Agile and Versatile Quantum Communication: Signatures and Secrets

Stefan Richter,[1,2,*,‡] Matthew Thornton,[1,2,†,‡] Imran Khan,[1,2] Hamish Scott,[3] Kevin Jaksch,[1,2] Ulrich Vogl,[1,2]
Birgit Stiller,[1,2] Gerd Leuchs,[1,2] Christoph Marquardt,[1,2] and Natalia Korolkova[3]

[1] *Max Planck Institute for the Science of Light, Staudtstraße 2, 91058 Erlangen, Germany*
[2] *Institute of Optics, Information and Photonics, University of Erlangen-Nuremberg,*
Staudtstraße 7/B2, Erlangen, Germany
[3] *School of Physics and Astronomy, University of St Andrews,*
North Haugh, St. Andrews KY16 9SS, United Kingdom

(Received 27 January 2020; revised 24 November 2020; accepted 18 December 2020; published 24 February 2021)

Agile cryptography allows for a resource-efficient swap of a cryptographic core in case the security of an underlying classical cryptographic algorithm becomes compromised. Conversely, versatile cryptography allows the user to switch the cryptographic task without requiring any knowledge of its inner workings. In this paper, we suggest how these related principles can be applied to the field of quantum cryptography by explicitly demonstrating two quantum cryptographic protocols, quantum digital signatures (QDS) and quantum secret sharing (QSS), on the same hardware sender and receiver platform. Crucially, the protocols differ only in their classical postprocessing. The system is also suitable for quantum key distribution (QKD) and is highly compatible with deployed telecommunication infrastructures, since it uses standard quadrature phase-shift keying encoding and heterodyne detection. For the first time, QDS protocols are modified to allow for postselection at the receiver, enhancing protocol performance. The cryptographic primitives QDS and QSS are inherently multipartite, and we prove that they are secure not only when a player internal to the task is dishonest, but also when (external) eavesdropping on the quantum channel is allowed. In our first proof-of-principle demonstration of an agile and versatile quantum communication system, the quantum states are distributed at GHz rates. A 1-bit message may be securely signed using our QDS protocols in less than 0.05 ms over a 2-km fiber link and in less than 0.2 s over a 20-km fiber link. To our knowledge, this also marks the first demonstration of a continuous-variable direct QSS protocol.

DOI: 10.1103/PhysRevX.11.011038 Subject Areas: Quantum Physics, Quantum Information

I. INTRODUCTION

Throughout history, cryptography has been threatened by advances in mathematics, computational power, and side-channel attacks, and may soon be threatened by quantum computers. The breaking of a cryptosystem, i.e., a suite of cryptographic algorithms and hardware needed to implement a particular security service, has usually triggered the development of new algorithms. These algorithms would subsequently be tested and hardened for years before they could finally be deployed in real-world applications to secure our ever-growing digital infrastructure. The redeployment of cryptographic software and hardware is a costly endeavor.

In the past decade, cryptoagility has emerged as a prospective solution to this problem [1]. One of the core ideas of cryptoagility is to provide a middleware with a two-way interface between the software application layer and the cryptocore or algorithm of the cryptosystem [Fig. 1(a)] so that whenever a new attack vector emerges, the deployed architecture may stay in place and only the vulnerable cryptocore is replaced. This middleware saves valuable deployment time as well as costs to reengineer the whole system. The technical challenge is to design the middleware flexible enough to support novel cryptocores.

Here we suggest how cryptoagility—and the related concept of cryptoversatility, in which multiple cryptographic tasks are performed on the same system—can be translated into quantum communication. Just as the quantum computer hardware provides qubits and gates to run different quantum algorithms on it, we propose that quantum communication hardware may support a diverse range of quantum communication protocols. By providing an abstraction layer

[*] stefan.richter@mpl.mpg.de
[†] mt45@st-andrews.ac.uk
[‡] S. R. and M. T. contributed equally to this work.

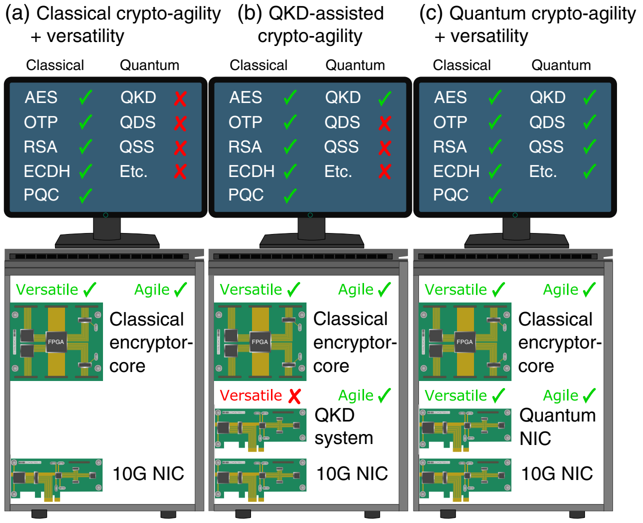

FIG. 1. Comparison between classical cryptoagility and the proposed agile and versatile quantum cryptography architecture. (a) Classical cryptoagility and versatility: Different classical cryptographic algorithms, such as Rivest-Shamir-Adleman (RSA), elliptic curve Diffie-Hellman (ECDHE), advanced encryption standard (AES), one-time pad (OTP), or postquantum cryptography (PQC) can be flexibly combined on the same hardware platform. A network interface card (NIC) is used to send and receive secure communication. (b) QKD-assisted cryptoagility: Classical cryptographic algorithms make use of a pool of secret keys generated by a QKD cryptocore. The quantum functionality is tied to the hardware implementation and cannot be upgraded easily, e.g., to perform QDS or QSS. (c) Quantum cryptoagility: Classical cryptographic algorithms and different quantum protocols can be swapped out and combined as necessary, requiring no changes to the underlying hardware architecture. 10G NIC—10 Gb/s Ethernet network interface card.

between quantum-enabled hardware and the postprocessing stack necessary to realize a quantum communication protocol, quantum versatility can be achieved. For our system, the abstraction layer also implies quantum agility.

In this paper, we explore agile and versatile quantum communication and present an experimental demonstration of the first "seed" system featuring quantum cryptoagility and versatility. Specifically, we investigate continuous-variable quantum digital signatures (CV QDS), quantum secret sharing (CV QSS), and quantum key distribution (CV QKD) on a common platform. The secure protocols which comprise the agile and versatile system use standard telecom sender and receiver techniques, thereby making the system both immediately compatible with deployed infrastructures, be it fiber networks or free-space links, and capable of high sending rates. Quantum coherent states, randomly chosen from an alphabet of four possible phases, are sent through a fiber-optic link, and highly efficient heterodyne detection is used at the receiver.

This first proof-of-principle agile and versatile quantum communication system is thus capable to perform three different quantum cryptographic protocols—QDS, QSS, and QKD—using the same sending and receiving hardware for all protocols. The employed physical system and the advances made in the security proofs of the protocols allow for an implementation compatible with telecom networks. Along with the agility and versatility aspects, this work marks the first demonstration of our CV-QSS scheme and the first demonstration of a CVQDS system with GHz sending rates and record speed to sign a 1-bit message. Our demonstration thus provides a step toward full quantum cryptoagility and versatility, in which several different quantum cryptographic protocols may be implemented on the same hardware deployment with alterations only at the level of classical postprocessing.

Our paper is outlined as follows. In Sec. II, we propose and discuss two alternative approaches toward quantum cryptoagility and versatility, show that existing trends in the QKD and QDS literature may be interpreted in each context, and provide practical indications for when a quantum system may be deemed either agile or versatile. In Sec. III, we discuss three cryptographic tasks—QDS, QSS, and QKD—and introduce several secure protocols which rely on the same physical setups. These protocols are implemented in Sec. IV, and the resulting key rates and figures of merit are displayed in Sec. V. We believe this demonstrates a crucial proof-of-principle step toward full quantum cryptoagility and cryptoversatility. Finally, we discuss our achievements through the lens of agility and versatility in Sec. VI.

II. QUANTUM CRYPTOAGILITY AND VERSATILITY

Classical cryptoagility and versatility are described pictorially in Fig. 1(a), in which a potentially vulnerable cryptocore may be readily replaced without affecting the rest of the deployed system, and in which several tasks can be accomplished via the same encryptor-core. The encrypted communication is then sent on the hardware level via a network interface card. The exact algorithm chosen to accomplish the task can be swapped and patched without knowledge of the end user. We suggest here two different approaches to consider a *quantum* cryptosystem as agile or versatile.

One can think of a first type of agility as classical cryptoagility assisted by QKD. Here, a QKD system acts as a black box that delivers fresh shared keys to classical cryptography applications; see Fig. 1(b). The advantage is that the middleware does not have to care about key generation or the QKD protocol itself. The downside is that although the generated key can be used for many different tasks, the QKD system itself may not be repurposed to run any other quantum protocol on it, limiting its versatility and potentially imposing an additional resource overhead.

The second approach, quantum cryptoagility + versatility, is depicted in Fig. 1(c). Compared to the first approach, the QKD system is replaced by a quantum network interface card (QNIC). The QNIC is able to perform multiple quantum communication protocols (e.g., QDS, QSS, or QKD) on the same hardware platform. It communicates its hardware capabilities through an interface to the protocol layer, where the matching protocol for the user task at hand is chosen. Such a layer stack is illustrated in Fig. 2 and demonstrated later in this paper. Note that here the choice of a particular quantum cryptographic application is reduced merely to a software and/or firmware update. A quantum cryptosystem structured like this carries direct analogy with the classical agile cryptosystem of Fig. 1: The hardware and agile interface stay the same, and only the cryptocore, classical, as in Fig. 1(a), or quantum, as in Fig. 1(c), changes. This second approach to agility can be thought of as a choice of quantum "app," and therefore, also allows versatile usage of the quantum hardware.

This second agile approach carries an advantage of economic use of resources. QKD requires resource-intensive postprocessing to generate a secure key, and real channel parameters (e.g., noise, losses) may be too restrictive to allow for efficient secret key distillation. Some tasks, however, can be performed directly without first generating a shared secure key via QKD. A good example is QDS protocols, in which a secure signature is created straight from a raw quantum state exchange, consuming fewer resources than an equivalent QKD protocol [2]. Thus, a versatile system capable of performing both QDS and QKD will in general allow for a more efficient use of quantum resources when full QKD is neither possible nor necessary.

To make explicit the ideas discussed above, we propose the terms quantum cryptoagility and quantum cryptoversatility to mean the following (see Fig. 2).

(i) Quantum cryptoagility: As a minimal requirement, a quantum cryptosystem can be considered agile if it exposes its cryptographic capabilities through a stable and opaque interface to the end user, allowing a compromised implementation to be modified without requiring changes to user software. A given cryptosystem may be agile up to different degrees, depending on which implementation components can be modified cost effectively after deployment. It is typically easy to update a system's software, harder to update or replace firmware, and quite difficult and costly to replace hardware. The transfer of the cryptoagility idea to the field of quantum cryptography slightly changes its meaning since the security of the quantum cryptocore can be proven information theoretically. However, considering practical implementation security and the emergence of novel quantum cryptographic protocols and performance improvements to existing ones, an agile strategy seems prudent.

