The acceptance band of alkaline memories is naturally limited to the optical transitions of alkali metal atoms. Most prominent are the D_1-lines of cesium and rubidium at 894 nm and 795 nm, respectively. Alternative options comprise the D_2 lines, or transitions to higher orbital angular momentum states such that a variety of near-infrared to the telecommunication C-band can be used [232–234]. Suited signal bandwidths range from few MHz up to the GHz regime, which allow for fast writing of quantum information into the memory. As sources of quantum token bits, weak coherent states or single photons can be used. While the former can be conveniently generated by attenuated lasers, the latter can be generated by semiconductor quantum dots, molecules, cavity-enhanced spontaneous parametric conversion [235] or four-wave-mixing in the same alkali metal species [236]. In both, recent experimental progress allowed first proof of concept experiments [82, 232, 237, 238].

The storage inside a ground state spin-wave is commonly limited by experimental factors, such as the spin-decoherence due to atomic collisions with the walls of the cell. Another disadvantageous process is the diffusion of atoms out of the optical probing region. Subsequently, storage times on the single photons level have been limited to the millisecond range but have been extended in the single-digit second range with coherent pulses and other measurement schemes. The direct storage of quantum information in nuclear spins of a noble gas would therefore be an interesting alternative. The research on

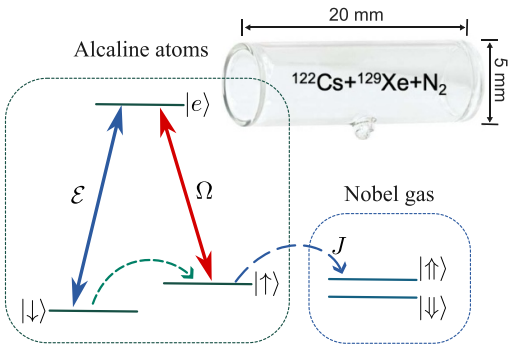

Figure 13. Visualization of the spin-exchange quantum memory scheme and an atomic vapor cell with filling of ^{133}Cs, ^{129}Xe with nuclear spin 1/2 and N_2 for fluorescence quenching. Initially, all alkali metal and noble atoms are prepared into the states $|\downarrow\rangle$ and $|\Downarrow\rangle$, respectively. A Photonic quantum state $\mathcal{E}$ and strong classical control field Ω induce a two photon transition between the alkaline ground states $|\downarrow\rangle$ and $|\uparrow\rangle$. When the noble gas spin is tuned in resonance by a magnetic field, the spin exchange collisions will lead to the strong coupling J, such that a coherent spin transfer to the noble gas can be achieved. For readout the process is reversed and the photonic quantum state is retrieved.

the nuclear magnetic properties has been extensively performed on ideal spin systems such as ^{3}He, ^{129}Xe (both spins of 1/2), or ^{21}Ne (spin 3/2). Unfortunately, a direct optical access to these systems is extraordinary hard [239]. Therefore, mediation by another species is needed for the polarization and optical read-out. Polarization of noble-gas spins is performed by spin-exchange optical pumping [240] for all rare gases. As the quantum information is stored in the form of single photons into the alkali part of the memory, an effective transition from the alkali ensemble toward the noble-gas ensemble is required. Such spin-exchange experiments have been carried out in the past decades [241]. Novel developments, which enhance the exchange toward strong coupling, have been performed recently [242], and enable an effective interface for noble-gas atoms toward the storage of quantum information into the memory.

Photon storage in alkali metal vapors at near room temperature is particularly appealing, as it requires neither complex cooling mechanisms nor large magnetic fields. In alkaline Λ-type memories, a single photon is mapped to a spin wave $|s\rangle = \sum_j e^{i\Delta k r_j} |\downarrow_1, .., \uparrow_j, \downarrow_N\rangle$, i.e. a coherent macroscopic superposition of all N atoms

The maturity of such memories has been continuously improved since the first demonstrations of memories based on EIT in the early 2000s [243]. In the past decade this development of quantum memory implementations in alkaline vapor gained remarkable momentum; reviews can be found in [244–246]. Here we will summarize a few highlights: the efficiency of a room-temperature EIT-like memory was pushed beyond 80%, by control pulse optimization [247, 248]; EIT-like quantum memories reached $\approx$ 1 GHz bandwidths [81]; storage of polarization states with more than 90% fidelity has been shown [83, 238]. We reduced the read-out noise of the memory considerably [59], which allowed single photon storage and retrieval for the first time in a ground-state vapor cell memory, with an photon–photon correlation function of $g^{(2)}(0) = 0.177(23)$. This testifies the quantum character of the light recovered [82]. We demonstrated a multiplexed random-access optical memory that allowed for storage and retrieval of several independent signals [61], which shows the potential to store large amounts of photonic quantum states. Moreover, these memories were readily integrated into a standalone mobile system [60, 249], and we developed simulation tools for accurate performance estimation [250]. Despite being a macroscopic superposition state, the spin wave exhibits a comparatively long coherence time, ranging from few μs to several ms [121]. To extend that into the regime of several minutes to hours, it was proposed by [84] to use strong coupling to noble gas spins during spin exchange collisions [241], alike sketched in figure 13. The ability to transfer the spin state from the alkali spin ensemble back and forth to the noble gas spins was also demonstrated just recently [242], where hour long coherence times in the ^{3}He noble gas ensemble were observed, also attainable in ^{129}Xe [120]. Such a room-temperature quantum memory, based on alkalies and noble gases, could be implemented in small spectroscopy cells (see figure 13) and would have the advantages of (i) continuous room-temperature operation, (ii) up to hour-long storage times, (iii) optical interface at the single-photon level, and (iv) ability of miniaturization & transportability.

A quantum token based on alkali atoms and noble gases will be suitable for numerous applications. The quantum money protocol from [18] can be implemented. For this purpose, the legitimates issuer (bank) generates a large scale of randomly selected Wiesner-type quantum states ordered in pairs and transfers them to the customer as a quantum token, which corresponds to a certain amount of money,

via a fiber-optic interface. The customer stores these in a transportable, multimodal quantum memory. The customer can then hand over the stored quantum token to a legitimate receiver (retailer) for payment. The retailer carries out measurements on the quantum token (challenges) and sends the results to the bank for authentication. If authentication is successful, the bank authorizes the quantum token as genuine and transfers the corresponding amount of money to the merchant's account. Another exciting use case is client-server identification using quantum PUF (qPUF). This application requires a secure identification protocol between the communicating parties to ensure a secure data exchange as outlined in [251]. Potential limitations to these application scenarios are that the process is so far limited to the usual alkali metal wavelengths, bulky magnetic shielding is required to suppress external field fluctuations. The number of required stored states for a token could increase due to noise/low fidelity, the robustness of the transmission of the spin wave from the alkali to the noble gas ensemble still needs to be experimentally demonstrated as well as the scalability. As the quantum superposition is linked to the internal states of freedom and a holding magnetic field is likely required, the quantum memory needs to be shielded within a homogeneous magnetic field from the environment. Magnetic disturbances and magnetic inhomogeneities would likely limit the stored quantum information. Moreover, a cross-talk to rotational sensing (gyroscopy) might be of interest. In effect, the memory can also act as an atomic gyroscope, and the relative orientation of the memory against the storage frame of reference will be required.

In summary, when these technical hurdles are overcome, atomic ensemble memories offer a unique potential for real-world applications due to there long coherence times and robust room-temperature operation.

9. qPUFs and quantum tokens

Authentication, the act of proving one's identity, has been a cornerstone of human society over centuries. It is expressed via objects such as keys and seals, via capabilities like signatures or via secrets, like passwords. Over the past decades, it has become a field of intense research in cryptography and is present in everyday-life via passwords, fingerprint scanners, signatures and personal identification numbers (PINs). Taking the way in which an ordinary key works as an example, identity may be proven by a lock in a simple way via the possession of a key: If a lock accepts only one key, then the person holding that key proves its identity by being able to open the lock. The lock then serves as mechanism that probes the key and, based on the response, either opens or stays closed. Such a mechanism which is able to verify the identity of a key is called a verifier. Due to its immense importance, cryptography has made strong attempts of quantifying the level of security provided by an authentication method. While from technological perspective, the concept of identity may even be associated with a certain physical state of the human brain, in which the password or PIN is stored, the security of an authentication method is hard to quantify at this level. Rather, the security of such methods is analyzed in terms of the mathematical complexity of breaking them and of the physical security of the involved actions or devices. The second approach replicates more closely the mechanism underlying present-day PUFs [35].

PUFs are hardware security primitives that exploit inherent, uncontrollable random physical variations introduced during the manufacturing process. These variations are practically impossible to replicate—even by the original manufacturer—making PUFs a powerful tool for authentication and key generation [252, 253]. The behavior of a PUF is commonly characterized by a set of challenge-response pairs (CRPs): for a given input challenge, the PUF produces a unique and unpredictable output response. Security relies on the assumption that, due to the underlying randomness, it is computationally infeasible to predict the correct response for an unseen challenge, even when a large number of CRPs are known [254]. Therefore a PUF can be authenticated via the pre-stored CRPs.

Despite their promise as lightweight hardware-security primitives, classical PUFs remain vulnerable to both modeling and physical attacks. Machine-learning and deep-learning modeling attacks collect CRPs and train a predictor that reproduces the PUF's input–output behavior on previously unseen challenges, effectively yielding a software clone [255–257]. Complementarily, side-channel attacks exploit the physical leakage produced during response evaluation, most notably the power consumption or response-evaluation timing correlated with the device's internal delays [258], or localized electromagnetic probing that resolves the switching activity of individual sub-circuits [259, 260]. Hybrid attacks that feed this side-channel leakage into the learning algorithm are particularly potent [261, 262]: the additional structural side information collapses the attack complexity from exponential to polynomial in the number of XOR chains and the challenge bit-length [258], and can further enable cross-PUF attacks in which one

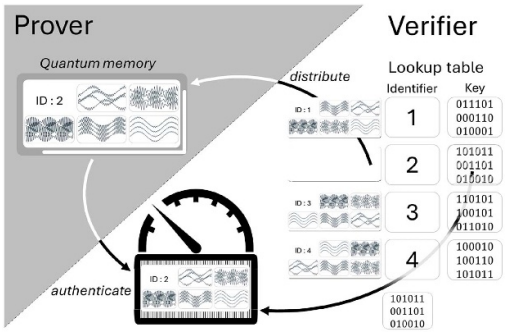

Figure 14. qPUF-based authentication scheme. The authentication protocol consists of two stages: token generation and token verification. During token generation, the verifier generates a quantum token together with a classical identifier bitstring. The quantum token is stored in the verifier's quantum memory, while the identifier bitstring and the qPUF device are given to the prover. During verification, the prover inputs the identifier bitstring into the qPUF, which acts as a classical-to-quantum random map, and obtains the corresponding quantum token. The prover sends this token back to the verifier, who compares it with the stored token using a SWAP test. Authentication succeeds if the two quantum states match, and fails otherwise. It was proved in [217] that a computationally bounded adversary with query access to the qPUF device cannot reproduce the quantum state corresponding to an arbitrary classical identifier bitstring for which they have not previously sampled the qPUF output.

device is modeled from the side-channel traces of another. To precisely understand the ultimate security limits of the PUF concept, recent work started to formalize it from a quantum theory perspective. Since the no-cloning property of unknown quantum states indicates that the *unclonability* of a PUF may actually be turned into a proven feature resting on physical theories rather than an empirically justified assumption, and first implementations are being attempted [263].