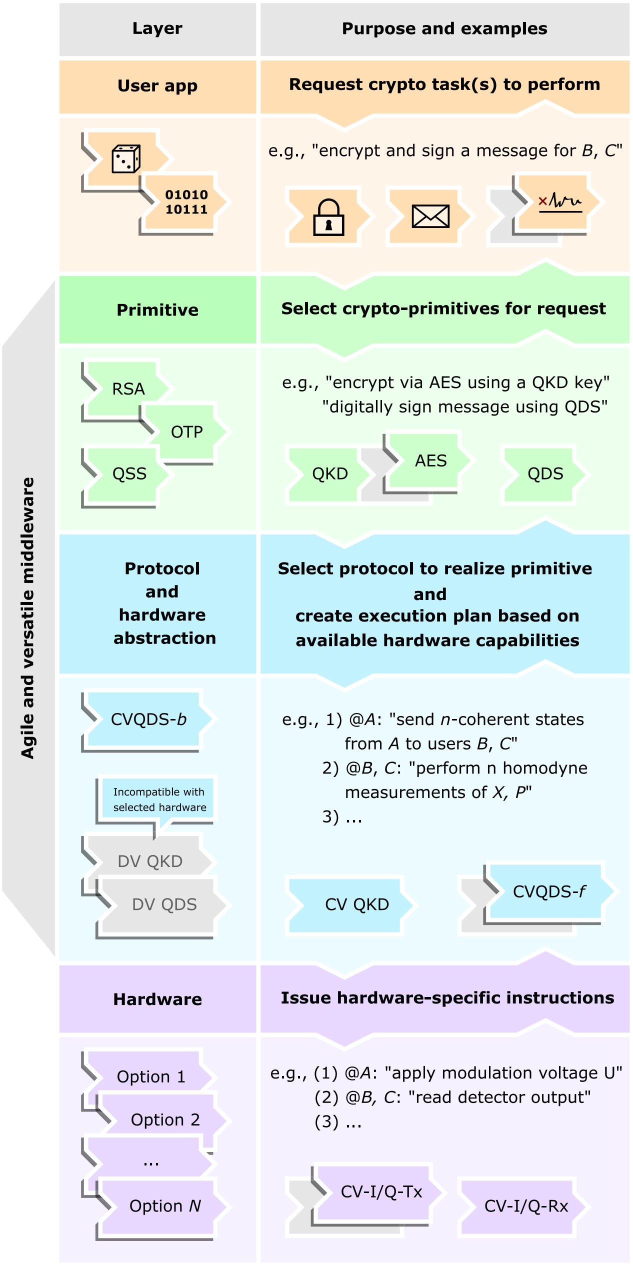
Layer
Purpose and examples
User app
Request crypto task(s) to perform
01010
10111
e.g., "encrypt and sign a message for *B*, *C*"
Primitive
Select crypto-primitives for request
RSA
OTP
QSS
e.g., "encrypt via AES using a QKD key"
"digitally sign message using QDS"
QKD
AES
QDS
Agile and versatile middleware
Protocol and hardware abstraction
Select protocol to realize primitive and create execution plan based on available hardware capabilities
CVQDS-*b*
Incompatible with selected hardware
DV QKD
DV QDS
e.g., 1) @*A*: "send *n*-coherent states from *A* to users *B*, *C*"
2) @*B*, *C*: "perform n homodyne measurements of *X*, *P*"
3) ...
CV QKD
CVQDS-*f*
Hardware
Issue hardware-specific instructions
Option 1
Option 2
...
Option *N*
e.g., (1) @*A*: "apply modulation voltage U"
(2) @*B*, *C*: "read detector output"
(3) ...
CV-I/Q-Tx
CV-I/Q-Rx

FIG. 2. A layer-based description of an agile and versatile quantum cryptosystem showing how its modular and decoupled components can be swapped out and recombined similarly to puzzle pieces. Quantum cryptoagility and versatility can both be realized by introducing a middleware (a collection of interface layers) between the user application (yellow) and quantum hardware (purple) layers. This requires that the hardware drivers expose a set of standardized functions to the layers above it. The middleware can then select suitable quantum cryptoprimitives and hardware-compatible protocols to fulfill a given user request for a given cryptographic task. In this manner, the middleware layers generalize and extend the functions of a key management system. For some of the acronyms in this figure, please refer to the caption of Fig. 1. CV-I/Q-Tx and CV-I/Q-Rx denote sender (Tx) and receiver (Rx) hardware modules capable of performing continuous-variable (CV) quadrature (I/Q) modulation and detection.

(ii) Quantum cryptoversatility: We consider a quantum system to be versatile if it implements different cryptographic tasks (e.g., QKD, QDS, QSS) on the same hardware platform and makes these tasks available to the user through a common interface. In a versatile quantum cryptosystem, the selection of a quantum protocol to fulfill the requested cryptographic task happens on the middleware level; see Fig. 2. Since the inner workings of the specific task is only of concern for the manufacturer but not the user, agility is also implied. The converse may not hold true.

Quantum cryptoagility and versatility may also be relevant topics for ongoing standardization efforts, such as the ETSI QKD ISG 004 and 014 standards [3,4] that define the interface between applications and key providers such as a key management system or QKD systems. Based on these two standards, quantum cryptoagility and versatility could eventually be added as another standard in a lower abstraction layer to form a full stack in the future.

The idea of a layered architecture for QKD-secured communication systems is a natural one and has been investigated before, e.g., in Refs. [5–8]. For example, large quantum networks of quantum senders and receivers, classical communication lines, and trusted or untrusted central nodes have been considered in Ref. [5], where the study of different network topologies and of the relationships between existing classical and future quantum networks is important. Further, quantum analogs to the TCP/IP (transmission control protocol/internet protocol) stack are discussed in Refs. [7,8], and quantum repeater links are also considered, allowing for additional teleportation-based protocols over the network. In contrast to these outlooks, our focus is on the layered stack required for individual nodes in the network and is complementary to these full-network approaches. Notably, to our knowledge, neither CV- nor discrete-variable (DV) -based systems capable of selectively performing several different quantum primitives on the same hardware have been demonstrated so far.

In the remainder of this paper, we thus demonstrate the versatility of two quantum systems by showing that the choice of quantum cryptographic task can be made entirely at the software level. Because of the employed middleware, which provides an innate separation between hardware and user layers, agility of our system is also implied.

III. BEYOND QKD: SIGNATURES AND SECRETS

In addition to the usual bipartite QKD, and in order to make our notion of quantum cryptoagility and versatility concrete, we consider the following multipartite tasks.

(i) QDS: allows for the secure authentication of a classical message. It has been shown that because of its small overhead, QDS may run over channels for which QKD is insecure [2].

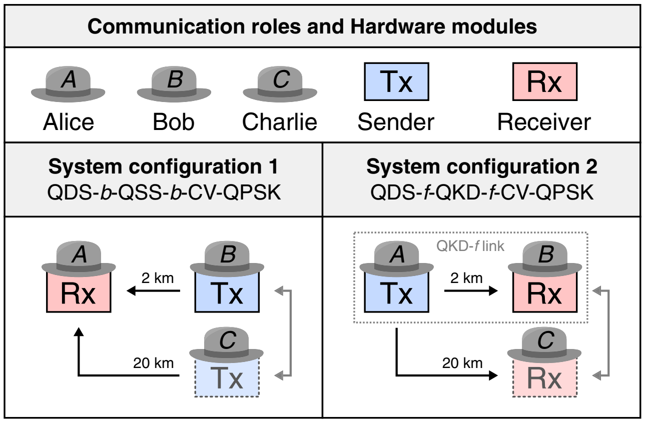

FIG. 3. The sender (Tx) and receiver (Rx) modules may be reconfigured to make Alice either the sender (“f configuration”) or receiver (“b configuration”) of quantum states. Each setup may be immediately considered *versatile*, since once either the f or b configuration is chosen, multiple different cryptographic tasks may be performed. *Agility* is implied by separation of the user and hardware layers through a stable and opaque interface (see Fig. 2). Shading and a dashed outline are used to indicate that a single device may be used to emulate two different end points as we describe in Sec. IV.

(ii) QSS: allows for the secure distribution of a classical secret among a conspiracy of potentially dishonest recipients.

In the spirit of quantum cryptoagility and versatility introduced earlier [Figs. 1(c) and 2], we explicitly propose two communication systems, i.e., configurations of the same underlying hardware, which can each fulfill multiple quantum cryptographic tasks. The two systems may thus both be considered as agile and versatile, and we denote them QDS-b-QSS-b-CV-QPSK (QPSK, quadrature phase-shift keying) and QDS-f-QKD-f-CV-QPSK; see Fig. 3. The labels indicate which cryptographic tasks (QDS, QSS, or QKD) they support; the underlying quantum states that they use (a CV-QPSK alphabet) and in which direction (f “forward” or b “backward”) the quantum states are exchanged. Labeling agile and versatile quantum cryptosystems by the hardware components they are based on and the protocols they support might prove useful in later efforts to standardize interfaces and provide some comparability between different implementations.

The agile and versatile approaches can, in principle, be applied to both discrete- and continuous-variable systems with the agile middleware (Fig. 2) ensuring that the end user does not need to care about whether (quasi)single photons or phase-encoded coherent states are used. For the remainder of the paper, we focus on the CV platform, noting that the use of the QPSK alphabet and heterodyne detection renders our system highly compatible with standard telecom infrastructure, potentially paving a way to integrating agile and versatile quantum cryptosystems into deployed communication links which run with up to 100-GHz sending rate [9,10]. With this compatibility in mind, the protocols presented here sit within the field of CV quantum cryptography, which aims toward fast sending rates over metropolitan distances. The four individual protocols each provide asymptotic security against a dishonest player performing a collective beam-splitter or entangling-cloner attack. Descriptions of each protocol and key details in their security proofs are sketched below, while the reader is referred to the Appendixes for technical details.

A. First agile and versatile system QDS-*b*-QSS-*b*-CV-QPSK

The first agile and versatile system we consider relies on the b configuration, with Bob and Charlie as the senders (Tx) of quantum states, while Alice performs heterodyne detection (Rx) (Fig. 3). This QDS-*b*-QSS-*b*-CV-QPSK system is capable of performing both QDS and QSS tasks via the protocols QDS-*b* and QSS-*b*, which we describe below. Our experiment detailed in Sec. IV also marks the first demonstration of CV QDS over insecure quantum channels.