Currently, two principal research directions can be clearly distinguished in the literature: The first one contains quantum tokens and QR-PUFs, the second one the so-called qPUFs. The concept of a quantum token is based on Wiesner's conjugate coding scheme [6], while the so-called QR-PUFs were introduced in [264]. The work [264] made no reference to [6], but from a theoretical perspective both approaches share important construction principles. One of these is the underlying idea of utilizing, as a means of authentication of the prover, a physical system that is *unclonable*. While this property follows from the no-cloning property in the case of quantum tokens, it is an assumption in [264]. Further, both QR-PUFs and quantum tokens utilize classical information or lookup tables (also called *trusted enrollment data*) at the verifier. This information can in principle be copied, as it is not protected by the no-cloning principle.

An authentication scheme following the concept of conjugate coding is depicted in figure 14. The alternative realization following the exposition in [264] is captured therein by assuming the measurement is realized based on the injection of quantum states, which are themselves generated based on classical information stored in the lookup table.

In contrast, qPUFs (that were introduced in [36], see figure 15), can be operated solely on the basis of quantum information at the verifier's side—no such memory is *a priori* needed at the prover [265]. However, for qPUFs only the hardness of cloning the hardware in possession of the prover is proven within a formal hardware model, thereby enabling information-theoretic security statements. We thus observe two design approaches with different security assumptions or properties, and pronounced differences in the design challenges.

Two types of attacks on qPUFs are considered: A first attack models an adversary trying to get hold of the table of queries and responses. Since the responses of a qPUF may be obtained as quantum states, the no-cloning theorem forbids an attacker to create a copy of the query and response table. Rather, such an attacker must steal the entire table, which may be noticed by the verifier. Further, qPUFs are designed to withstand a specific type of cloning attack where the attacker gets hold of the qPUF and creates their own table of query and response table before returning the qPUF to its legitimate user to avoid detection of the attack: As has been proven in recent work [217], any such effort will require a significant amount of resources.

qPUFs have recently gained significant attention as a foundation for secure authentication, storage, and identification in next-generation communication systems [266, 267]. Leveraging the quantum no-cloning principle and the inherent randomness of physical quantum systems, qPUFs offer a promising path toward robust cryptographic primitives that can withstand even quantum adversaries. One line of research introduces a qPUF-based approach for secure authentication protocols [268]. In

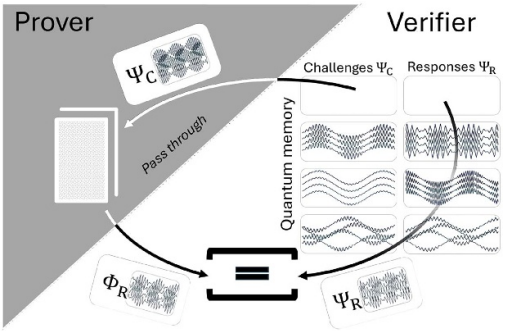

Figure 15. Authentication scheme based on qPUFs [217]. Both Ψ_C and Ψ_R are generated at the time where the authentication takes place based on pre-stored entangled states.

these schemes, the unique quantum response of a device to a given input challenge enables reliable and unclonable identity verification. The protocol design ensures that even an adversary with partial knowledge of challenge-response behavior cannot predict new responses, thanks to quantum principles and non-replicability of the physical device.

Extending this concept, several works have investigated the application of qPUFs to secure data storage and identification systems [269–271]. The work shows how each device's quantum response can serve as a robust and physically bound identifier or secure storage primitive. These applications are particularly relevant in distributed systems where hardware-level trust anchors are essential.

A further development combines qPUF-based key generation and secure storage in the presence of side information [272]. Here, side information might originate from environmental noise or partial leakage to an adversary. The proposed framework demonstrates how secret keys can still be reliably extracted while ensuring provable security, even in the presence of such information.

These implementations build upon a comprehensive theoretical foundation that quantifies the information-theoretic properties of qPUFs [273]. This work provides detailed entropy bounds and uniqueness guarantees, showing that qPUFs can generate high-quality randomness suitable for cryptographic use and discusses trade-offs between robustness and key reproducibility.

A complementary approach investigates secret key generation and storage mechanisms purely based on qPUFs [274, 275]. These works consider scenarios with practical constraints such as noisy quantum measurements and device variations. It proposes strategies to mitigate error effects while maintaining security.

Potential applications of qPUFs in the internet of things (IoT) are examined in another study [276]. It highlights the suitability of qPUFs for decentralized, low-power devices where conventional cryptographic methods may be infeasible. This line of work opens new avenues for integrating quantum security primitives into embedded systems and edge computing environments.

In [277] an authenticated QKD protocol using maximally entangled qubit pairs that secures BB84 under minimal assumptions was presented. The protocol enables secret-key expansion through reuse of pre-shared information. In noisy conditions, simulations with cavity-enhanced atomic frequency comb memories show that both statistical methods and trained DNNs can detect adversaries with over 80% accuracy at 150 μs memory time and 1 m distance.

Two patents were submitted describing practical qPUF-based security systems. They outline a method for securely storing and retrieving data messages in a memory device using physical identification mechanisms [278], and techniques for securely enrolling data into a device and later identifying whether a specific message was previously stored [279]. Both inventions are designed to be resilient against duplication and unauthorized access, supporting future secure hardware development.

These works establish a coherent framework for using quantum randomness as a trust anchor in digital systems, demonstrating the theoretical and practical potential of qPUFs for post-quantum security, secure IoT, and critical infrastructure.

While QR-PUFs have already been demonstrated in laboratory experiments, fully qPUFs remain, to the best of our knowledge, without an end-to-end experimental realization that meets the formal qPUF definitions and associated security notions. In particular, quantum-secure authentication of a *classical* multiple-scattering optical key using few-photon (weak coherent) challenges has been experimentally demonstrated, providing security against digital emulation attacks in remote settings [264, 280]. Related photonic platforms that are compatible with quantum-readout ideas include scalable integrated photonic

PUFs (e.g. silicon-photonic interferometric structures) and reconfigurable disordered polymers, which improve stability and facilitate large-scale deployment [281, 282].

In contrast, qPUFs as formalized in [36] require the device itself to realize an intrinsically quantum primitive (often modeled as an unknown quantum transformation or, more generally, a quantum channel) that is efficiently verifiable and resistant to quantum-polynomial-time forgery. A major obstacle for implementing such constructions is the physical realization of sufficiently high-dimensional *random* quantum transformations with controlled noise, together with a reproducible verification interface [36]. One pragmatic route is therefore to consider *one-time* (consumable) quantum tokens–analogous in spirit to private-key conjugate coding—where verification necessarily disturbs the stored state and thus each authentication attempt consumes the token, requiring a fresh re-initialization or re-issuance for subsequent use. Such one-time usage can reduce the adversary's ability to accumulate information across repeated interactions, but shifts the engineering burden to reliable quantum state preparation and (possibly) short-term quantum storage [36]. Finally, realizing more advanced qPUF-based authentication schemes that aim at stronger notions of unforgeability via measurement-based or non-unitary constructions [217] is expected to require additional quantum resources, in particular quantum storage and coherent control to preserve quantum states across the verification procedure [94, 217].

10. Quantum tokens in the post-quantum world

Quantum tokens are related to quantum cryptography, i.e. they use quantum technology to provide cryptographic functionalities. PQC is conceptually different: Due to Shor's algorithm and its ability to compute discrete logarithms and large prime factors [283], it has been known for many years that the cryptographic public-key algorithms that are currently ubiquitously in use will not provide any security once cryptographically relevant quantum computers exist, i.e. quantum computers with enough stable qubits and low enough error rates to run Shor's algorithm successfully on instances currently used in public-key cryptography. According to the German Federal Office for Information Security, it is likely that such quantum computers will already exist by 2040 [284].

The response of the cryptographic community to this threat is the development of cryptographic schemes which base their security on hard mathematical problems which are assumed to resist attacks with quantum computers, such as Shor's algorithm. This kind of cryptography is called PQC, or quantum-resistant cryptography. In contrast, the cryptography used today, which will not withstand attacks by quantum computers, is called classical cryptography. Hence, PQC does not use quantum technology (and is not part of quantum cryptography), but promises security against attackers who can use a powerful quantum computer.

For at least two reasons, using PQC in practical applications may not begin only when cryptographically relevant quantum computers exist: First, the migration to post-quantum security, i.e. the exchange of currently used cryptographic schemes with post-quantum schemes, is a very complex and time-consuming undertaking and a field of research in its own right. Second, quantum computers are not only a threat once they exist—from an attacker's perspective it might be a good idea to collect large amounts of classically encrypted data now and store it until cryptographically relevant quantum computers exist. These can then be used to decrypt the data and to learn the information that should actually be confidential. These so-called 'store now, decrypt later' attacks can be prevented by using PQC already today.

A major difference between quantum tokens and PQC has already been pointed out: While quantum tokens use quantum technology, PQC is designed to run on classical, non-quantum computing devices. Another difference concerns their security promise: Quantum tokens use quantum technology, which means that they can achieve information-theoretic security [24]. Post-quantum cryptographic schemes, on the contrary, usually rely on mathematical complexity assumptions, meaning that cryptanalytic attacks might exist, both classical and quantum attacks. The maturity of quantum tokens and PQC is a further difference: As this paper demonstrates, first experimental demonstrations exist, but quantum tokens are still a long way from being widely used in practice. For PQC, however, the US-American National Institute of Standards and Technologies initiated a standardization process already in 2016, leading to five post-quantum schemes that have been selected for standardization by now (two key-encapsulation mechanisms and three digital signature schemes). Three of those have already been standardized [285]. An additional standardization process for digital signature schemes is currently underway [286]. Consequently, PQC is ready to be used in practice, and many practical applications exist, e.g. [287–290].

There are also two relevant similarities between quantum tokens and PQC: The first concerns the purpose of their use: both quantum tokens and PQC are intended to be used to achieve specific security goals. The second similarity is that the rapid development of quantum technologies is greatly accelerating their use in practical applications: for PQC, the rapid development of quantum technologies implies that they are becoming increasingly important, and for quantum tokens, that they can be realized.

Since the practical application of both PQC and quantum tokens is driven by the rapid development of quantum technologies, there will come a time when both can be combined in practical use. Although the migration to post-quantum security is challenging, it is easier than a future migration to security solutions that integrate quantum technology, since PQC principally does not require specialized hardware. Hence, the combination of quantum tokens and PQC is especially interesting for use cases where the necessary effort in quantum infrastructure is justified by the additional security guarantees that quantum tokens offer. For instance, when it comes to putting QKD into practice, proponents emphasize that combining QKD with classical symmetric cryptography, e.g. the AES encryption algorithm, combines unconditionally secure key establishment with efficient and practical encryption. Opponents, however, stress that QKD requires authentication, which is often realized with public-key cryptography, i.e. complexity-based cryptography. When the authentication of QKD relies on mathematical complexity assumptions, however, the promise of QKD to be unconditionally secure no longer holds true in practice. One perspective now could be that investing in QKD technology is not effective, but key establishment should continue to be based on public-key cryptography (and, hence, PQC). Another perspective, would be to solve the issue of authentication in certain scenarios differently, e.g. through a physical meeting of the parties involved. While this may sound unnecessary complicated at first glance, there are high-security areas where this kind of authentication is completely adequate. In such high-security use cases, hence, investing in QKD technology and combining QKD with PQC can be useful in order to achieve a very high level of security. In the future, similar scenarios will arise where quantum tokens and PQC can be combined and where the advantages of quantum tokens outweigh their supposed investment costs, especially in terms of their unforgeability, the possibility of local validation, and the user privacy that can be achieved with quantum tokens.