1. The QDS-b protocol

The very first QDS scheme was proposed in Ref. [11] and required a quantum memory. In the last two decades, DV-QDS protocols have first lifted this requirement [12–15] and then also have lifted the need for a trusted quantum channel [2,16] and have brought their hardware requirements closer to those of QKD [17]. Recently, DV-QDS implementations based on deployed networks have been demonstrated successfully over metropolitan distances [18–22]. Indeed, in several QDS papers, a nascent form of quantum versatility is mentioned, either explicitly [18,20,23] or implicitly [19,21], but so far the comparison has always been that the distribution of quantum states for QDS is analogous—or in some cases identical—to that required for QKD. For example, Ref. [18] differs from differential-phase-shift QKD only in postprocessing. Similarly, one protocol in Ref. [17] is designed specifically to share sender and receiver with QKD, while another requires first full QKD and then classical communication to sign a message. Despite these recognitions, to our knowledge, the full utility of applying the idea of quantum cryptoagility and versatility to a deployed quantum network has not yet been explored, nor have additional cryptographic protocols been studied in this framework.

Unlike those preceding QDS protocols, in which Alice was the sender of quantum states, in QDS-*b*, Bob and Charlie are the senders of quantum states, while Alice is the recipient [Fig. 3(b)]. This reversal of roles allows QDS-*b* to be performed on our first agile and versatile system QDS-*b*-QSS-*b*-CV-QPSK.

The protocol QDS-*b* runs as follows:

(i) For each future message $m \in \{0, 1\}$, which Alice wishes to securely sign, Bob and Charlie both send Alice a sequence, length L, of coherent states chosen randomly from the QPSK alphabet. Bob and Charlie each keep a record of which states they have sent.

(ii) Alice performs heterodyne detection on each received state and forms eliminated signatures $A^m_{B,C}$ by writing down which two states from QPSK are the *least compatible* with her measurement outcome, that is, which states have the smallest conditional probability of being sent.

(iii) Bob and Charlie swap a random half of their signature elements in order to guard against dishonest Alice [24]. Bob (Charlie) now possesses signatures X^m_B (X^m_C), which consist of two halves of length $L/2$, one of which was generated by Bob (Charlie), and one of which was received during the swapping.

(iv) Later, Alice sends her message m and the corresponding $A^m_{B,C}$, first to Bob. Bob compares his record of which states were sent and counts the number of mismatches. A mismatch occurs if Alice claims to have eliminated a state which Bob indeed did send. Provided there are sufficiently few mismatches, he accepts m as genuine and forwards to Charlie, who likewise accepts or rejects by counting the number of mismatches.

A QDS scheme must be secure against both *forging* attacks, in which a dishonest Bob will attempt to convince Charlie that a message is genuine, and *repudiation* attacks, in which a dishonest Alice will attempt to force Bob and Charlie to disagree about the message's validity. Furthermore, noting that a QDS protocol which declares all possible signatures as fake may be considered trivially secure, we require that the protocol should succeed if all parties are honest; that is, it should be *robust*.

The full security proof of QDS-*b* may be found in Appendix A. Here we simply note that security against forgery is guaranteed by picking a highly nonorthogonal alphabet of coherent states; i.e., the amplitude of the QPSK alphabet should be sufficiently small.

The main security result for QDS-*b* is the following expression for the binary entropy h:

$$h(p_e) \geq 1 - \chi \tag{1}$$

of a forging Bob's probability p_e to induce a mismatch with Charlie. The χ denotes Bob's Holevo information about Charlie's distributed state. Then the final signature length L required to sign a 1-bit message with ϵ_{fail} probability of failure is implicitly given by [25,28]

$$\epsilon_{\mathrm{fail}} \leq 2\, \exp\left[-\frac{(p_e - p_{\mathrm{err}})^2}{16} L\right], \tag{2}$$

provided that security parameter $p_e - p_{\mathrm{err}} > 0$, where p_{err} is an honest player's mismatch probability, which can be estimated during the protocol. In other words, QDS-*b* is secure against any attack provided that a dishonest player causes more mismatches than an honest player.

The protocol QDS-*b* performs well over channels with low loss and low excess noise, but in order to reach feasible signature lengths over realistic channels, we employ the *postselection* technique [29]. To our knowledge, this is the first time this technique has been leveraged in the context of QDS. Alice will discard measurement outcomes for which she has a large probability of mismatch, thereby reducing p_{err}. Since a forger will attack the sender (Tx) of quantum states rather than Alice, the probability p_e is unaffected by postselection. The security parameter $p_e - p_{\mathrm{err}}$ may then be readily altered simply by choice of postselection region. The full postselection calculation is found in Appendix B.

The experimental implementation of the protocol is presented in Sec. IV, and the signature length L required to sign a 1-bit message to $\varepsilon_{\mathrm{fail}}$ chance of failure is given in Sec. V.

2. The QSS-b protocol

A secret-sharing scheme allows for Alice to distribute a classical secret between recipients Bob and Charlie. Bob and Charlie should be able to perfectly reconstruct the secret when they behave honestly, while either Bob or Charlie working alone should gain no information.

Although some existing *classical* secret-sharing schemes are already information-theoretically secure [30], they encounter problems when distributing the shares of the secret across insecure channels and may fall prey to an eavesdropper with a sufficiently powerful quantum computer. A potential solution is to employ a QSS protocol which uses quantum resources in order to share the classical secret [31,32]. For example, the scheme put forward in Ref. [31] relies on large multipartite entangled states for distillation of keys between the dealer, Alice, and a degree of freedom shared between recipients. In another protocol [32], security is reached via a "round-robin" distribution stage with each player interacting with the same transmitted quantum state.

Crucially, unlike these approaches which require dedicated hardware setups or distribution of large entangled states, the QSS-*b* protocol presented here accomplishes the secret-sharing task using only distribution of QPSK coherent states and heterodyne detection, and thus forms an integral part of our first agile system QDS-*b*-QSS-*b*-CV-QPSK (Fig. 3). We demonstrate in Sec. V that QSS-*b* attains a larger key rate than an equivalent information-theoretically secure classical secret-sharing scheme using two continuous-variable QKD setups.

In the QSS-*b* protocol, the dealer (Alice) is assumed honest, while either one of Bob or Charlie may be dishonest. Additionally, a dishonest fourth player, Eve, may be present. For now, we assume that a dishonest Bob or Charlie will send states only from the QPSK alphabet, though this could be relaxed in future work.

The protocol QSS-*b* runs as follows:

(i) Bob and Charlie send sequences of coherent states to Alice, which are independently and randomly chosen from the QPSK alphabet. Alice performs heterodyne measurement of phase and records her outcomes $A_B, A_C \in \mathbb{C}$. Bob and Charlie keep a record X_B, X_C of which states they have sent.

(ii) Alice forms a variable $X_A \simeq F(A_B, A_C)$ which is some function F of her measurement results. She then encodes the secret using the X_A and makes the encoded secret publicly available.

(iii) Later, when Alice wishes to allow Bob and Charlie to reconstruct the secret, she leaks the function F and enough information to perform a reconciliation procedure between her X_A and the $X_A \simeq F(X_B, X_C)$ generated by Bob and Charlie. The reconciliation proceeds as in regular QKD.

(iv) Bob and Charlie, by working together to form and reconcile $F(X_B, X_C)$, gain a copy of Alice's key. Thus, they are able to decrypt her message.

The protocol should prevent dishonest players from reconstructing the secret unless they collaborate with the honest player. Specifically, they are forced to collaborate by Alice's choice of F which requires information from both players to reach the key. The function F can be arbitrarily chosen and optimized over, though for concreteness we choose F to be linear, i.e.,

$$F(X_B, X_C) = gX_B + hX_C \tag{3}$$

for $g, h \in \mathbb{R}$; Alice is free to choose a more general F if it is optimal for her setup.

The security proof for QSS-*b* is found in Appendix C. The main security result is a calculation of the key rate κ generated between Alice and a Bob-Charlie collaboration. The key rate corresponds to the number of secure key bits which may be encrypted per channel use, i.e., after both Bob and Charlie have sent a state. One channel use thus corresponds to distribution of *two* coherent states.

In the presence of dishonest Eve and honest Bob or Charlie, the key rate κ is given by the following Devetak-Winter bound [31,33]

$$\kappa \geq I(X_B, X_C : X_A) - \chi\ (X_A : \mathbb{E}) \tag{4}$$

relating the mutual information I between Bob or Charlie's classical information $X_{B,C}$ and Alice's information X_A, and the Holevo information χ which Eve's quantum system $\mathbb{E}$ holds about X_A.

More general bounds to guard against dishonest Bob or Charlie are given in the Appendix. The QSS-*b* protocol is implemented in Sec. IV, and the key rate to allow for secure secret sharing is given in Sec. V.

B. Second agile and versatile system QDS-f-QKD-f-CV-QPSK

In addition to our first agile and versatile system described above, which is capable of readily switching between QDS and QSS tasks, we demonstrate that cryptographic protocols which already exist in the literature may be viewed through an agility or versatility lens. We therefore turn to consider a second agile and versatile system denoted QDS-f-QKD-f-CV-QPSK, which is capable of performing either QDS or QKD tasks in a "forward" configuration (Fig. 3).

A QDS protocol in which Alice sends quantum coherent states was previously considered in Ref. [28]. There, it is Bob and Charlie who form eliminated signatures and check for mismatches between their eliminated signatures and Alice's declaration of which states she sent. We here denote this protocol QDS-f.

To go beyond Ref. [28], we apply the postselection technique to QDS-f, which decreases the number of quantum states L required to sign a message, particularly in the presence of channel noise. Since (in contrast to QDS-b) it is now Bob and Charlie who heterodyne, rather than Alice, both terms p_e and p_{err} now change with the choice of postselection region. The effects of postselection on QDS-f and key steps from the security proof are detailed in Appendix B.

Finally, we round off the second agile and versatile system by noting that the discrete-modulation QPSK QKD protocol analyzed, e.g., in Ref. [34] may be readily implemented using the same hardware setup as QDS-f without requiring reconfiguration. This protocol, which we here denote QKD-f, may be performed between either Alice-Bob or Alice-Charlie. The full security proof is found in Ref. [34], and we display the estimated maximum rate of secure key generation for our system under QKD-f in Sec. V.

IV. EXPERIMENT

An optical sender (Tx) and receiver (Rx) module as shown in Fig. 4 is used to experimentally investigate the performance of the protocols QDS-f, QKD-f, QDS-b, and QSS-b. Depending on the required configuration, Tx and Rx take on the roles indicated in Fig. 3. Our protocols do not require the quantum state exchange between parties $A-B$ and $A-C$ to be simultaneous. For this demonstration, we thus emulate the deployment of identical Tx and Rx hardware at B and C by instead sequentially linking a single Rx and Tx using a 2-km (−0.65-dB) or 20-km (−4.75-dB) SMF-28 optical fiber channel. Each state exchange between $A-B$ and $A-C$ is performed as an independent subexperiment.