11. Discussion and conclusion

Quantum tokens constitute an emerging hardware-assisted security primitive that leverages quantum effects to enable information-theoretic security of communication and authentication, which are difficult to achieve in purely classical systems. Quantum token architectures rely largely on optical and solid-state platforms and their economical perspective is directly connected to the optical communication market size, which is projected to expand from USD 25.8 billion in 2025 to USD 59.4 billion by 2035 [291, 292], driven by demands for high-capacity networks and advanced photonic infrastructure. The prospective deployment of quantum tokens within wireless and embedded systems similarly aligns with growth in the RF communication market size, forecast to increase from USD 40.5 billion in 2025 to USD 88.0 billion by 2030 [293], supported by the proliferation of 5G technologies, IoT devices, and next-generation RF front-end technologies. At the same time, the broader quantum technology ecosystem is undergoing rapid maturation, with significant public and private investment advancing quantum communication, computing, and sensing capabilities, as documented in the 2025 Quantum Technology Monitor [294]. Because quantum tokens can provide secure authentication rooted in the no-cloning theorem rather than in asymmetric computational difficulty, they address security challenges that are becoming increasingly salient within the information security sector, whose global market size is already USD 218.98 billion and expected to reach USD 699.39 billion by 2034 [295, 296] in response to escalating cyberthreats and the transition toward quantum-resilient security frameworks. These converging market trajectories underscore the broader technological and economic importance of research aimed at developing practical, scalable quantum token systems capable of supporting future authentication tasks across emerging communication infrastructures.

While fully deployable, end-to-end quantum token infrastructures (issuance, storage, verification, and lifecycle management under adversarial conditions) have not yet been demonstrated, intensive experimental progress on quantum memories, interfaces, encoding protocols, and photonic and cryogenic integration indicates a credible route toward practical realizations. In this paper, we surveyed and compared selected physical approaches for implementing *state-based quantum tokens* using quantum memory elements, focusing on (i) token-state encoding in the optical and microwave domains, (ii) transmission and

access models, and (iii) quantum memory architectures and dominant sources of decoherence, loss, and verification error.

A recurring design principle across several leading platforms is to transfer a token state—initially prepared in an optical or microwave degree of freedom—into a *long-lived* nuclear spin register, thereby decoupling the token lifetime from the comparatively short coherence of excited electronic states and photonic modes. In many prominent proposals and demonstrations, this long-lived register is provided by nuclear-spin or hyperfine degrees of freedom (see figure 16), which often exhibit reduced coupling to environmental noise and can preserve phase coherence substantially longer than electronic excitations. At the same time, alternative long-lived quantum memory registers are also relevant (e.g. engineered bosonic modes in superconducting resonators), emphasizing that nuclear spins are a powerful but not exclusive pathway to long-duration storage.

In this paper, we have discussed the potential of *color centers in diamond*, which provide a representative solid-state route to optically addressable token generation and nuclear-spin-assisted storage. In architectures based on *nitrogen-vacancy (NV)* centers, photonic nanostructures such as nanopillars can improve optical access, while nearby ^{13}C nuclear spins offer long-lived storage registers. Security mechanisms in this family can exploit limited information extractability from finite quantum resources and the detectability of disturbance under attempted duplication. Where complete hardware token demonstrations are not yet available, protocol-level evaluations using gate-based quantum processors (as experimental emulators) can provide evidence of feasibility under specified noise and adversary models, while leaving open the system-level questions of device-specific imperfections, leakage channels, and physical side channels in a deployable token. Closely related, *silicon-vacancy (SiV)* centers offer attractive optical transitions and compatibility with nanophotonic integration. When coupled to nearby nuclear spins, SiV-based schemes provide a plausible route to compact memories with improved optical interfacing. Integration with platforms such as Si_3N_4 photonic circuitry is promising for scalability and packaging; however, compatibility with Telecom-band networking generally requires either operation in the appropriate wavelength regime or the inclusion of explicit frequency-conversion interfaces, which should be treated as part of the system design rather than assumed implicitly.

Quantum-token implementations based on *rare-earth materials* are notable for their potential to interface with both optical and microwave fields. In the optical domain, rare-earth memories commonly employ protocols such as AFC storage or EIT, mapping optical excitations—directly or via intermediate electronic-spin manifolds—into longer-lived spin degrees of freedom. Across the literature, these systems have demonstrated long-lived spin coherence and, in selected settings, storage and retrieval for weak coherent optical pulses and single-photon-level inputs, with efficiencies and fidelities that can be substantially enhanced in cavity-assisted or Purcell-enhanced architectures. Certain ions (e.g. praseodymium in suitable host crystals) provide favorable level structures that can facilitate more direct mappings between optical and long-lived spin or hyperfine states, potentially reducing control overhead and limiting error accumulation across multi-step transfer sequences.

Room-temperature *atomic-vapor platforms* offer an alternative route toward deployable token concepts with reduced infrastructure complexity. EIT-based vapor memories have demonstrated storage of photonic encodings, including polarization degrees of freedom, with performance limited by optical depth, magnetic noise, diffusion, and technical stability. Separately, alkali–noble-gas spin-exchange systems provide access to noble-gas nuclear-spin coherence that can be exceptionally long under well-controlled conditions. Combining these ingredients suggests a pathway to ambient-condition tokens, but it also highlights the importance of careful engineering to maintain stability in realistic environments and to quantify performance under adversarial interaction models.

Microwave quantum tokens arise naturally in superconducting circuit platforms, where nonclassical microwave states (e.g. squeezed or displaced states) can be generated and measured with high accuracy in cryogenic environments. Storage can be realized either in long-lived superconducting resonators or via transfer into spin ensembles, such as donors in silicon or rare-earth ions, that act as microwave memories. These architectures are well matched to integration with superconducting quantum processors and can support short-range, high-assurance authentication scenarios. Here, near-field or guided cryogenic interconnects represent realistic near-future targets, while the free-space, open air microwave quantum communication may require more time to be developed and brought to real applications.

Beyond token-based primitives, *qPUFs* aim to provide authentication from intrinsically quantum challenge—response behavior and are studied under formal security definitions against quantum adversaries. qPUFs therefore complement quantum tokens: tokens are often modeled as stored quantum states verified by a measurement, while qPUFs are commonly modeled as devices implementing quantum processes whose behavior should be hard to emulate. Importantly, neither paradigm eliminates the need

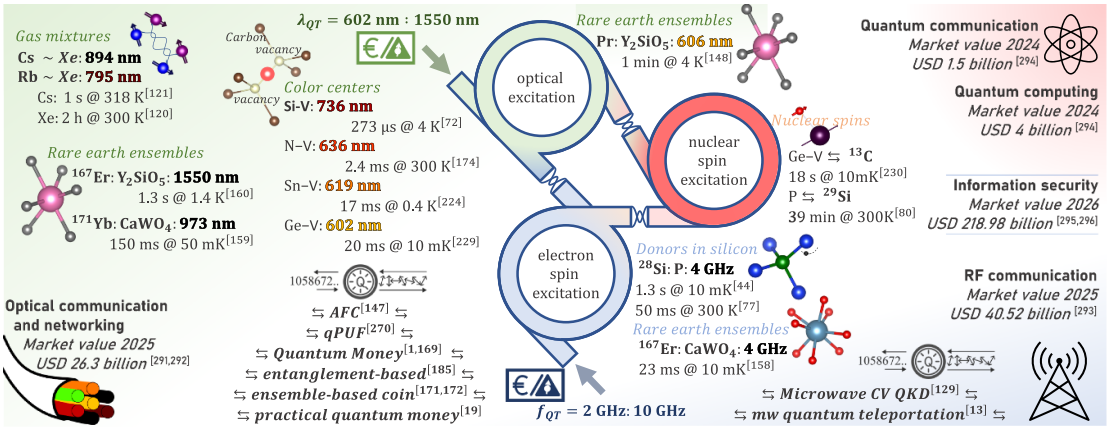

Figure 16. Schematic description of all discussed quantum token realizations. The quantum tokens can be generated in a range of laser optics frequencies (green-colored area), directly absorbed as an excitation on optical states, which can be further converted into electron or nuclear spin transitions, where the latter can be generated either directly (e.g. in Pr:Y_2SiO_5) or mediated via electron spin excitations. Alternatively, quantum tokens can be generated using transitions in the RF and microwave frequency regimes (blue-colored area). They can then be directly absorbed into the electron spin states and subsequently transferred into the nuclear spin-state excitations, which offer the longest achievable storage times for quantum states. For each memory system, the longest reported storage time and the corresponding thermal conditions are noted. While all listed spin systems aim for storing the quantum token states in nuclear spin excitations, the reported storage times mostly reflect the longest published storage time in electron spin states. Additionally, the suitable QKD protocols are summarized on the laser-optical or microwave side of the figure. The market values for the classical and quantum fields highlight the economic potential of the quantum token research.

to address implementation-level security: practical deployments must still account for noise, calibration drift, and classical side channels (timing, power, electromagnetic leakage), and must explicitly specify adversarial access (e.g. single-use versus repeated verification attempts).

Finally, quantum tokens can be naturally integrated with classical cryptographic layers. In particular, combining token-based authentication with PQC can yield a robust defense-in-depth architecture: easy to implement PQC can protect classical communication channels, key management, and stored data, while quantum tokens can strengthen authentication and identity verification by providing the information-theoretic security layer. Such hybrid designs are particularly attractive for critical infrastructure and long-term confidentiality, because a possible breakdown of the PQC layer will not imply compromising of the entire system.

In summary, quantum tokens offer a promising direction for quantum-enhanced authentication and secure transactions, and the range of candidate realizations, which span to spanning solid-state defects, rare-earth and atomic ensembles, and superconducting microwave systems, underscores the adaptability of the concept across technological ecosystems. Moving from laboratory prototypes toward deployment will require advances in memory lifetimes and efficiencies under realistic operating conditions, integrated interfaces (including photonics, transduction, and packaging), and end-to-end security analyses that incorporate both device imperfections and explicit adversary models. Continued progress along these lines will clarify the practical roles quantum tokens can play alongside classical and post-quantum security infrastructures in applications ranging from identity management and access control to high-assurance transactions.

Acknowledgments

All authors acknowledge the support of Bundesministerium für Forschung, Technologie und Raumfahrt (BMFTR) via the funding program ‘Grand challenge of the quantum communication’, with projects QuaMToMe (Grant No. 16KISQ036), HybridQToken (Grant No. 16KISQ043K), Q.TOK (Grant numbers 16KISQ039, 16KISQ038 and 16KISQ037K), QPIS (Grant No. 16KISQ032K), DIQTOK (Grant numbers 16KISQ034K and 16KISQ035), NEQSIS (Grant Numbers 16KISQ029K, 16KISQ030, and 16KISQ031), Q-ToRX (Grant Numbers 16KISQ040K, 16KISQ041 and 16KISQ042). NK, KF and HH acknowledge support by the Deutsche Forschungsgemeinschaft via Germany’s Excellence Strategy (Grant No. EXC-2111- 390814868), and JN via the Emmy-Noether program (Grant No. NO 1129/2-1). HB and CD were supported by the German Federal Ministry of Research, Technology and Space (BMFTR) through the projects QuaPhySI (Grants 16KISQ1598K and 16KIS2234), QR.N (Grants 16KIS2195 and 16KIS2196),

QSTARS (Grants 16KIS2611 and 16KIS2602), QUIET (Grants 16KISQ093 and 16KISQ0170), QD-CamNetz (Grants 16KISQ077 and 16KISQ169), and Q-TREX (Grants 16KISR027K and 16KISR038). TS was supported by the BMFTR through the project DiNOQuant (Grant No. 13N14921), GP by the EU ERC St. Grant QUREP (851810). Additional support was provided by the 6GQT initiative, funded by the Bavarian State Ministry of Economic Affairs, Regional Development and Energy. HB further acknowledges funding from the German Research Foundation (DFG) under Germany's Excellence Strategy EXC-2092 – 390781972. JK was supported by the German Federal Ministry of Research, Technology and Space (BMFTR) under the project SEQUIN (16KIS2134). CD additionally received funding from the DFG under Grant DE 1915/2-1. JW further acknowledges funding from the German Research Foundation (DFG) under SPP1514, Grant. No. 563423354.

Data availability statement

No new data were created or analysed in this study.

ORCID iDs

Nadezhda Kukharchyk 0000-0002-4636-020X
Martin E Garcia 0000-0003-2418-1902
Ilja Gerhardt 0000-0001-5807-2929
Rudolf Gross 0000-0003-4524-7552
David Hunger 0000-0001-6156-6145
Wolfgang Kilian 0000-0001-5812-5736
Kai Müller 0000-0002-4668-428X
Cyril Popov 0000-0002-4646-5319
Kilian Singer 0000-0001-9726-0367
Janik Wolters 0000-0002-4107-1265

References

[1] Einstein A, Podolsky B and Rosen N 1935 Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.* **47** 777–80
[2] Bouwmeester D, Pan J W, Mattle K, Eibl M, Weinfurter H and Zeilinger A 1997 Experimental quantum teleportation *Nature* **390** 575–79
[3] Horodecki R, Horodecki P, Horodecki M and Horodecki K 2009 Quantum entanglement *Rev. Mod. Phys.* **81** 865–942
[4] Kun D, Strömberg T, Spagnolo M, Dakić B, Rozema L A and Walther P 2025 Direct and efficient detection of quantum superposition *Phys. Rev. A* **111** L050402
[5] Terhal B M, Wolf M M and Doherty A C 2025 Quantum entanglement: a modern perspective *Phys. Today* **78** 40–46
[6] Wiesner S 1983 Conjugate coding *ACM SIGACT News* **15** 78–88
[7] Wootters W K and Zurek W H 1982 A single quantum cannot be cloned *Nature* **299** 802–3
[8] Dieks D 1982 Communication by EPR devices *Phys. Lett. A* **92** 271–2
[9] Bennett C H and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing *Proc. IEEE Int. Conf. on Computers, Systems and Signal Processing (Bangalore)* vol 10 pp 175–9
[10] Horodecki R 2021 Quantum information *Acta Phys. Pol. A* **139** 197–218
[11] Bennett C H, Bessette F, Brassard G, Salvail L and Smolin J 1992 Experimental quantum cryptography *J. Cryptol.* **5** 3–28
[12] Chen Y A *et al* 2021 An integrated space-to-ground quantum communication network over 4,600 kilometres *Nature* **589** 214–19
[13] Fedorov K G *et al* 2021 Experimental quantum teleportation of propagating microwaves *Sci. Adv.* **7** eabk0891
[14] Arute F *et al* 2019 Quantum supremacy using a programmable superconducting processor *Nature* **574** 505–10
[15] Liu H L *et al* 2025 Robust quantum computational advantage with programmable 3050-photon Gaussian boson sampling (arXiv:2508.09092 [quant-ph])
[16] Kjaergaard M, Schwartz M E, Braumüller J, Krantz P, Wang J I J, Gustavsson S and Oliver W D 2020 Superconducting qubits: current state of play *Annu. Rev. Condens. Matter Phys.* **11** 369–95
[17] Singh M, Sood S K and Bhatia M 2025 Post-quantum cryptography: a review on cryptographic solutions for the era of quantum computing *Arch. Comput. Methods Eng.* **33** 1134–3060
[18] Pastawski F, Yao N Y, Jiang L, Lukin M D and Cirac J I 2012 Unforgeable noise-tolerant quantum tokens *Proc. Natl Acad. Sci.* **109** 16079–82
[19] Bozzio M, Orieux A, Trigo Vidarte L, Zaquine I, Kerenidis I and Diamanti E 2018 Experimental investigation of practical unforgeable quantum money *npj Quantum Inf.* **4** 5
[20] Guan J Y, Arrazola J M, Amiri R, Zhang W, Li H, You L, Wang Z, Zhang Q and Pan J W 2018 Experimental preparation and verification of quantum money *Phys. Rev. A* **97** 032338
[21] Aaronson S and Christiano P 05192012 Quantum money from hidden subspaces *Proc. 44th Annual ACM Symp. on Theory of Computing* pp 41–60
[22] Yuen P 2025 Noise-tolerant public-key quantum money from a classical oracle *Quantum* **9** 1691

[23] Bozzio M, Crépeau C, Wallden P and Walther P 2025 Quantum cryptography beyond key distribution: theory and experiment *Rev. Mod. Phys.* **97** 045006
[24] Schiansky P, Kalb J, Sztatecsny E, Roehsner M C, Guggemos T, Trenti A, Bozzio M and Walther P 2023 Demonstration of quantum-digital payments *Nat. Commun.* **14** 3849
[25] Barnum H, Crepeau C, Gottesman D, Smith A and Tapp A 2002 Authentication of quantum messages *The 43rd Annual IEEE Symp. on Foundations of Computer Science, 2002. Proc.* pp 449–58
[26] Liu L R, He M Q, Zhang D B and Wang Z D 2025 Public-key quantum authentication and digital signature schemes based on the QMA-complete problem (arXiv:2506.16904 [quant-ph])
[27] Bennett C H and Brassard G 2014 Quantum cryptography: public key distribution and coin tossing *Theor. Comput. Sci.* **560** 7–11
[28] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dusek M, Lütkenhaus N and Peev M 2009 The security of practical quantum key distribution *Rev. Mod. Phys.* **81** 1301–50
[29] Aaronson S 2018 Shadow tomography of quantum states *Proc. 50th Annual ACM SIGACT Symp. on Theory of Computing* pp 325–38
[30] Gavinsky D 2012 Quantum money with classical verification *2012 IEEE 27th Conf. on Computational Complexity* pp 42–52
[31] Bartkiewicz K, Černoch A, Chimczak G, Lemr K, Miranowicz A and Nori F 2017 Experimental quantum forgery of quantum optical money *npj Quantum Inf.* **3** 7
[32] Chen H, Jia H, Wu X, Wang X and Wang M 2021 Quantum token for network authentication *2021 IEEE Int. Conf. on Web Services (ICWS)* pp 688–92
[33] Murray H and Malone D 2021 Quantum multi-factor authentication *Emerg. Technol. Auth. Authentication* **13136** 50–67
[34] Brassard G 2005 Brief history of quantum cryptography: a personal perspective *2005 IEEE Information Theory Worksh. on Theory and Practice in Information-Theoretic Security* pp 19–23
[35] Pappu R, Recht B, Taylor J and Gershenfeld N 2002 Physical one-way functions *Science* **297** 2026–30
[36] Arapinis M, Delavar M, Doosti M and Kashefi E 2021 Quantum physical unclonable functions: possibilities and impossibilities *Quantum* **5** 475
[37] Škorić B 2010 Quantum readout of physical unclonable functions *Int. J. Quantum Inf.* **10** 1250001
[38] Škorić B 2012 Quantum readout of physical unclonable functions *Int. J. Quantum Inf.* **10** 1250001
[39] Nikolopoulos G M and Diamanti E 2017 Continuous-variable quantum authentication of physical unclonable keys *Sci. Rep.* **7** 46047
[40] Kent A 2019 S-money: virtual tokens for a relativistic economy *Proc. Math. Phys. Eng. Sci.* **475** 20190170
[41] Kent A, Lowndes D, Pitalúa-García D and Rarity J 2022 Practical quantum tokens without quantum memories and experimental tests *npj Quantum Inf.* **8** 28
[42] Jiang Y F *et al* 2024 Experimental practical quantum tokens with transaction time advantage (arXiv:2408.13063 [quant-ph])
[43] Wang F, Ren M, Sun W, Guo M, Sellars M J, Ahlefeldt R L, Bartholomew J G, Yao J, Liu S and Zhong M 2025 Nuclear spins in a solid exceeding 10-hour coherence times for ultra-long-term quantum storage *PRX Quantum* **6** 010302
[44] Tyryshkin A M *et al* 2011 Electron spin coherence exceeding seconds in high-purity silicon *Nat. Mater.* **11** 143
[45] Fesquet F, Kronowetter F, Renger M, Yam W K, Gandorfer S, Inomata K, Nakamura Y, Marx A, Gross R and Fedorov K G 2024 Demonstration of microwave single-shot quantum key distribution *Nat. Commun.* **15** 7544
[46] Romanenko A, Pilipenko R, Zorzetti S, Frolov D, Awida M, Belomestnykh S, Posen S and Grassellino A 2020 Three-dimensional superconducting resonators at T $<$ 20mK with photon lifetimes up to $\tau = 2$ s *Phys. Rev. Appl.* **13** 034032
[47] Xie E *et al* 2018 Compact 3D quantum memory *Appl. Phys. Lett.* **112** 202601
[48] Nojiri Y, Honasoge K E, Marx A, Fedorov K G and Gross R 2024 Onset of transmon ionization in microwave single-photon detection *Phys. Rev. B* **109** 174312
[49] Wang C *et al* 2022 Towards practical quantum computers: transmon qubit with a lifetime approaching 0.5 milliseconds *npj Quantum Inf.* **8** 3
[50] Somoroff A, Ficheux Q, Mencia R A, Xiong H, Kuzmin R and Manucharyan V E 2023 Millisecond coherence in a superconducting qubit *Phys. Rev. Lett.* **130** 267001
[51] Place A P M *et al* 2021 New material platform for superconducting transmon qubits with coherence times exceeding 0.3 milliseconds *Nat. Commun.* **12** 1779
[52] Yoneda J *et al* 2018 A quantum-dot spin qubit with coherence limited by charge noise and fidelity higher than 99.9 *Nat. Nanotechnol.* **13** 102–6
[53] Wang P, Luan C Y, Qiao M, Um M, Zhang J, Wang Y, Yuan X, Gu M, Zhang J and Kim K 2021 Single ion qubit with estimated coherence time exceeding one hour *Nat. Commun.* **12** 233
[54] Ruster T, Schmiegelow C T, Kaufmann H, Warschburger C, Schmidt-Kaler F and Poschinger U G 2016 A long-lived Zeeman trapped-ion qubit *Appl. Phys. B* **122** 254
[55] Levine H *et al* 2019 Parallel implementation of high-fidelity multiqubit gates with neutral atoms *Phys. Rev. Lett.* **123** 170503
[56] Dudin Y O, Li L and Kuzmich A 2013 Light storage on the time scale of a minute *Phys. Rev. A* **87** 031801
[57] MacCabe G S, Ren H, Luo J, Cohen J D, Zhou H, Sipahigil A, Mirhosseini M and Painter O 2020 Nano-acoustic resonator with ultralong phonon lifetime *Science* **370** 840–43
[58] Seis Y, Capelle T, Langman E, Saarinen S, Planz E and Schliesser A 2022 Ground state cooling of an ultracoherent electromechanical system *Nat. Commun.* **13** 1507
[59] Esguerra L, Meßner L, Robertson E, Ewald N V, Gündoğan M and Wolters J 2023 Optimization and readout-noise analysis of a warm-vapor electromagnetically-induced-transparency memory on the cs D_1 line *Phys. Rev. A* **107** 042607
[60] Jutisz M, Erl A, Wolters J, Gündoğan M and Krutzik M 2025 Stand-alone mobile quantum memory system *Phys. Rev. Appl.* **23** 024045
[61] Meßner L, Robertson E, Esguerra L, Lüdge K and Wolters J 2023 Multiplexed random-access optical memory in warm cesium vapor *Opt. Express* **31** 10150–8
[62] Orphal-Kobin L, Unterguggenberger K, Pregnolato T, Kemf N, Matalla M, Unger R S, Ostermay I, Pieplow G and Schröder T 2023 Optically coherent nitrogen-vacancy defect centers in diamond nanostructures *Phys. Rev. X* **13** 011042
[63] Torun C G Munns J H D Herrmann F M Villafane V Müller K Thies A Pregnolato T Pieplow G and Schröder T 2023 Optical probing of phononic properties of a tin-vacancy color center in diamond (arXiv:2312.05335)
[64] Karapatzakis I *et al* 2024 Microwave control of the tin-vacancy spin qubit in diamond with a superconducting waveguide *Phys. Rev. X* **14** 031036