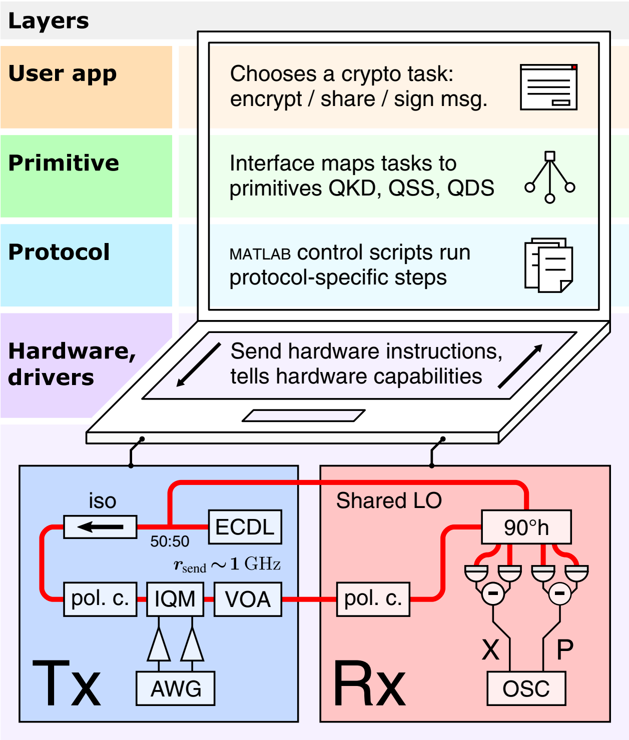
Layers
User app
Primitive
Protocol
Hardware, drivers
Chooses a crypto task: encrypt / share / sign msg.
Interface maps tasks to primitives QKD, QSS, QDS
MATLAB control scripts run protocol-specific steps
Send hardware instructions, tells hardware capabilities
iso
ECDL
50:50
$r_{\text{send}} \sim 1$ GHz
pol. c.
IQM
VOA
AWG
Tx
Shared LO
90°h
pol. c.
X
P
OSC
Rx

FIG. 4. Top: schematic drawing indicating how the different abstraction layers of quantum cryptoagility and versatility (see Fig. 2) are realized in our demo system as different pieces of software running on a laptop connected to our sender (Tx) and receiver (Rx) hardware. Bottom: the Tx and Rx modules used to perform four distinct quantum protocols, assuming different communication roles A, B, or C as shown in Fig. 3. ECDL, external-cavity diode laser; iso, isolator; VOA, variable optical attenuator; IQM, I/Q modulator; pol.c., polarization controller; AWG, arbitrary waveform generator; LO, local oscillator; 90°h, 90°hybrid; OSC, oscilloscope

(i) Sender module (Tx): A Pure Photonics PPCL-300 external cavity diode laser with a linewidth of 15 kHz tuned to a wavelength of 1550 nm acts as an optical carrier. Using a Fujitsu DP-QPSK 40-Gbps LiNbO$_3$-integrated I/Q modulator driven at a rate of 1 GHz by a Keysight M8195A arbitrary waveform generator, the sender randomly prepares pulses of coherent states chosen from the QPSK alphabet $\{|\pm\alpha_0\rangle, |\pm i\alpha_0\rangle\}$. These states are attenuated to a chosen output amplitude $\alpha < \alpha_0$ with a variable optical attenuator and sent to the receiver.

(ii) Receiver module (Rx): The receiver module interferes the incoming signal with a local oscillator in an integrated Kylia COH24-X 90° hybrid and performs heterodyne detection of the electric field quadratures X and P for each state using two Discovery DSC-R412 balanced optical receivers with an analog 3-dB bandwidth of 20 GHz. For the purposes of this demonstration, the local oscillator is sourced from the carrier laser and transmitted to the receiver using an additional fiber. The optical receiver outputs are digitized and processed on a Tektronix

TABLE I. Figures of merit for the experimental runs. QDS signature lengths (L) and signing times (t) required to sign a 1-bit message for security level of $\varepsilon = 0.01\%$. The QSS and QKD key rates correspond to the maximum estimated number of bits of secure key which may be generated per use of the quantum channel. In QSS-b, one channel use corresponds to distribution of *two* quantum states, one from Bob and one from Charlie, and so we display 2κ for fair comparison with QKD.

Experiment				QDS-b		QDS-f		QSS-b	QKD-f
Run	d (km)	$\bar{\alpha}(\sqrt{\text{snu}})$	$\xi(\%)$	$L(\text{bits}^{-1})$	t(ms)	$L(\text{bits}^{-1})$	t(ms)	2κ	κ
1	2	0.64	2.7	5.70×10^6	5.7	4.79×10^4	0.048	0.3726	0.3479
2	20	0.67	1.9	$(\cdots)$	$\cdots$	2.26×10^9	2260	0.1058	0.1024
3	20	0.55	2.1	$(\cdots)$	$\cdots$	1.37×10^8	137	0.0858	0.0840
4	20	0.64	1.7	$(\cdots)$	$\cdots$	2.08×10^8	208	0.1004	0.0976

DPO77002SX digital sampling oscilloscope using a sampling rate of 25 GS/s. Digital signal processing (DSP) is applied to the quadrature time traces consisting of a high-pass-filtering operation to eliminate low-frequency noise components and a phase recovery step using reference states.

Experiments are performed for different modulation amplitudes α, as indicated in Table I. For each state exchange, a total of 1.92×10^6 states are sent in frames of 64, with four bright phase reference states at the start of each frame. Of those, 1.54×10^6 states or 80.2% remain after the digital signal processing. A phase-space diagram of the quantum state constellation and a section of the measured raw data [35] can be seen in Fig. 5.

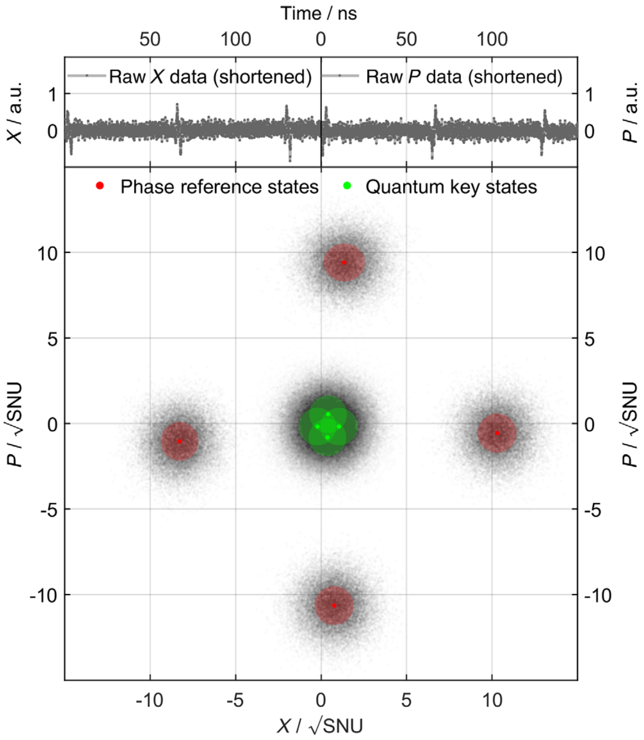

FIG. 5. Top: raw quadrature data traces produced by our quantum communication system running QPSK modulation [35]. Bottom: a resulting phase-space constellation diagram after digital signal processing is applied to the raw data. Shaded circles indicate the means and variances of the coherent states sent and received, including quantum key states (green) and auxiliary phase reference states (red). SNU: shot noise unit, defined as the quadrature variance which is measured when no signal input is applied

V. RESULTS

The agile and versatile system QDS-b-QSS-b-CV-QPSK is investigated over the 2-km fiber link with average $\bar{\alpha} = 0.64$ and an excess noise in the channel of 2.7% in the laboratory conditions that represent the first targeted implementation of an agile and versatile quantum communication system. We obtain practical figures of merit for each of the protocols (5.7 ms to sign a 1-bit message for QDS-b and $2\kappa = 0.3726$ key rate for QSS-b) listed in Table I. The protocol QSS-b is also investigated in several 20-km experimental runs for different α and different levels of excess noise with key rate up to $2\kappa = 0.1058$, completing the first demonstration of our practical CV QSS (Fig. 6).

The second agile and versatile system QDS-f-QKD-f-CV-QPSK is investigated over a 2-km laboratory fiber link and in several runs over 20 km for different amplitudes and different levels of excess noise in order to explore performance at larger distances, which are less favorable for CV communication systems. Alongside the agility and versatility aspects, this experiment demonstrates the fastest-to-date QDS system at intracity distances, allowing to sign a 1-bit message in less than 0.05 ms over a 2-km fiber link. It also allows for a secure performance of the agile system at 20 km distance with feasible signature lengths (Fig. 7) with signing times close to the recent best DV experiments (Fig. 8).

The maximum calculated secure key rates for QKD-f for this agile and versatile system are displayed in Fig. 7 and Table I. The maximum obtainable QKD key rate for the system is $\kappa = 0.1024$.

We detail and benchmark the different aspects of the experimental performance of the two agile and versatile systems in what follows.

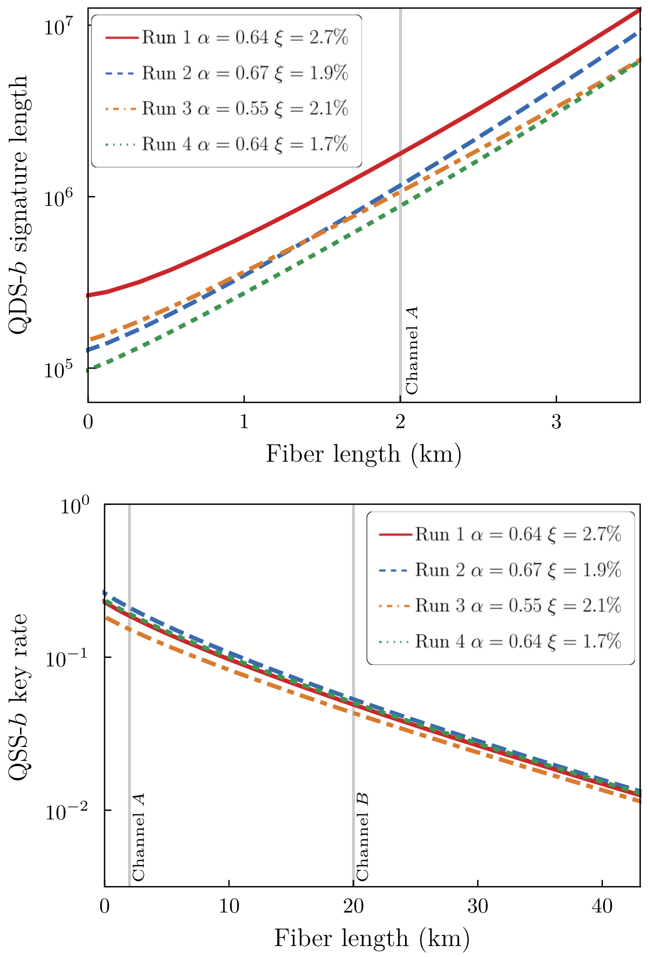

FIG. 6. Performance of agile and versatile system QDS-b-QSS-b-CV-QPSK. Top: QDS signature lengths under protocol QDS-b with an entangling-cloner attack. The signature lengths at a distance of 2 km remain modest both in the ideal (above) and experimental realizations (Table I), and the system is robust to choice of α. Bottom: maximum calculated QSS key rates under protocol QSS-b with a dishonest Eve performing a beam-splitter attack, and either Bob or Charlie dishonest. The key rate is robust to variations in α and remains large even for our 20-km channel. Solid (red), dashed (blue), dot-dashed (orange), and dotted (green) lines correspond to the performance deduced by parameters from experimental runs 1, 2, 3, and 4, respectively. Vertical grid lines depict loss levels over experimental channels A and B corresponding to fiber lengths 2 km (0.65-dB loss) and 20 km (4.75-dB loss).

A. Settings for the system runs

We perform the experiment detailed above over two different channels which we denote channel A and channel B corresponding to 2- and 20-km fiber length, respectively. During the experiment, measurement outcomes corresponding to the parameters detailed in Table I are obtained. Each element of the QPSK alphabet has slightly different sending amplitude in each experiment, and we display the average amplitude $\bar{\alpha}$ in the table. The excess noise ξ above the shot noise is calculated for each quadrature x, p and $\xi = \max\{\xi_x, \xi_p\}$ is taken as a worst-case scenario. We now process our measured data with reference to each of the four quantum protocols and thus demonstrate quantum cryptoversatility, thereby implying agility for our systems.

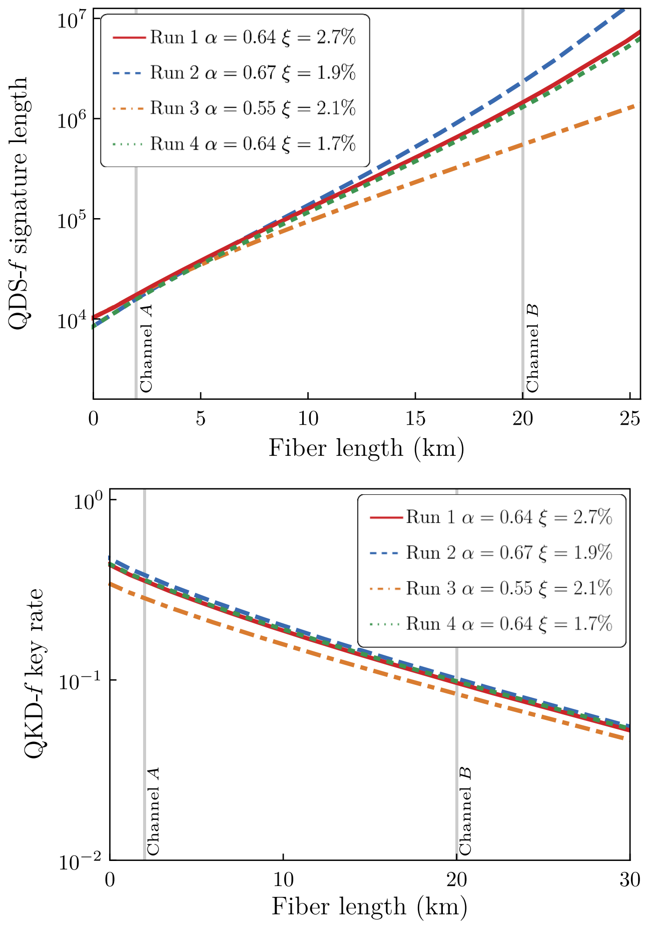

FIG. 7. Calculated performance of agile and versatile system QDS-f-QKD-f-CV-QPSK. Top: QDS signature lengths under protocol QDS-f under a beam-splitter attack. Signature lengths L at 20 km (channel B) remain feasible with both ideal (above) and experimental realizations (Table I). At 2 km (channel A), the protocol requires small signature lengths and thus is the fastest QDS protocol over comparable distances (Fig. 8). Bottom: calculated maximum QKD key rates under protocol QKD-f with a beam-splitter attack. Both: vertical grid lines denote channel losses at which we perform an experiment. Solid (red), dashed (blue), dot-dashed (orange), and dotted (green) lines correspond to experiments 1, 2, 3, and 4, respectively, and vertical grid lines depict loss levels over experimental channels A and B corresponding to fiber lengths 2 km (0.65-dB loss) and 20 km (4.75-dB loss).

B. First agile and versatile system QDS-*b*-QSS-*b*-CV-QPSK

In the first agile and versatile system QDS-b-QSS-b-CV-QPSK, the sender module Tx is understood to play the role of either Bob or Charlie, while Rx plays the role of Alice.

1. *QDS-b*

Signature lengths are calculated using data parameters from Table I with the postselection region $\mathcal{R}(\Delta_r)$ optimized at each channel loss; see Appendix. B. In the ideal case, the probability p_{err} is calculated using Eq. (B3) under the model described in Appendix B, which includes both channel excess noise ξ ascribed to Eve and a detector efficiency of 50% which Eve cannot exploit. We allow Eve to perform the entangling-cloner attack [28] which is expected to be optimal in the limit $\alpha \rightarrow 0$, and close to optimal for the small α's used here, and probability p_e may be estimated as in Appendix A once the worst-case α and ξ are estimated from the data. The ideal signature lengths for QDS-b are displayed in Fig. 6.

More realistic signature lengths may be calculated by taking into account in the estimate of p_e the actual amplitudes and sending probabilities which Tx sent, rather than an average, and by measuring p_{err} directly from the output of Rx. The p_{err} calculated this way takes into account all sources of detector loss and trusted noise which will increase p_{err}, and thus, the measured L will be larger than those in Fig. 6.

Further, in comparisons between commercial implementations, the implicit Bob-Charlie QKD channel for the swapping stage of the QDS protocol should be included in a figure of merit to give a realistic accounting of the resource requirements. We stress, however, that the aim of our QDS analysis is primarily to give a comparison with recent QDS schemes (see Fig. 8). Therefore, our approach to the classical postprocessing focuses on the QDS distribution stages (following the QDS literature [2,18,25–27]) in order to allow for this comparison.

For experimental run 1 over the 2-km channel under entangling-cloner attack, signature length $L = 5.7 \times 10^6$ is required to sign a single bit (Table I). However, even at 20 km, QDS-b can still be made secure by choosing a large postselection region with $\Delta_r \gg 1$, but for loss levels more than approximately 2 dB, the signature length required becomes impractically large.

2. *QSS-b*

For our secret-sharing protocol QSS-b (Fig. 6), the Holevo information is calculated by estimating channel transmission T and excess noise ξ from the data and assuming the dishonest players perform a beam-splitter attack. In our reported results, we optimize over $g, h \in \mathbb{R}$ which parametrize the function $F(X_B, X_C) = gX_B + hX_C$.

The mutual information is calculated by calculating the probability $p(x|\alpha_k)$ of measuring $x \in \mathbb{C}$ at the output when coherent state α_k is sent, noting again that the realistic nonidentical amplitudes and probabilities of the implemented QPSK alphabet may be readily included. Further details are found in Appendix C.

The maximum QSS key rates are calculated from the measured experimental parameters (Table I). We see that twice the key rate 2κ is greater than the comparable key rate κ for QKD-f (remembering that one channel use is defined differently between QKD and QSS). In other words, QSS-b outperforms pairwise QKD by consuming fewer quantum resources. Protocol QSS-b is therefore preferable over a classical information-theoretically secure protocol which can be performed over pairwise QKD-encrypted channels.

C. Second agile and versatile system QDS-*f*-QKD-*f*-CV-QPSK

For the second agile system QDS-f-QKD-f-CV-QPSK, Tx plays the role of Alice while Rx plays either Bob or Charlie.

1. *QDS-f*

The performance of protocol QDS-f is displayed in Fig. 7 under a beam-splitter attack. The excess noise and detector efficiency from experiment are included, and p_e and p_{err} are calculated via analogous methods to QDS-b above. We see that in the ideal analysis of Fig. 7, protocol QDS-f allows for very small signature lengths $\mathrm{O}(10^4)$ at 2 km, while at 20 km the predicted lengths are still very modest at $\mathrm{O}(10^6)$.

For small channel loss, the required L is roughly invariant over a broad range of α, which suggests that QDS-f is robust to experimental differences and is thus easy to implement on an agile and versatile system alongside future alternative cryptographic protocols which may require a more restrictive choice of α. For large channel loss, however, the choice of α becomes increasingly important, but using, for example, the mean $\bar{\alpha} = 0.55$ and $\xi = 2.1\%$ from experimental run 3, QDS-f is predicted to remain secure even down to 20-dB loss with still-feasible signature lengths $\mathrm{O}(10^9)$, which would allow a 1-bit message to be signed in approximately 1 s.

A more realistic signature length may be calculated by using the p_{err} directly measured from the output of Rx, which includes all noise sources and detector inefficiencies. This inclusion results in the signature lengths which are displayed in Table I. Crucially, they remain highly feasible over the metropolitan distances where continuous-variable cryptography is expected to be effective. Of particular note is the $L = 47\,887$ required to securely sign a 1-bit message over 2-km fiber, which to our knowledge makes QDS-f the fastest-ever demonstration of a QDS protocol requiring just 0.047 ms to sign a message at our 1-GHz sending rate (Fig. 8).

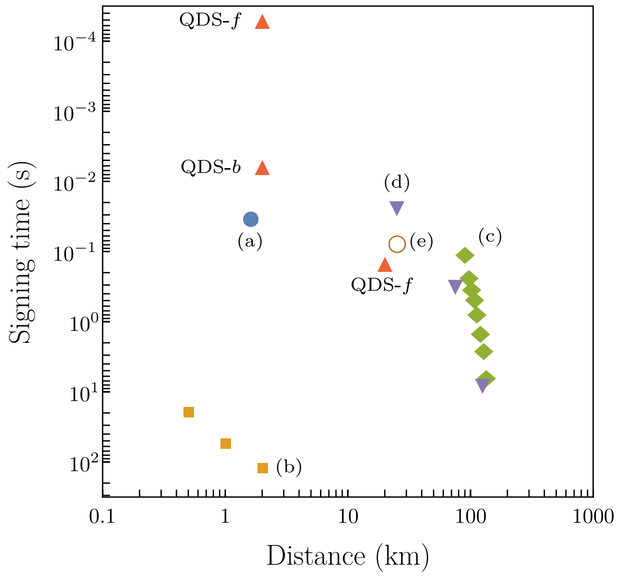

FIG. 8. Time required to sign a 1-bit message and the corresponding channel lengths for several recent QDS protocols. At the short distances (approximately 2 km) favored by the continuous-variable platform, our QDS-f and QDS-b allow for signing times of less than 0.05 and 6 ms, respectively, improving previous results in CV (a) and discrete-variable systems (b). At 20 km, QDS-f has signing time comparable to recent DV-QDS systems (c)–(e). Protocols depicted: red triangles, current paper; (a) free-space CV QDS [25]; (b) unambiguous-state-elimination-based QDS [26]; (c) differential-phase-shift-based QDS [18]; (d) GHz BB84 QDS [21]; (e) early QDS-QKD "versatile" system with measurement-device-independent capabilities [23].