[65] Mendoza Delgado M, Tsunaki L, Michaelson S, Kuntumalla M K, Reithmaier J P, Hoffman A, Naydenov B and Popov C 2025 Impact of annealing and nanostructuring on properties of NV centers created by different techniques *Diam. Relat. Mater.* **154** 112126
[66] Morello A *et al* 2010 Single-shot readout of an electron spin in silicon *Nature* **467** 687
[67] Weichselbaumer S, Zens M, Zollitsch C W, Brandt M S, Rotter S, Gross R and Huebl H 2020 Echo trains in pulsed electron spin resonance of a strongly coupled spin ensemble *Phys. Rev. Lett.* **125** 137701
[68] Kukharchyk N, Sholokhov D, Morozov O, Korableva S L, Kalachev A A and Bushev P A 2018 Optical coherence of ^{1}66Er :^{7} $LiYF_4$ crystal below 1 K *New J. Phys.* **20** 023044
[69] Casabone B, Deshmukh C, Liu S, Serrano D, Ferrier A, Hümmer T, Goldner P, Hunger D and de Riedmatten H 2021 Dynamic control of purcell enhanced emission of erbium ions in nanoparticles *Nat. Commun.* **12** 3570
[70] Deshmukh C, Beattie E, Casabone B, Grandi S, Serrano D, Ferrier A, Goldner P, Hunger D and de Riedmatten H 2023 Detection of single ions in a nanoparticle coupled to a fiber cavity *Optica* **10** 1339–44
[71] Goldner P, Ferrier A and Guillot-Noël O 2015 Chapter 267 - rare earth-doped crystals for quantum information processing *Handbook Phys. Chem. Rare Earths* **46** 1–78
[72] Klotz M, Tangemann A and Kubanek A 2025 Ultra-high strained diamond spin register with coherent optical control *npj Quantum Inf.* **11** 91
[73] Maurer P C *et al* 2012 Room-temperature quantum bit memory exceeding one second *Science* **336** 1283–86
[74] Beukers H K C *et al* 2025 Control of solid-state nuclear spin qubits using an electron spin *Phys. Rev. X* **15** 021011
[75] Inc P *et al* 2024 Distributed quantum computing in silicon (arXiv:2406.01704 [quant-ph])
[76] Trusheim M E *et al* 2020 Transform-limited photons from a coherent tin-vacancy spin in diamond *Phys. Rev. Lett.* **124** 023602
[77] Steger M, Saeedi K, Thewalt M L W, Morton J J L, Riemann H, Abrosimov N V, Becker P and Pohl H J 2012 Quantum information storage for over 180 s using donor spins in a ^{2}8Si *Science* **336** 1280
[78] Davies E R 1974 A new pulse ENDOR technique *Phys. Lett. A* **47** 1–2
[79] Hoehne F, Dreher L, Huebl H, Stutzmann M and Brandt M S 2011 Electrical detection of coherent nuclear spin oscillations in phosphorus-doped silicon using pulsed ENDOR *Phys. Rev. Lett.* **106** 187601
[80] Saeedi K, Simmons S, Salvail J Z, Dluhy P, Riemann H, Abrosimov N V, Becker P, Pohl H J, Morton J J L and Thewalt M L W 2013 Room-temperature quantum bit storage exceeding 39 minutes using ionized donors in silicon-28 *Science* **342** 830–33
[81] Wolters J, Buser G, Horsley A, Béguin L, Jöckel A, Jahn J P, Warburton R J and Treutlein P 2017 Simple atomic quantum memory suitable for semiconductor quantum dot single photons *Phys. Rev. Lett.* **119** 060502
[82] Buser G, Mottola R, Cotting B, Wolters J and Treutlein P 2022 Single-photon storage in a ground-state vapor cell quantum memory *PRX Quantum* **3** 020349
[83] Namazi M, Kupchak C, Jordaan B, Shahrokhshahi R and Figueroa E 2017 Ultralow-noise room-temperature quantum memory for polarization qubits *Phys. Rev. Appl.* **8** 034023
[84] Katz O, Shaham R, Reches E, Gorshkov A V and Firstenberg O 2022 Optical quantum memory for noble-gas spins based on spin-exchange collisions *Phys. Rev. A* **105** 042606
[85] Afzelius M, Sangouard N, Johansson G, Staudt M U and Wilson C M 2013 Proposal for a coherent quantum memory for propagating microwave photons *New J. Phys.* **15** 065008
[86] Dicke R H 1954 Coherence in spontaneous radiation processes *Phys. Rev.* **93** 99–110
[87] Businger M, Tiranov A, Kaczmarek K T, Welinski S, Zhang Z, Ferrier A, Goldner P and Afzelius M 2020 Optical spin-wave storage in a solid-state hybridized electron-nuclear spin ensemble *Phys. Rev. Lett.* **124** 053606
[88] Ma Y, Ma Y Z, Zhou Z Q, Li C F and Guo G C 2021 One-hour coherent optical storage in an atomic frequency comb memory *Nat. Commun.* **12** 2381
[89] Seri A, Lenhard A, Rieländer D, Gündoğan M, Ledingham P M, Mazzera M and de Riedmatten H 2017 Quantum correlations between single telecom photons and a multimode on-demand solid-state quantum memory *Phys. Rev. X* **7** 021028
[90] Saunders D J, Munns J H D, Champion T F M, Qiu C, Kaczmarek K T, Poem E, Ledingham P M, Walmsley I A and Nunn J 2016 Cavity-enhanced room-temperature broadband Raman memory *Phys. Rev. Lett.* **116** 090501
[91] Kalachev A, Berezhnoi A, Hemmer P and Kocharovskaya O 2019 Raman quantum memory based on an ensemble of silicon-vacancy centers in diamond *Laser Phys.* **29** 104001
[92] Lan S Y, Radnaev A G, Collins O A, Matsukevich D N, Kennedy T A and Kuzmich A 2009 A multiplexed quantum memory *Opt. Express* **17** 13639–45
[93] Kunz P D Santra S Meyer D H Castillo Z A Malinovsky V S and Cox K C 2019 Spatial multiplexing in a cavity-enhanced quantum memory (arXiv:1903.02625 [physics])
[94] Vernaz-Gris P, Huang K, Cao M, Sheremet A S and Laurat J 2018 Highly-efficient quantum memory for polarization qubits in a spatially-multiplexed cold atomic ensemble *Nat. Commun.* **9** 363
[95] Fesquet F *et al* 2023 Perspectives of microwave quantum key distribution in the open air *Phys. Rev. A* **108** 032607
[96] Gonzalez-Raya T, Casariego M, Fesquet F, Renger M, Salari V, Möttönen M, Omar Y, Deppe F, Fedorov K G and Sanz M 2022 Open-air microwave entanglement distribution for quantum teleportation *Phys. Rev. Appl.* **18** 044002
[97] Blais A, Huang R S, Wallraff A, Girvin S M and Schoelkopf R J 2004 Cavity quantum electrodynamics for superconducting electrical circuits: an architecture for quantum computation *Phys. Rev. A* **69** 062320
[98] Wallraff A, Schuster D I, Blais A, Frunzio L, Huang R S, Majer J, Kumar S, Girvin S M and Schoelkopf R J 2004 Strong coupling of a single photon to a superconducting qubit using circuit quantum electrodynamics *Nature* **431** 162–7
[99] Chiorescu I, Bertet P, Semba K, Nakamura Y, Harmans C J P M and Mooij J E 2004 Coherent dynamics of a flux qubit coupled to a harmonic oscillator *Nature* **431** 159–62
[100] Menzel E P *et al* 2012 Path entanglement of continuous-variable quantum microwaves *Phys. Rev. Lett.* **109** 250502
[101] Fedorov K G *et al* 2018 Finite-time quantum entanglement in propagating squeezed microwaves *Sci. Rep.* **8** 6416
[102] Renger M *et al* 2022 Flow of quantum correlations in noisy two-mode squeezed microwave states *Phys. Rev. A* **106** 052415
[103] Pogorzalek S *et al* 2019 Secure quantum remote state preparation of squeezed microwave states *Nat. Comm.* **10** 2604
[104] Mariantoni M, Menzel E P, Deppe F, Araque Caballero M, Baust A, Niemczyk T, Hoffmann E, Solano E, Marx A and Gross R 2010 Planck spectroscopy and quantum noise of microwave beam splitters *Phys. Rev. Lett.* **105** 133601
[105] Eichler C, Bozyigit D, Lang C, Steffen L, Fink J and Wallraff A 2011 Experimental state tomography of itinerant single microwave photons *Phys. Rev. Lett.* **106** 220503
[106] Afzelius M, Simon C, de Riedmatten H and Gisin N 2009 Multimode quantum memory based on atomic frequency combs *Phys. Rev. A* **79** 052329

[107] Bennett C H, Brassard G, Breidbart S and Wiesner S 1983 Quantum cryptography, or unforgeable subway tokens *Advances in Cryptology* (Springer) pp 267–75
[108] Ekert A K 1991 Quantum cryptography based on Bell's theorem *Phys. Rev. Lett.* **67** 661–3
[109] Scarani V, Acín A, Ribordy G and Gisin N 2004 Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations *Phys. Rev. Lett.* **92** 057901
[110] Jain N *et al* 2022 Practical continuous-variable quantum key distribution with composable security *Nat. Commun.* **13** 4740
[111] Zhang Y, Bian Y, Li Z, Yu S and Guo H 2024 Continuous-variable quantum key distribution system: past, present and future *Appl. Phys. Rev.* **11** 011318
[112] Hajomer A A E, Derkach I, Jain N, Chin H M, Andersen U L and Gehring T 2024 Long-distance continuous-variable quantum key distribution over 100-km fiber with local local oscillator *Sci. Adv.* **10** eadi9474
[113] Hajomer A A E, Derkach I, Usenko V C, Andersen U L and Gehring T 2025 Coexistence of continuous-variable quantum key distribution and classical data over 120 km fiber *Phys. Rev. Lett.* **135** 170804
[114] Liu C, Wang M, Stein S A, Ding Y and Li A 2023 Quantum memory: a missing piece in quantum computing units (arXiv:2309.14432 [quant-ph])
[115] Molina A, Vidick T and Watrous J 2013 Optimal counterfeiting attacks and generalizations for Wiesner's quantum money *Theory of Quantum Computation, Communication and Cryptography* pp 45–64
[116] Brassard G and Salvail L 1994 Secret-key reconciliation by public discussion *Advances in Cryptology—EUROCRYPT'93* pp 410–23
[117] Buttler W T, Lamoreaux S K, Torgerson J R, Nickel G H, Donahue C H and Peterson C G 2003 Fast, efficient error reconciliation for quantum cryptography *Phys. Rev. A* **67** 052303
[118] Gallager R 1962 Low-density parity-check codes *IEEE Trans. Inf. Theory* **8** 21–28
[119] Liu Z, Wu Z and Huang A 2020 Blind information reconciliation with variable step sizes for quantum key distribution *Sci. Rep.* **10** 171
[120] Kilian W, Haller A, Seifert F, Grosenick D and Rinneberg H 2007 Free precession and transverse relaxation of hyperpolarized ^{1}29Xe gas detected by SQUIDs in ultra-low magnetic fields *Eur. Phys. J. D* **42** 197–202
[121] Katz O and Firstenberg O 2018 Light storage for one second in room-temperature alkali vapor *Nat. Commun.* **9** 2074
[122] Pirandola S, Eisert J, Weedbrook C, Furusawa A and Braunstein S L 2015 Advances in quantum teleportation *Nat. Photon.* **9** 641–52
[123] Braunstein S L and Kimble H J 2000 Dense coding for continuous variables *Phys. Rev. A* **61** 042302
[124] Axline C J *et al* 2018 On-demand quantum state transfer and entanglement between remote microwave cavity memories *Nat. Phys.* **14** 705–10
[125] Leung N, Lu Y, Chakram S, Naik R K, Earnest N, Ma R, Jacobs K, Cleland A N and Schuster D I 2019 Deterministic bidirectional communication and remote entanglement generation between superconducting qubits *npj Quantum Inf.* **5** 18
[126] Magnard P *et al* 2020 Microwave quantum link between superconducting circuits housed in spatially separated cryogenic systems *Phys. Rev. Lett.* **125** 260502
[127] Yam W K, Gandorfer S, Fesquet F, Handschuh M, Honasoge K E, Marx A, Gross R and Fedorov K G 2026 Quantum teleportation over thermal microwave network *Phys. Rev. Lett.* **136** 180801
[128] O'Sullivan J *et al* 2022 Random-access quantum memory using chirped pulse phase encoding *Phys. Rev. X* **12** 041014
[129] Cerf N J, Lévy M and van Assche G 2001 Quantum distribution of Gaussian keys using squeezed states *Phys. Rev. A* **63** 052311
[130] Larsen B L, Hajomer A A E, Abiuso P, Izumi S, Gehring T, Neergaard-Nielsen J S, Acín A and Andersen U L 2026 Continuous variable measurement-device-independent quantum certification *Phys. Rev. X* **16** 011070
[131] Owari M, Plenio M B, Polzik E S, Serafini A and Wolf M M 2008 Squeezing the limit: quantum benchmarks for the teleportation and storage of squeezed states *New J. Phys.* **10** 113014
[132] Jensen K, Wasilewski W, Krauter H, Fernholz T, Nielsen B M, Owari M, Plenio M B, Serafini A, Wolf M M and Polzik E S 2011 Quantum memory for entangled continuous-variable states *Nat. Phys.* **7** 13–16
[133] Honasoge K E, Handschuh M, Yam W K, Gandorfer S, Bazulin D, Bruckmoser N, Koch L, Marx A, Gross R and Fedorov K G 2025 Fabrication of low-loss Josephson parametric devices *Phys. Rev. B* **111** 214508
[134] Julsgaard B, Grezes C, Bertet P and Mølmer K 2013 Quantum memory for microwave photons in an inhomogeneously broadened spin ensemble *Phys. Rev. Lett.* **110** 250503
[135] Feher G and Gere E A 1959 Electron spin resonance experiments on donors in silicon. II. Electron spin relaxation effects *Phys. Rev.* **114** 1245
[136] Weichselbaumer S, Natzkin P, Zollitsch C W, Weiler M, Gross R and Huebl H 2019 Quantitative modeling of superconducting planar resonators for electron spin resonance *Phys. Rev. Appl.* **12** 024021
[137] Wesenberg J H, Ardavan A, Briggs G A D, Morton J J L, Schoelkopf R J, Schuster D I and Molmer K 2009 Quantum computing with an electron spin ensemble *Phys. Rev. Lett.* **103** 070502
[138] Zollitsch C W, Mueller K, Franke D P, Goennenwein S T B, Brandt M S, Gross R and Huebl H 2015 High cooperativity coupling between a phosphorus donor spin ensemble and a superconducting microwave resonator *Appl. Phys. Lett.* **107** 142105
[139] Kukharchyk N, Sholokhov D, Morozov O, Korableva S L, Kalachev A A and Bushev P A 2020 Electromagnetically induced transparency in a mono-isotopic ^{1}67Er :^{7} $LiYF_4$ crystal below 1 kelvin: microwave photonics approach *Opt. Express* **28** 29166
[140] Strinić A, Oehrl P, Marx A, Bushev P A, Huebl H, Gross R and Kukharchyk N 2025 Broadband electron paramagnetic resonance spectroscopy of ^{1}67Er:^{7}$LiYF_4$ at millikelvin temperatures *Phys. Rev. B* **111** 214430
[141] Fedorov K G *et al* 2016 Displacement of propagating squeezed microwave states *Phys. Rev. Lett.* **117** 020502
[142] Gandorfer S, Renger M, Yam W K, Fesquet F, Marx A, Gross R and Fedorov K G 2025 Two-dimensional Planck spectroscopy for microwave photon calibration *Phys. Rev. Appl.* **23** 024064
[143] Oehrl P, Fesquet F, Honasoge K E, Handschuh M, Marx A, Gross R, Fedorov K G and Huebl H 2025 Probing an electron spin ensemble with squeezed microwave signals (arXiv:2512.17490)
[144] Dibos A M, Raha M, Phenicie C M and Thompson J D 2018 Atomic source of single photons in the telecom band *Phys. Rev. Lett.* **120** 243601
[145] Kindem J M, Ruskuc A, Bartholomew J G, Rochman J, Huan Y Q and Faraon A 2020 Control and single-shot readout of an ion embedded in a nanophotonic cavity *Nature* **580** 201–4
[146] Ulanowski A, Merkel B and Reiserer A 2022 Spectral multiplexing of telecom emitters with stable transition frequency *Sci. Adv.* **8** eabo4538

[147] Tittel W, Afzelius M, Kinos A, Rippe L and Walther A 2025 Quantum networks using rare-earth ions *Quantum Sci. Technol.* **10** 033002
[148] Heinze G, Hubrich C and Halfmann T 2023 Stopped light and image storage by electromagnetically induced transparency up to the regime of one minute *Phys. Rev. Lett.* **111** 033601
[149] Hain M, Stewen N and Halfmann T 2025 Light storage by electromagnetically induced transparency for one second at the level of a single photon in Pr:Y_2SiO_5 prepared with multiple frequency ensembles *New J. Phys.* **27** 023029
[150] Teller M, Plascencia S, Sastre Jachimska C, Grandi S and de Riedmatten H 2025 A solid-state temporally multiplexed quantum memory array at the single-photon level *npj Quantum Inf.* **11** 92
[151] Wei S H *et al* 2024 Quantum storage of 1650 modes of single photons at telecom wavelength *npj Quantum Inf.* **10** 19
[152] Zhong T *et al* 2018 Optically addressing single rare-earth ions in a nanophotonic cavity *Phys. Rev. Lett.* **121** 183603
[153] Chen S, Raha M, Phenicie C M, Ourari S and Thompson J D 2020 Parallel single-shot measurement and coherent control of solid-state spins below the diffraction limit *Science* **370** 592–5
[154] Xia K *et al* 2022 Tunable microcavities coupled to rare-earth quantum emitters *Optica* **9** 445–50
[155] Gritsch A, Ulanowski A, Pforr J and Reiserer A 2025 Optical single-shot readout of spin qubits in silicon *Nat. Commun.* **16** 64
[156] Gupta S, Huang Y, Liu S, Pei Y, Gao Q, Yang S, Tomm N, Warburton R J and Zhong T 2025 Dual epitaxial telecom spin-photon interfaces with long-lived coherence *Nat. Commun.* **16** 9814
[157] Genov G T, Schraft D, Vitanov N V and Halfmann T 2017 Arbitrarily accurate pulse sequences for robust dynamical decoupling *Phys. Rev. Lett.* **118** 133202
[158] Le Dantec M *et al* 2021 Twenty-three–millisecond electron spin coherence of erbium ions in a natural-abundance crystal *Sci. Adv.* **7** eabj9786
[159] Tiranov A *et al* 2026 Sub-second spin and lifetime-limited optical coherences in 171Yb3+:CaWO4 *Nat. Commun.* **17** 4115
[160] Rančić M, Hedges M P, Ahlefeldt R L and Sellars M J 2018 Coherence time of over a second in a telecom-compatible quantum memory storage material *Nat. Phys.* **14** 50–54
[161] Corrielli G, Seri A, Mazzera M, Osellame R and de Riedmatten H 2016 Integrated optical memory based on laser-written waveguides *Phys. Rev. Appl.* **5** 054013
[162] Saglamyurek E, Sinclair N, Jin J, Slater J A, Oblak D, Bussières F, George M, Ricken R, Sohler W and Tittel W 2011 Broadband waveguide quantum memory for entangled photons *Nature* **469** 512–5
[163] Casabone B, Benedikter J, Hümmer T, Oehl F, Lima K D O, Hänsch T W, Ferrier A, Goldner P, Riedmatten H D and Hunger D 2018 Cavity-enhanced spectroscopy of a few-ion ensemble in Eu3+:Y2O3 *New J. Phys.* **20** 095006
[164] Eichhorn T *et al* 2025 *Nanophotonics* **14** 1817–26
[165] Sardi F, Foteinou V, Stöhr R, Kolesov R and Wrachtrup J 2024 Photonic integration of 171ytterbium single photon sources into an $LiNbO_3$-based photonic platform *SPIE Quantum West Quantum Computing, Communication and Simulation IV* (*San Francisco, California, United States)13 Mar 2024 Quantum Computing, Communication and Simulation* IV (SPIE) **12911**
[166] Yang L, Wang S and Tang H X 2023 Toward radiative-limited coherence of erbium dopants in a nanophotonic resonator *Appl. Phys. Lett.* **123** 124001
[167] Ourari S *et al* 2023 Indistinguishable telecom band photons from a single Er ion in the solid state *Nature* **620** 977–81
[168] Ruskuc A, Wu C J, Green E, Hermans S L N, Pajak W, Choi J and Faraon A 2025 Multiplexed entanglement of multi-emitter quantum network nodes *Nature* **639** 54–59
[169] Strocka Y Belhassen M Schröder T and Pieplow G 2025 Secure quantum token processing with color centers in diamond (arXiv:2503.04985 [quant-ph])
[170] Singer K Popov C and Naydenov B 2022 Verfahren zum Erstellen eines Quanten-Datentokens patent DE 10 2022 107 528 A1 2023.10.05
[171] Tsunaki L, Bauerhenne B, Xibraku M, Garcia M E, Singer K and Naydenov B 2025 Ensemble-based quantum token protocol benchmarked on IBM quantum processors *Quantum Sci. Technol.* **10** 045042
[172] Bauerhenne B, Tsunaki L, Thieme J, Naydenov B and Singer K 2025 Security analysis of ensemble-based quantum token protocol under advanced attacks *Quantum Sci. Technol.* **10** 045043
[173] Mendoza Delgado M *et al* 2025 Technological steps for realization of diamond-based quantum tokens *Nanotechnological Advances in Environmental, Cyber and CBRN Security* pp 29–45
[174] Herbschleb E D *et al* 2019 Ultra-long coherence times amongst room-temperature solid-state spins *Nat. Commun.* **10** 3766
[175] Munuera-Javaloy C, Puebla R and Casanova J 2021 Dynamical decoupling methods in nanoscale NMR *Europhys. Lett.* **134** 30001
[176] Naydenov B, Dolde F, Hall L T, Shin C, Fedder H, Hollenberg L C L, Jelezko F and Wrachtrup J 2011 Dynamical decoupling of a single-electron spin at room temperature *Phys. Rev. B* **83** 081201
[177] Tian Z, Chang H, Lv X, Yang M, Wang Z, Yang P, Zhang P, Li G and Zhang T 2024 Extending the coherence time limit of a single-alkali-atom qubit by suppressing phonon-jumping-induced decoherence *Optica* **11** 1391–6
[178] Klotz M, Waltrich R, Lettner N, Agafonov V N and Kubanek A 2024 Strongly coupled spins of silicon-vacancy centers inside a nanodiamond with sub-megahertz linewidth *Nanophotonics* **13** 2361–6
[179] Klotz M *et al* 2022 Pro- longed orbital relaxation by locally modified phonon density of states for the SiV- center in nanodiamonds *Phys. Rev. Lett.* **128** 153602
[180] Kubanek A *et al* 2022 Hybrid quantum nanophotonics-interfacing color center in nanodiamonds with photonics *Prog. Nanophoton.* **147** 123–74
[181] Fehler K G, Ovvyan A P, Antoniuk L, Lettner N, Gruhler N, Davydov V A, Agafonov V N, Pernice W H and Kubanek A 2020 Purcell-enhanced emission from individual SiV-center in nanodiamonds coupled to a Si3N4-based, photonic crystal cavity *Nanophotonics* **9** 3655–62
[182] Fehler K G, Antoniuk L, Lettner N, Ovvyan A P, Waltrich R, Gruhler N, Davydov V A, Agafonov V N, Pernice W H and Kubanek A 2021 Hybrid quantum photonics based on artificial atoms placed inside one hole of a photonic crystal cavity *ACS Photonics* **8** 2635–41
[183] Lettner N, Antoniuk L, Ovvyan A P, Gehring H, Wendland D, Agafonov V N, Pernice W H and Kubanek A 2024 Controlling all degrees of freedom of the optical coupling in hybrid quantum photonics *ACS Photonics* **11** 696–702
[184] Antoniuk L, Lettner N, Ovvyan A P, Haugg S, Klotz M, Gehring H, Wendland D, Agafonov V N, Pernice W H and Kubanek A 2024 All-optical spin access via a cavity-broadened optical transition in on-chip hybrid quantum photonics *Phys. Rev. Appl.* **21** 054032
[185] Bernien H, Hensen B, Pfaff W, Koolstra G, Blok M S, Robledo L, Taminiau T H M M, Twitchen D J, Childress L and Hanson R 2013 Heralded entanglement between solid-state qubits separated by three metres *Nature* **497** 86–90