2. *QKD-f*

The calculated maximum secure key rates under protocol QKD-f are plotted in Fig. 7 under a beam-splitter attack. The performance of the protocol agrees with Ref. [34] and corroborates their results over comparable parameter regimes in amplitude, transmission, and noise. The QPSK amplitudes reported in our experiment, however, are close to optimal. Calculated maximum key rates deduced from experimental parameters are displayed in Table I.

Finally, we want to note that key rates in a concrete implementation will depend on a number of parameters. For example, error correction in CV QKD can be computationally very demanding and will limit the obtainable key rate. An agile and versatile system therefore allows itself to resort to the protocol with the least demand on resources for a given task.

VI. CONCLUSION

Agile and versatile quantum cryptography allows the introduction of a layer abstraction between the quantum-optical hardware and the protocol layer based on firmware and software. This abstraction allows future quantum cryptography systems to be optimized toward agility and versatility and to explore how this concept can be applied to already existing ones. To underpin this concept, we experimentally demonstrate versatility by showing that the same quantum sender and receiver can be utilized independently of the protocol run on top of it. Because the agile middleware is opaque to the user layer, by design, the inner workings of the task are inaccessible to the user. This opacity implies agility. The proposed layer abstraction could potentially be further developed through standardization groups [3,4].

For the demonstrations, we utilize a continuous-variable quantum communication system that is almost exclusively built from commercial off-the-shelf telecom components. This makes it inherently compatible with telecom networks and allows C-band operation and high sending rates, since telecom components for coherent communication are optimized for GHz sending rates, even ranging up to 100 GHz as the state of the art. This setup is operated at a sending rate of 1 GHz; however, there is no known fundamental limit to these rates. The current limitation is the electronic noise of the coherent detection unit, which can be further optimized in future works.

The continuous-variable protocols investigated are QDS, QSS, and QKD. We show for the first time that postselection can be utilized for QDS and prove its enhanced robustness to noise and to channel loss. Postselection on QDS measurement outcomes decreases the required signature lengths and thus allows us to demonstrate the shortest signing time for realistic distances of 2 km and signing times comparable to recent discrete-variable QDS protocols over 20 km. Furthermore, the security of the QDS protocols is proven for forward and backward sending configurations, enabling them to be used in both of the agile and versatile systems presented in this paper.

ACKNOWLEDGMENTS

This research receives funding from the European Union's Horizon 2020 research and innovation program under Grant Agreement No. 820466 (CiViQ). This research is also funded by the German Federal Ministry of Education and Research within the project Hardware-based Quantum Security. The authors gratefully acknowledge the support from the Scottish Universities Physics Alliance and the Engineering and Physical Sciences Research Council. This project was supported within the framework of the International Max Planck Partnership with Scottish Universities.

APPENDIX A: QDS-*b* SECURITY PROOF

Recall that a QDS protocol must be secure against repudiation and forgery, and it should be robust and succeed if all players are honest. We prove the security of our protocol against each of these attacks, and finally derive Eq. (2), which implicitly defines the main figure of merit of a QDS protocol, the signature length L required to sign a 1-bit message.

During a repudiation attack, Alice will try to cause Bob and Charlie to disagree about whether her message is genuine. Security against repudiation follows along lines similar to Refs. [25,26,28], and we reproduce key details below for completeness.

We assume that Alice is free to manipulate her declared $A^m_{B,C}$, and she has full control over the mismatch rates $p_B(p_C)$ with respect to states which she originally sent to Bob or Charlie, and the $p_{B,C}$ may even be chosen to be zero.

After swapping, step 3 of the protocol, Bob and Charlie both possess two half-signatures, each of length $L/2$, consisting either of states which they held originally or which they received during swapping. Alice succeeds in her repudiation attack if Bob accepts both of his halves as genuine, and Charlie rejects at least one of his halves as fake. Therefore, the probability of successful repudiation is given by

$$\varepsilon_{\rm rep} = P[(A \cap B) \cap (C \cup D)],$$

where $A(B)$ denotes the event that Bob accepts on his first (second) half, and $C(D)$ denotes the event that Charlie rejects on his first (second) half. Now, using probability inequalities $P(X \cap Y) \leq \min\{P(X), P(Y)\}$ and $P(X \cup Y) \leq P(X) + P(Y)$ and Hoeffding's inequalities [36], we see that $\min\{P(A), P(B)\} \leq \exp[-(p - s_B)^2 L]$ and $P(C) + P(D) \leq 2\exp[-(s_C - p)^2 L]$, where $p \coloneqq \max\{p_B, p_C\}$.

Therefore, we arrive at

$$\begin{aligned}\varepsilon_{\rm rep} &\leq \min\{2\exp[-(p - s_B)^2 L], 2\exp[-(s_C - p)^2 L]\} \\ &\leq 2\exp\left[\frac{-(s_C - s_B)^2}{4} L\right],\end{aligned}$$

provided that $s_B < s_C$, and where in the second inequality we take $p = (s_B + s_C)/2$ in order to maximize $\varepsilon_{\rm rep}$.

A QDS protocol is robust if it succeeds when all parties are honest. Even in this case, there is a probability $p_{\rm err}$ of mismatch, owing to the nonorthogonality of the QPSK alphabet. Since $s_B < s_C$, an honest message is more likely to be rejected by Bob than Charlie, so we bound this probability. The message will be rejected if Bob detects more than $s_B L/2$ mismatches on either half of his eliminated signature. Using Hoeffding's inequalities, this event occurs with probability

$$\epsilon_{\rm reject} \leq 2\exp[-(s_B - p_{\rm err})^2 L],$$

provided that $s_B > p_{\rm err}$; i.e., Bob's mismatch threshold is greater than the honest mismatch rate.

In a forging attack, an eavesdropper will aim to minimize their mismatch probability with respect to either of the $X^m_{B,C}$ generated by Bob and Charlie. Since Bob already knows half of X^m_C (the information which Bob himself forwarded), and since $s_B < s_C$, the most dangerous forger is a dishonest Bob. He is therefore assumed to eavesdrop on Charlie's distribution of quantum states and tries to gain information about the $L/2$ signature elements which Charlie generated himself.

Using Hoeffding's inequalities as in Ref. [28], we see that a forging attack succeeds with probability

$$\varepsilon_{\rm forg} \leq 2\exp\left[-(p_e - s_C)^2 \frac{L}{2}\right]$$

when $p_e > s_C$, and therefore, all that is required is to bound p_e, which we now do.

Consider the jth signature element. Charlie holds some c_j denoting which state from the QPSK alphabet he sent. Bob will declare an eliminated signature element $B_j = \{b^1_j, b^2_j\}$, which is chosen to minimize p_e. The b^1_j, b^2_j correspond to adjacent elements of the QPSK alphabet. A mismatch occurs if $b^1_j = c_j$ or $b^2_j = c_j$. Additionally, we assume that B_j is the result of some optimal strategy involving Bob's quantum system $\mathbb{B}_j$.

We define an error variable E_j, which takes the value 1 if a mismatch occurs, and 0 otherwise. Then, $p_e \equiv P(E_j = 1)$, and the Shannon entropy $H(E_j) = h(p_e)$ is the binary entropy, since $|E_j| = 2$. Now, consider the conditional entropy $H(E_j, b^1_j, b^2_j|c_j)$. Via the chain rule for conditional entropies,

$$H(E_j, b^1_j, b^2_j|c_j) = H(b^1_j, b^2_j|c_j),$$

where we use the fact that once b^1_j, b^2_j, and c_j are known, E_j is uniquely determined. Using the chain rule on $H(E_j, b^1_j, b^2_j|c_j)$ again but for a different variable, we get

$$\begin{aligned}H(E_j, b^1_j, b^2_j|c_j) &= H(b^1_j, b^2_j|E_j, c_j) + H(E_j|c_j) \\ &\leq H(b^1_j, b^2_j|E_j, c_j) + h(p_e)\end{aligned}$$

since conditioning can never increase entropy. Therefore, by expanding the variable E_j,

$$\begin{aligned}H(b^1_j, b^2_j|c_j) \leq{}& (1 - p_e)H(b^1_j, b^2_j|E_j = 0, c_j) \\ &+ p_e H(b^1_j, b^2_j|E_j = 1, c_j) + h(p_e).\end{aligned}$$

Now, $H(b^1_j, b^2_j|E_j = 0, c_j) \leq \log_2(2) = 1$, and similarly for $E_j = 1$, and so

$$H(b^1_j, b^2_j|c_j) \leq 1 + h(p_e). \tag{A1}$$

Finally, we expand the conditional entropy in terms of the joint entropy and the mutual information,

$$H(b_j^1, b_j^2 | c_j) = H(b_j^1, b_j^2) - I(b_j^1, b_j^2 \colon c_j) \geq 2 - \chi(b_j^1, b_j^2 \colon c_j), \tag{A2}$$

where we use the fact that *a priori* there are four choices for the pair b_j^1, b_j^2, and where χ is the Holevo information [37]. Combining Eqs. (A1) and (A2), we arrive at Eq. (1) from the main text.

Once p_e and p_{err} are bounded for the protocol, the probability $\varepsilon_{\mathrm{fail}}$ that the protocol fails can be found. For concreteness, we assign equal probability to the failure of the protocol either by allowing a forging or repudiation attack, or by aborting when all players are honest, that is

$$\varepsilon_{\mathrm{fail}} = \varepsilon_{\mathrm{forg}} = \varepsilon_{\mathrm{rep}} = \varepsilon_{\mathrm{reject}},$$

and by choosing $s_B = p_{\mathrm{err}} + (p_e + p_{\mathrm{err}})/4$, $s_C = p_{\mathrm{err}} + 3(p_e - p_{\mathrm{err}})/4$, in order to satisfy the second two equalities, we arrive at Eq. (2) from the main text

$$\varepsilon_{\mathrm{fail}} \leq 2 \exp\left[-\frac{(p_e - p_{\mathrm{err}})^2}{16} L\right] \tag{A3}$$

when $p_{\mathrm{err}} < s_B < s_C < p_e$.

Finally, we note that under a beam-splitter attack, Eve's *a priori* state is

$$\rho_E = \sum_{k=0}^{3} \left| \sqrt{1-T}\alpha_k \right\rangle \left\langle \sqrt{1-T}\alpha_k \right| \tag{A4}$$

when states $|\alpha_k\rangle$ from the QPSK alphabet are sent through a lossy channel with transmittivity T. Eve's *a posteriori* state is simply $\rho_E^k = |\sqrt{1-T}\alpha_k\rangle\langle\sqrt{1-T}\alpha_k|$, from which her Holevo information is calculated as

$$\chi = S(\rho_E) - \sum_{k=0}^{3} p(k) S(\rho_E^k) \tag{A5}$$

with S the von Neumann entropy.