[186] Waltrich R, Klotz M, Agafonov V N and Kubanek A 2023 Two-photon interference from silicon-vacancy centers in remote nanodiamonds *Nanophotonics* **12** 3663–9
[187] Schäfer M, Kambs B, Herrmann D, Bauer T and Becher C 2025 Two-stage, low noise quantum frequency conversion of single photons from silicon-vacancy centers in diamond to the telecom C-band *Adv. Quantum Technol.* **8** 2300228
[188] Bersin E *et al* 2024 Telecom networking with a diamond quantum memory *PRX Quantum* **5** 010303
[189] Bhaskar M K *et al* 2020 Experimental demonstration of memory-enhanced quantum communication *Nature* **580** 60–64
[190] Bradley C E, Randall J, Abobeih M H, Berrevoets R C, Degen M J, Bakker M A, Markham M, Twitchen D J and Taminiau T H 2019 A ten-qubit solid-state spin register with quantum memory up to one minute *Phys. Rev. X* **9** 031045
[191] Bopp J M, Plock M, Turan T, Pieplow G, Burger S and Schröder T 2024 Sawfish' photonic crystal cavity for near-unity emitter-to-fiber interfacing in quantum network applications *Adv. Opt. Mater.* **12** 2301286
[192] Pregnolato T, Stucki M E, Bopp J M, v. d. Hoeven M H, Gokhale A, Krüger O and Schröder T 2024 Fabrication of Sawfish photonic crystal cavities in bulk diamond *APL Photonics* **9** 036105
[193] Grotowski S *et al* 2025 Optimizing the growth conditions of superconducting MoSi thin films for single photon detection *Sci. Rep.* **15** 2438
[194] Strohauer S, Wietschorke F, Schmid C, Grotowski S, Zugliani L, Jonas B, Müller K and Finley J J 2025 Current crowding–free superconducting nanowire single-photon detectors *Sci. Adv.* **11** eadt0502
[195] Majety S, Strohauer S, Saha P, Wietschorke F, Finley J J, Müller K and Radulaski M 2023 Triangular quantum photonic devices with integrated detectors in silicon carbide *Mater. Quantum Technol.* **3** 015004
[196] Zugliani L *et al* 2023 Tailoring superconducting nanowire single-photon detectors for quantum technologies *2023 IEEE Globecom Worksh. (GC Wkshps)* pp 1051–6
[197] Strohauer S *et al* 2023 Site-selective enhancement of superconducting nanowire single-photon detectors via local helium ion irradiation *Adv. Quantum Technol.* **6** 2300139
[198] Flaschmann R *et al* 2023 Optimizing the growth conditions of al mirrors for superconducting nanowire single-photon detectors *Mater. Quantum Technol.* **3** 035002
[199] Mamann H, Nieddu T, Hoffet F, Bozzio M, de Loubresse F G, Kerenidis I, Diamanti E, Urvoy A and Laurat J 2025 Quantum cryptography integrating an optical quantum memory *Sci. Adv.* **11** eadx3223
[200] Pieplow G, Torun C G, Gurr C, Munns J H D, Herrmann F M, Thies A, Pregnolato T and Schröder T 2025 Quantum electrometer for time-resolved material science at the atomic lattice scale *Nat. Commun.* **16** 6435
[201] de Santis L, Trusheim M E, Chen K C and Englund D R 2021 Investigation of the Stark effect on a centrosymmetric quantum emitter in diamond *Phys. Rev. Lett.* **127**
[202] Lee J P, Villa B, Bennett A J, Stevenson R M, Ellis D J P, Farrer I, Ritchie D A and Shields A J 2019 A quantum dot as a source of time-bin entangled multi-photon states *Quantum Sci. Technol.* **4** 025011
[203] Bouchard F, England D, Bustard P J, Heshami K and Sussman B 2022 Quantum communication with ultrafast time-bin qubits *Phys. Rev. X* **3** 010332
[204] Yu H *et al* 2025 Quantum key distribution implemented with d-level time-bin entangled photons *Nat. Commun.* **16** 171
[205] Gündoğdu S, Pazzagli S, Pregnolato T, Kolbe T, Hagedorn S, Weyers M and Schröder T 2025 AlGaN/AlN heterostructures: an emerging platform for integrated photonics *npj Nanophotonics* **2** 2
[206] Wei Y C *et al* 2025 Universal distributed blind quantum computing with solid-state qubits *Science* **388** 509–13
[207] Omlor F, Tissot B and Burkard G 2025 Entanglement generation using single-photon pulse reflection in realistic networks *Phys. Rev. A* **111** 012612
[208] Knaut C M *et al* 2024 Entanglement of nanophotonic quantum memory nodes in a telecom network *Nature* **629** 573–8
[209] Costa B Scaparra B Wei X Riedl H Koblmüller G Zallo E Finley J Hanschke L and Müller K 2025 Telecom quantum dots on GaAs substrates as integration-ready high performance single-photon sources (arXiv:2505.22886 [cond-mat])
[210] Kaupp J, Reum Y, Kohr F, Michl J, Buchinger Q, Wolf A, Peniakov G, Huber-Loyola T, Pfenning A and Höfling S 2023 Purcell-enhanced single-photon emission in the telecom C-band *Adv. Quantum Technol.* **6** 2300242
[211] Birowosuto M D, Sumikura H, Matsuo S, Taniyama H, van Veldhoven P J, Nötzel R and Notomi M 2012 Fast purcell-enhanced single photon source in 1,550-nm telecom band from a resonant quantum dot-cavity coupling *Sci. Rep.* **2** 321
[212] Chamier F V, Hanel J, Müller C, Li W, Kögler R A and Benson O 2025 Low-noise cascaded frequency conversion of 637.2 nm light to the telecommunication C-band in a single-waveguide device (arXiv:2502.14557 [quant-ph])
[213] Stolk A J *et al* 2024 Metropolitan-scale heralded entanglement of solid-state qubits *Sci. Adv.* **10** ead6442
[214] Mann F, Chrzanowski H M, Gewers F, Placke M and Ramelow S 2023 Low-noise quantum frequency conversion in a monolithic cavity with bulk periodically poled potassium titanyl phosphate *Phys. Rev. Appl.* **20** 054010
[215] Dréau A, Tchebotareva A, Mahdaoui A E, Bonato C and Hanson R 2018 Quantum frequency conversion of single photons from a nitrogen-vacancy center in diamond to telecommunication wavelengths *Phys. Rev. Appl.* **9** 064031
[216] Zaske S *et al* 2012 Visible-to-telecom quantum frequency conversion of light from a single quantum emitter *Phys. Rev. Lett.* **109** 147404
[217] Ghosh S, Galetsky V, Julià Farré P, Deppe C, Ferrara R and Boche H 2024 Existential unforgeability in quantum authentication from quantum physical unclonable functions based on random von neumann measurement *Phys. Rev. Res.* **6** 043306
[218] Borregaard J, Pichler H, Schröder T, Lukin M D, Lodahl P and Sørensen A S 2020 One-way quantum repeater based on near-deterministic photon-emitter interfaces *Phys. Rev. X* **10** 021071
[219] Trusheim M E *et al* 2019 Lead-related quantum emitters in diamond *Phys. Rev. B* **99** 075430
[220] Iwasaki T, Miyamoto Y, Taniguchi T, Siyushev P, Metsch M H, Jelezko F and Hatano M 2017 Tin-vacancy quantum emitters in diamond *Phys. Rev. Lett.* **119** 253601
[221] Neu E, Steinmetz D, Riedrich-Möller J, Gsell S, Fischer M, Schreck M and Becher C 2011 Single photon emission from silicon-vacancy colour centres in chemical vapour deposition nano-diamonds on iridium *New J. Phys.* **13** 025012
[222] Amiri R and Arrazola J M 2017 Quantum money with nearly optimal error tolerance *Phys. Rev. A* **95** 062334
[223] Thiering G and Gali A 2018 Ab initio magneto-optical spectrum of group-IV vacancy color centers in diamond *Phys. Rev. X* **8** 021063
[224] Harris I B W and Englund D 2024 Coherence of group-IV color centers *Phys. Rev. B* **109** 085414
[225] Pieplow G Strocka Y Isaza-Monsalve M Munns J H D and Schröder T 2023 Deterministic creation of large photonic multipartite entangled states with group-IV color centers in diamond (arXiv:2312.03952 [quant-ph])
[226] Torun C G *et al* 2023 SUPER and subpicosecond coherent control of an optical qubit in a tin-vacancy color center in diamond (arXiv:2312.05246)