It is fitting to close this section with a brief discussion of the state of security proofs within the field of CV QDS. In security proofs for QDS, we see the usual contrast between CV and DV platforms that is well documented in the QKD literature. CV protocols offer a wide range of advantages in terms of implementations (speed, compatibility with infrastructure, etc.), but the security proofs are more involved than those on the DV platform, owing to the formidably large Hilbert spaces. An advanced and general DV-QDS security analysis is presented in Ref. [2], which adapts a decoy-state BB84 QKD protocol to the task of QDS. Specifically, their paper leverages tight bounds for the smooth minentropy to their QDS security proof in order to provide security against coherent attacks. This approach has the additional advantage of providing security in the finite-size setting.

While security against coherent attacks has been proven for the decoy-state BB84 setup, other QDS platforms typically reach security levels which are comparable with the neighboring QKD protocol. This is the case, for example, for the differential-phase-shift QDS of Refs. [18,38], and it is the case for the fully continuous-variable QDS protocol presented here. QKD on the fully CV platform relying on phase measurement of coherent states has only recently been proven secure against general coherent attacks in the finite-size regime [39], and even then, only for a Gaussian modulation of the coherent states. This choice of modulation is theoretically necessary—to simplify and bound the attack of the eavesdropper—but it is experimentally unrealistic. To our knowledge, there is no full security proof for QPSK QKD which offers security against the general coherent attacks in the finite-size regime. Binary [40] and ternary [41] modulations have been asymptotically secured against collective attacks, but the bounds are not tight, and the techniques are not expected to be generalizable to larger alphabets.

Recent QKD works [42,43] have made advances toward full security with the QPSK alphabet by providing security against coherent attacks in the asymptotic limit. The first, Ref. [42], provides security by relying on a small-amplitude assumption to ensure that the QPSK alphabet is close to a Gaussian modulation. They also make the assumption of Gaussian optimality; neither of these techniques are applicable to CV QDS. The second work, Ref. [43], removes these assumptions and applies convex optimization methods to provide security by building upon cutting-edge reformulations of the Devetak-Winter key rate bound and related semidefinite programming optimizations. Similar work should in the future be a key focus of the CVQDS community. We simply note here that should there become available a tight lower bound for the eavesdropper's smooth minentropy under the QPSK alphabet, we can readily insert it into our present QDS analysis with only minor modification to our proof.

APPENDIX B: POSTSELECTION IN CV QDS

In the QKD context, it has been known for some time that postselection will improve key rates in the presence of excess noise and is even a requirement for distilling a key for $T < 1/2$ in the direct-reconciliation regime [29]. We are thus motivated to apply postselection to our QDS protocols in order to allow a message to be securely signed over a larger range of channel parameters.

To apply the postselection technique, recipients in the protocol will disregard unfavorable measurement outcomes, i.e., those for which a dishonest player is deemed to have too much knowledge or for which the probability of an honest mismatch is too high. We thus define a region $\mathcal{R}$ of phase space and allow honest players to only accept measurement outcomes $x \notin \mathcal{R}$. The region $\mathcal{R}$ is then varied to increase the range of channel parameters for which the QDS protocols are secure and to minimize signature length L.

To be concrete, in this work we take $\mathcal{R}$ parametrized by Δ_r, Δ_θ in polar coordinates in phase space. This postselection region was also considered in the recent QKD work of Ref. [43], but if desired, more general regions may be readily considered. A protocol using no postselection technique may be retained by setting $\Delta_r \to 0$ and $\Delta_\theta \to 0$.

We now consider how this application of postselection affects security of QDS-b and QDS-f.

1. QDS-*b*

The crucial quantity which controls the security of a QDS protocol is $g_{\text{sec}} \coloneqq p_e - p_{\text{err}}$, which intuitively describes how much worse a dishonest player should fare than an honest player. The protocol is secure provided that $g_{\text{sec}} > 0$.

In QDS-b, p_e does not depend on Alice's heterodyne measurement, since a dishonest player will attack the sender (Tx) of the quantum states, and so p_e is unaffected by postselection. We thus calculate the transformation of p_{err}.

Although in an actual run of the protocol the honest mismatch rate p_{err} should be estimated from a publicly disclosed subset of $A^m_{B,C}$ and $X^m_{B,C}$, it is illustrative to consider how p_{err} may be calculated theoretically. When Charlie sends state $|\alpha_k\rangle$ through a lossy channel, transmittivity T, then Alice receives outcome $x \in \mathbb{C}$ with probability

$$p(x|\alpha_k) = \frac{1}{\pi}\exp\left(-|x - \sqrt{\frac{T}{2}}\alpha_k|^2\right). \tag{B1}$$

Thus, the probability of eliminating the state $|\alpha\rangle$ when no postselection is used is

$$\begin{aligned} p_{\text{err}} &= \int_0^\infty r\,dr \int_{\pi/2}^{3\pi/2} d\theta p(re^{i\theta}|\alpha) \\ &= \frac{1}{2}\text{erfc}\left(\sqrt{\frac{T}{2}}|\alpha|\right). \end{aligned} \tag{B2}$$

Postselecting on the region $\mathcal{R}$, the mismatch probability becomes

$$\begin{aligned} p_{\text{err}}(\Delta_r, \Delta_\theta) = \frac{1}{\mathcal{N}}\int_{\Delta_r}^\infty r\,dr\bigg(&\int_{3\pi/2-\Delta_\theta}^{\pi+\Delta_\theta} d\theta f(r,\theta) \\ &+ \int_{\pi/2+\Delta_\theta}^{\pi-\Delta_\theta} d\theta f(r,\theta)\bigg) \end{aligned} \tag{B3}$$

with $f(r,\theta) = p(re^{i\theta}|\alpha)$ and $\mathcal{N}$ the probability that the outcome $x \in \mathbb{C}$ is accepted; i.e., it falls within $\mathbb{C}\backslash\mathcal{R}$. Probability $\mathcal{N}$ is calculated analogously to Eq. (B3).

For QDS-b the probability p_e does not depend on Alice's heterodyne measurement, since a dishonest player will attack the sender (Tx) of the quantum states. The dishonest player's *a posteriori* state depends not on a recipient's heterodyne outcome but only on the chosen distributed alphabet state (Appendix A). The postselection technique alters the probability distribution of heterodyne measurement outcomes which are used in the protocol; coherent-state sending probabilities remain uniform and unaffected. Therefore, for QDS-b, the dishonest mismatch probability p_e is unaffected by the choice of postselection region. This independence from $\mathcal{R}$ will no longer be the case for QDS-f, and we discuss this in detail in the next section.

Our analysis of the effects of postselection follows identically when excess noise is included, simply by substituting in the requisite formulas from Refs. [28,34]. Finally, we note that when postselection is used, the signature length L calculated from Eq. (2) should be rescaled in order to remain a useful figure of merit. While the normally calculated L counts how many signature elements are required to sign the message, many of the states which were sent during the protocol will be rejected. Including the rejected states in our accounting, the figure of merit is rescaled as $L \to \tilde{L} \coloneqq L/\mathcal{N}$. These L and $\tilde{L}$ may now be directly compared between protocols, and so in Sec. V we make no distinction between L and $\tilde{L}$.

2. QDS-*f*

Postselection affects probability p_{err} in the same way as it does under protocol QDS-b. For our protocol QDS-f, a dishonest player's declaration depends on an honest player's heterodyne outcome: So the dishonest mismatch probability p_e must now also vary with $\mathcal{R}$. We recall that the key security result for QDS-f, taking dishonest Bob as the forger, is [28]

$$h(p_e) \geq 1 - \chi \tag{B4}$$

with χ the Holevo information between Bob's quantum system and Charlie's eliminated signature element. For the jth signature element in QDS-f, this information takes the form

$$\chi(x_1^j, x_2^j : \mathbb{B}_j) = S(\rho_B^j) - \sum_{x_1^j, x_2^j} p(x_1^j, x_2^j) S(\rho_B^{x_1^j, x_2^j}). \tag{B5}$$

The *a posteriori* state $\rho_B^{x_1^j, x_2^j}$ is the quantum state held by Bob when Charlie's eliminated signature element is x_1^j, x_2^j, and ρ_B^j is Bob's *a priori* state which is mixed over all eliminated signature elements.

Under the beam-splitter or entangling-cloner attacks considered in this work, the conditional state $\rho^j_{B|c}$ held by Bob after Charlie measures $c \in \mathbb{C}$ may be readily calculated as in Ref. [28]. Then, since Charlie's eliminated signature element is entirely determined by the quadrant in which c lies, the state $\rho_B^{x_1^j,x_2^j}$ is calculated by mixing $\rho_{B|c}^j$ over an entire quadrant of phase space

$$\begin{aligned}\rho_B^{x_1^j,x_2^j} &= \frac{1}{\mathcal{N}}\int \rho_{B|c}^j d^2c \\ &= 4\int_0^\infty r\,dr \int_0^{\pi/2} \rho_{B|re^{i\theta}}d\theta,\end{aligned} \tag{B6}$$

where $\mathcal{N}$ is the required normalization factor, and where in the second line we explicitly show the calculation for a particular eliminated signature element.

Then, we see that when postselection over region $\mathcal{R}(\Delta_r,\Delta_\theta)$ is used, Eq. (B6) should be modified

$$\rho_B^{x_1^j,x_2^j} = \frac{1}{\mathcal{N}}\int_{\Delta_r}^\infty r\,dr \int_{\Delta_\theta}^{\pi/2-\Delta_\theta} \rho_{B|re^{i\theta}}d\theta \tag{B7}$$

with $\mathcal{N}$ the same normalization factor as in Eq. (B3). The *a priori* state is likewise found by mixing Eq. (B7) over all quadrants, and thus, p_e may be calculated. The figure of merit for QDS-f under postselection is now $\tilde{L}$, as in the preceding section, though since this may be directly compared with L in the absence of postselection, we make no distinction in the main body of the paper. All results presented have the optimal choice of $\mathcal{R}(\Delta_r)$, noting that variations in Δ_θ provide only small changes to signature lengths in both QDS-b and QDS-f, and so in the main body of the paper, we set $\Delta_\theta = 0$ in order to focus on the much larger effects of the radial variations.

APPENDIX C: QSS-*b* SECURITY CALCULATIONS

We first demonstrate the security calculation of the protocol in the presence of an external eavesdropper, with Bob and Charlie assumed honest. The starting point for our calculation is

$$\kappa_{\mathrm{Eve}} \geq I(X_B,X_C:X_A) - \chi(X_A:\mathbb{E}) \tag{C1}$$

denoting the maximum calculated key rate between the shared variable X_B, X_C of Bob or Charlie, and Alice's $X_A \coloneqq F(A_B,A_C)$. Eve's quantum system is denoted $\mathbb{E}$.