[227] Debroux R et al 2021 Quantum control of the tin-vacancy spin qubit in diamond Phys. Rev. X 11 041041
[228] Pieplow G, Belhassen M and Schröder T 2024 Efficient microwave spin control of negatively charged group-IV color centers in diamond Phys. Rev. B 109 115409
[229] Senkalla K, Genov G, Metsch M H, Siyushev P and Jelezko F 2024 Germanium vacancy in diamond quantum memory exceeding 20 ms Phys. Rev. Lett. 132 026901
[230] Grimm N, Senkalla K, Vetter P J, Frey J, Gundlapalli P, Calarco T, Genov G, Müller M M and Jelezko F 2025 Coherent control of a long-lived nuclear memory spin in a germanium-vacancy multi-qubit node Phys. Rev. Lett. 134 043603
[231] Ben-David S and Sattath O 2023 Quantum tokens for digital signatures Quantum 7 901
[232] Thomas S E et al 2024 Deterministic storage and retrieval of telecom light from a quantum dot single-photon source interfaced with an atomic quantum memory Sci. Adv. 10 eadi7346
[233] Maaß B, Ewald N V, Barua A, Reitzenstein S and Wolters J 2024 Room-temperature ladder-type optical memory compatible with single photons from semiconductor quantum dots Phys. Rev. Appl. 22 044050
[234] Finkelstein R, Poem E, Michel O, Lahad O and Firstenberg O 2018 Fast, noise-free memory for photon synchronization at room temperature Sci. Adv. 4 eaa8598
[235] Mottola R, Buser G, Müller C, Kroh T, Ahlrichs A, Ramelow S, Benson O, Treutlein P and Wolters J 2020 An efficient, tunable and robust source of narrow-band photon pairs at the 87Rb D1 line Opt. Express 28 3159–70
[236] Craddock A N, Wang Y, Giraldo F, Sekelsky R, Flament M and Namazi M 2024 High-rate subgigahertz-linewidth bichromatic entanglement source for quantum networking Phys. Rev. Appl. 21 034012
[237] Maaß B Barua A Ewald N V Robertson E Gaur K Park S I Rodt S, Song J D Reitzenstein S and Wolters J 2025 On-demand storage and retrieval of single photons from a semiconductor quantum dot in a room-temperature atomic vapor memory (arXiv:2501.15663 [quant-ph])
[238] Wang Y Craddock A N Mendoza J M Sekelsky R Flament M and Namazi M 2025 High-fidelity entanglement between a telecom photon and a room-temperature quantum memory (arXiv:2503.11564 [quant-ph])
[239] Altiere E, Miller E R, Hayamizu T, Jones D J, Madison K W and Momose T 2018 High-resolution two-photon spectroscopy of a $5p^5 6p \leftarrow 5p^6$ transition of xenon Phys. Rev. A 97 012507
[240] Gentile T R, Nacher P J, Saam B and Walker T G 2017 Optically polarized ^{3}He Rev. Mod. Phys. 89 045004
[241] Kornack T W and Romalis M V 2002 Dynamics of two overlapping spin ensembles interacting by spin exchange Phys. Rev. Lett. 89 253002
[242] Shaham R, Katz O and Firstenberg O 2022 Strong coupling of alkali-metal spins to noble-gas spins with an hour-long coherence time Nat. Phys. 18 506–10
[243] Phillips D F, Fleischhauer A, Mair A, Walsworth R L and Lukin M D 2001 Storage of light in atomic vapor Phys. Rev. Lett. 86 783–6
[244] Shinbrough K, Pearson D R, Fang B, Goldschmidt E A and Lorenz V O 2023 Chapter five - broadband quantum memory in atomic ensembles Adv. At. Mol. Opt. Phys. 72 297–360
[245] Heshami K, England D G, Humphreys P C, Bustard P J, Acosta V M, Nunn J and and B J S 2016 Quantum memories: emerging applications and recent advances J. Mod. Opt. 63 2005–28
[246] Sangouard N, Simon C, de Riedmatten H and Gisin N 2011 Quantum repeaters based on atomic ensembles and linear optics Rev. Mod. Phys. 83 33–80
[247] Guo J, Feng X, Yang P, Yu Z, Chen L Q, Yuan C H and Zhang W 2019 High-performance Raman quantum memory with optimal control in room temperature atoms Nat. Commun. 10 148
[248] Robertson E, Esguerra L, Meßner L, Gallego G and Wolters J 2024 Machine-learning optimal control pulses in an optical quantum memory experiment Phys. Rev. Appl. 22 024026
[249] Wang Y, Craddock A N, Sekelsky R, Flament M and Namazi M 2022 Field-deployable quantum memory for quantum networking Phys. Rev. Appl. 18 044058
[250] Robertson E J, Maaß B, Tschernig K and Wolters J 2026 A digital twin of atomic ensemble quantum memory experiments based on an effective quantum channel description Adv. Quantum Technol. 9 e00472
[251] Doosti M, Kumar N, Delavar M and Kashefi E 2021 Client-server identification protocols with quantum PUF ACM Trans. Quantum Comput. 2 197
[252] Che W, Saqib F and Plusquellic J 2015 PUF-based authentication 2015 IEEE/ACM Int. Conf. on Computer-Aided Design (ICCAD) pp 337–44
[253] Delvaux J, Gu D, Schellekens D and Verbauwhede I 2015 Helper data algorithms for PUF-based key generation: overview and analysis IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst. 34 889–902
[254] Shamsoshoara A, Korenda A, Afghah F and Zeadally S 2020 A survey on physical unclonable function (PUF)-based security solutions for internet of things Comput. Netw. 183 107593
[255] Rührmair U, Sehnke F, Sölter J, Dror G, Devadas S and Schmidhuber J 2010 Modeling attacks on physical unclonable functions Proc. 17th ACM Conf. on Computer and Communications Security pp 237–49
[256] Rührmair U and Sölter J 2014 PUF modeling attacks: an introduction and overview 2014 Design, Automation & Test in Europe Conf. & Exhibition (DATE) pp 1–6
[257] Mursi K T, Thapaliya B, Zhuang Y, Aseeri A O and Alkatheiri M S 2020 A fast deep learning method for security vulnerability study of XOR PUFs Electronics 9 1715
[258] Rührmair U, Xu X, Sölter J, Mahmoud A, Majzoobi M, Koushanfar F and Burleson W 2014 Efficient power and timing side channels for physical unclonable functions Int. Worksh. on Cryptographic Hardware and Embedded Systems pp 476–92
[259] Merli D, Heyszl J, Heinz B, Schuster D, Stumpf F and Sigl G 2013 Localized electromagnetic analysis of RO PUFs 2013 IEEE Int. Symp. on Hardware-Oriented Security and Trust (HOST) pp 19–24
[260] Merli D, Schuster D, Stumpf F and Sigl G 2011 Side-channel analysis of PUFs and fuzzy extractors Int. Conf. on Trust and Trustworthy Computing pp 33–47
[261] Xu X and Burleson W 2014 Hybrid side-channel/machine-learning attacks on PUFs: a new threat? 2014 Design, Automation & Test in Europe Conf. & Exhibition (DATE) pp 1–6
[262] Nozaki Y and Yoshikawa M 2018 EM based machine learning attack for XOR arbiter PUF Proc. 2nd Int. Conf. on Machine Learning and Soft Computing pp 19–23
[263] Nilesh K, Geitz M, Döring R, Deppe C and Boche H 2025 Implementation of quantum PUF in future network 2025 IEEE Future Networks World Forum (FNWF) pp 1–6

[264] Skoric B 2009 Quantum readout of physical unclonable functions: remote authentication without trusted readers and authenticated quantum key exchange without initial shared secrets
[265] Julià Farré P, Galetsky V, Belhassen M, Pieplow G, Nilesh K, Boche H, Schröder T, Nötzel J and Deppe C 2026 Secure authentication via quantum physical unclonable functions: a review *Advan. Quantum Technol.* **9**
[266] Amiri Z *et al* 2026 Chapter 18 - quantum technology concepts for 6G networks *6G-life* (Academic) pp 401–22
[267] Amiri Z *et al* 2026 Chapter 19 - quantum technology applications for 6G networks *6G-life* (Academic) pp 423–42
[268] Nilesh K, Deppe C and Boche H 2025 Authentication based on quantum PUF *ICC 2025 - IEEE Int. Conf. on Communications* pp 6796–801
[269] Nilesh K, Deppe C and Boche H 2025 Secure storage and identification using quantum PUF *ICC 2025 - IEEE Int. Conf. on Communications* pp 6802–7
[270] Nilesh K, Deppe C, Geitz M and Boche H 2025 Secure storage for identification using fully quantum PUF *GLOBECOM 2025-2025 IEEE Global Communications Conf.* pp 1974–9
[271] Nilesh K, Deppe C, Geitz M and Boche H 2026 Quantum PUF and quantum biometric-based identification supporting authentication *ICC 2026 (IEEE Int. Conf. on Communications)*
[272] Nilesh K, Deppe C and Boche H 2025 Quantum PUF based secret key generation and secure storage with side information *2025 IEEE Int. Symp. on Information Theory (ISIT)* pp 1–5
[273] Nilesh K, Deppe C and Boche H 2024 Information theoretic analysis of a quantum PUF *2024 IEEE Int. Symp. on Information Theory (ISIT)* pp 3320–5
[274] Nilesh K, Deppe C and Boche H 2025 Secret key generation and storage based on QPUF *2025 IEEE Information Theory Worksh. (ITW)* pp 1–6
[275] Nilesh K, Deppe C and Boche H 2026 Reusability in quantum PUF and biometric sources *ISIT 2026 (IEEE Int. Symp. on Information Theory)*
[276] Nilesh K, Deppe C and Boche H 2024 Quantum PUF and its applications with information theoretic analysis *2024 IEEE 10th World Forum on Internet of Things (WF-IoT)* pp 1–6
[277] Farré P J, Galetsky V, Ghosh S, Nötzel J and Deppe C 2025 Entanglement-assisted authenticated BB84 protocol *Phys. Scr.* **100** 105113
[278] Boche H Deppe C Kumar N and Geitz M 2025 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
[279] Boche H Deppe C Kumar N and Geitz M 2025 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
[280] Goorden S A, Horstmann M, Mosk A P Škorić B, and Pinkse P W H 2014 Quantum-secure authentication of a physical unclonable key *Optica* **1** 421
[281] Tarik F B, Famili A, Lao Y and Ryckman J D 2022 Scalable and CMOS compatible silicon photonic physical unclonable functions for supply chain assurance *Sci. Rep.* **12** 15653
[282] Nocentini S, Rührmair U, Barni M, Wiersma D S and Riboli F 2024 All-optical multilevel physical unclonable functions *Nat. Mater.* **23** 369–76
[283] Shor P W 1994 Algorithms for quantum computation: discrete logarithms and factoring *Proc. 35th Annual Symp. on Foundations of Computer Science* pp 124–34
[284] F O for Information Security 2024 Status of quantum computer development (available at: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Quantencomputer/Entwicklungstand_QC_V_2_1.pdf?__blob=publicationFile&v=)
[285] NIST 2025 Selected algorithms - post-quantum cryptography (available at: https://csrc.nist.gov/Projects/post-quantum-cryptography/selected-algorithms)
[286] NIST 2025 Standardization of additional digital signature schemes - post-quantum cryptography (available at: https://csrc.nist.gov/Projects/pqc-dig-sig/standardization)
[287] 2025 Open quantum safe (OQS) (available at: https://openquantumsafe.org/)
[288] Connell G and Schmidt R 2025 Signal protocol and post-quantum ratchets (available at: https://signal.org/blog/spqr/)
[289] 2025 Google expands post-quantum cryptography support with quantum-safe digital signatures (available at: https://thequantuminsider.com/2025/02/24/google-expands-post-quantum-cryptography-support-with-quantum-safe-digital-signatures/)
[290] 2024 Tuta mail jetzt mit postquantensicherer verschlüsselung (available at: https://tuta.com/de/blog/post-quantum-cryptography)
[291] 2025 Optical communication and networking global market report 2025 (available at: https://www.thebusinessresearchcompany.com/report/optical-communication-and-networking-global-market-report)
[292] 2025 Optical communication and networking market size and share forecast outlook 2025 to 2035 (available at: https://www.futuremarketinsights.com/reports/optical-communication-and-networking-market)
[293] 2026 RF components market report 2026 (available at: https://www.thebusinessresearchcompany.com/report/optical-communication-and-networking-global-market-report)
[294] 2025 The year of quantum: from concept to reality in 2025 (available at: https://www.mckinsey.com/capabilities/tech-and-ai/our-insights/the-year-of-quantum-from-concept-to-reality-in-2025/)
[295] 2026 Information security market size, share, growth, and industry analysis, by type, by application, regional insights and forecast to 2035 (available at: https://www.marketgrowthreports.com/market-reports/information-security-market-108695)
[296] 2025 Cybersecurity market 2026–2034 (available at: https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165)