Let b, c denote elements from the QPSK alphabet which are sent by Bob or Charlie. Then the mutual information may be calculated once the probability $p(X_A = a|X_B = b, X_C = c)$ for Alice to receive element $X_A = a$ conditioned on particular QPSK states is known. In the ideal case, probability $p(X_B = b, X_C = c) = 1/16$ since each of the QPSK states is equally likely, and so $p(X_B = b, X_C = c|X_A = a)$ may be calculated using Bayes's formula. Then, $H(X_B,X_C|X_A)$ is calculated by integrating $p(X_A = a)H(X_B,X_C|X_A = a)$ over all possible outcomes a, and finally,

$$I(X_B,X_C:X_A) = H(X_B,X_C) - H(X_B,X_C|X_A).$$

The Holevo term in Eq. (C1) may be calculated in the usual way from Eve's *a priori* and *a posteriori* states, with ρ_E mixed over all X_A, and ρ_E^a Eve's state when Alice holds $X_A = a$, with the channel modeled under either beam-splitter or entangling-cloner attacks.

Before the channel, the total Bob-Charlie state is $\rho_{B,C} = \rho_B \otimes \rho_C$, where in the ideal case each $\rho_B(\rho_C)$ is an equally weighted mixture over the QPSK alphabet. Passing through the channels, $\rho_{\mathbb{A},\mathbb{E}} = \rho_{\mathbb{A}_B,\mathbb{E}_B} \otimes \rho_{\mathbb{A}_C,\mathbb{E}_C}$ where, for example, under a beam-splitter attack

$$\begin{aligned}\rho_{\mathbb{A}_B,\mathbb{E}_B} = \frac{1}{4}\sum_{k=0}^{3} &|\sqrt{T}\beta_k\rangle_A\langle\sqrt{T}\beta_k| \\ &\otimes |\sqrt{1-T}\beta_k\rangle_E\langle\sqrt{1-T}\beta_k|\end{aligned}$$

and similarly for $\rho_{\mathbb{A}_C,\mathbb{E}_C}$. Alice heterodynes on each of her modes and receives outcomes A_B, A_C.

Since the function F is in general not injective, Eve's state is found by mixing $\rho_{\mathbb{E}|A_B} \otimes \rho_{\mathbb{E}|A_C}$ over Alice's measurement outcomes A_B, A_C to reach the *a posteriori* state $\rho_{\mathbb{E}|X_A}$. Finally, the *a priori* state is given by

$$\rho_{\mathbb{E}} = \int d^2X_A P(X_A)\rho_{\mathbb{E}|X_A}, \tag{C2}$$

and so Eve's Holevo information may be calculated. The Holevo information under an entangling-cloner attack is calculated analogously, but now the channel mixes the input ρ_B, ρ_C with one arm of one of Eve's two entangled two-mode squeezed vacuum states. The remainder of the calculation proceeds identically and is shown, e.g., in Ref. [28] in the context of QDS.

Including a dishonest Bob, the key rate reads

$$\kappa_B \geq I(X_A:X_B,X_C) - \chi(X_A:\mathbb{E}\mathbb{B}), \tag{C3}$$

where $\mathbb{E}\mathbb{B}$ is a quantum system shared between Bob and Eve. The main difference in the calculation of both mutual information and Holevo information terms is that now the Eve-Bob conspiracy has knowledge about which state Bob sent, and so Bob's alphabet should no longer be mixed over.

A dishonest Charlie is taken into account identically, and the final key rate, including possibility for either Bob or Charlie to be dishonest, is given by [31]

$$\kappa \geq \min\{\kappa_B,\kappa_C\}. \tag{C4}$$

[1] B. Sullivan, *Security Briefs—Cryptographic Agility*, MSDN Mag. **24** (2009), https://docs.microsoft.com/en-us/archive/msdn-magazine/2009/august/cryptographic-agility; L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone, National Institute of Standards and Technology Report No. 8105, 2016.

[2] R. Amiri, P. Wallden, A. Kent, and E. Andersson, *Secure Quantum Signatures Using Insecure Quantum Channels*, Phys. Rev. A **93**, 032325 (2016).

[3] ETSI Industry Specification Group, *Quantum Key Distribution (QKD); Application Interface*, 2010.

[4] ETSI Industry Specification Group, *Quantum Key Distribution (QKD); Protocol and Data Format of REST-Based Key Delivery API*, 2019, https://www.etsi.org/deliver/etsi_gs/QKD/001_099/014/01.01.01_60/gs_qkd014v010101p.pdf.

[5] P. K. Tysowski, X. Ling, N. Lütkenhaus, and M. Mosca, *The Engineering of a Scalable Multi-Site Communications System Utilizing Quantum Key Distribution (QKD)*, Quantum Sci. Technol. **3**, 024001 (2018).

[6] A. Dahlberg, M. Skrzypczyk, T. Coopmans, L. Wubben, F. Rozpedek, M. Pompili, A. Stolk, P. Pawełczak, R. Knegjens, J. de Oliveira Filho, R. Hanson, and S. Wehner, in *Proceedings of the ACM Special Interest Group on Data Communication, SIGCOMM '19* (Association for Computing Machinery, New York, 2019), pp. 159–173.

[7] W. Kozlowski and S. Wehner, in *Proceedings of the Sixth Annual ACM International Conference on Nanoscale Computing and Communication, NANOCOM '19* (Association for Computing Machinery, New York, 2019), pp. 1–7.

[8] W. Kozlowski, A. Dahlberg, and S. Wehner, *Designing a Quantum Network Protocol*, arXiv:2010.02575.

[9] I. Khan, B. Stiller, K. Jaksch, K. Günthner, C. Peuntinger, J. Geyer-Ramsteck, D. Elser, C. Pacher, C. Marquardt, and G. Leuchs, *Continuous-Variable Quantum Communication at 10 GHz and Compatible with Telecom Networks*, in *Proceedings of the QCrypt Conference, Washington, DC*, 2015 (unpublished).

[10] I. Khan, B. Stiller, K. Jaksch, N. Jain, C. Peuntinger, K. Günthner, T. Röthlingshöfer, D. Elser, C. Marquardt, and G. Leuchs, *Towards Continuous-Variable Quantum Key Distribution at GHz Rates*, in *Proceedings of the QCrypt Conference, Tokyo, Japan*, 2015 (unpublished).

[11] D. Gottesman and I. Chuang, *Quantum Digital Signatures*, arXiv:quant-ph/0105032.

[12] E. Andersson, M. Curty, and I. Jex, *Experimentally Realizable Quantum Comparison of Coherent States and Its Applications*, Phys. Rev. A **74**, 022304 (2006).

[13] P. J. Clarke, R. J. Collins, V. Dunjko, E. Andersson, J. Jeffers, and G. S. Buller, *Experimental Demonstration of Quantum Digital Signatures Using Phase-Encoded Coherent States of Light*, Nat. Commun. **3**, 1174 (2012).

[14] V. Dunjko, P. Wallden, and E. Andersson, *Quantum Digital Signatures without Quantum Memory*, Phys. Rev. Lett. **112**, 040502 (2014).

[15] R. J. Collins, R. J. Donaldson, V. Dunjko, P. Wallden, P. J. Clarke, E. Andersson, J. Jeffers, and G. S. Buller, *Realization of Quantum Digital Signatures without the Requirement of Quantum Memory*, Phys. Rev. Lett. **113**, 040502 (2014).

[16] H.-L. Yin, Y. Fu, and Z.-B. Chen, *Practical Quantum Digital Signature*, Phys. Rev. A **93**, 032316 (2016).

[17] P. Wallden, V. Dunjko, A. Kent, and E. Andersson, *Quantum Digital Signatures with Quantum-Key-Distribution Cmponents*, Phys. Rev. A **91**, 042304 (2015).

[18] R. J. Collins, R. Amiri, M. Fujiwara, T. Honjo, K. Shimizu, K. Tamaki, M. Takeoka, E. Andersson, G. S. Buller, and M. Sasaki, *Experimental Transmission of Quantum Digital Signatures over 90 km of Installed Optical Fiber Using a Differential Phase Shift Quantum Key Distribution System*, Opt. Lett. **41**, 4883 (2016).

[19] H.-L. Yin, W.-L. Wang, Y.-L. Tang, Q. Zhao, H. Liu, X.-X. Sun, W.-J. Zhang, H. Li, I. V. Puthoor, L.-X. You, E. Andersson, Z. Wang, Y. Liu, X. Jiang, X. Ma, Q. Zhang, M. Curty, T.-Y. Chen, and J.-W. Pan, *Experimental Measurement-Device-Independent Quantum Digital Signatures over a Metropolitan Network*, Phys. Rev. A **95**, 042338 (2017).

[20] H.-L. Yin, Y. Fu, H. Liu, Q.-J. Tang, J. Wang, L.-X. You, W.-J. Zhang, S.-J. Chen, Z. Wang, Q. Zhang, T.-Y. Chen, Z.-B. Chen, and J.-W. Pan, *Experimental Quantum Digital Signature over 102 km*, Phys. Rev. A **95**, 032334 (2017).

[21] X.-B. An, H. Zhang, C.-M. Zhang, W. Chen, S. Wang, Z.-Q. Yin, Q. Wang, D.-Y. He, P.-L. Hao, S.-F. Liu, X.-Yu. Zhou, G.-C. Guo, and Z.-F. Han, *Practical Quantum Digital Signature with a Gigahertz BB84 Quantum Key Distribution System*, Opt. Lett. **44**, 1133 (2019).

[22] H.-J. Ding, J.-J. Chen, L. Ji, X.-Yu. Zhou, C.-H. Zhang, C.-M. Zhang, and Q. Wang, *280-km Experimental Demonstration of a Quantum Digital Signature with One Decoy State*, Opt. Lett. **45**, 1711 (2020).

[23] G. L. Roberts, M. Lucamarini, Z. L. Yuan, J. F. Dynes, L. C. Comandar, A. W. Sharpe, A. J. Shields, M. Curty, I. V. Puthoor, and E. Andersson, *Experimental Measurement-Device-Independent Quantum Digital Signatures*, Nat. Commun. **8**, 1098 (2017).

[24] The exchange of eliminated signature elements in a QDS protocol must be kept hidden from Alice. This swapping is most straightforwardly done over an encrypted channel which implicitly requires QKD. To allow for a fair comparison to existing QDS schemes and implementations, we omit an accounting for this QKD link, instead using in further QDS analyses the figures of merit commonly used by the QDS community [2,18,25–27].

[25] C. Croal, C. Peuntinger, B. Heim, I. Khan, C. Marquardt, G. Leuchs, P. Wallden, E. Andersson, and N. Korolkova, *Free-Space Quantum Signatures Using Heterodyne Detection*, Phys. Rev. Lett. **117**, 100503 (2016).

[26] R. J. Donaldson, R. J. Collins, K. Kleczkowska, R. Amiri, P. Wallden, V. Dunjko, J. Jeffers, E. Andersson, and G. S. Buller, *Experimental Demonstration of Kilometer-Range Quantum Digital Signatures*, Phys. Rev. A **93**, 012329 (2016).

[27] R. J. Collins, R. J. Donaldson, and G. S. Buller, *Progress in Experimental Quantum Digital Signatures*, Proc. SPIE Int. Soc. Opt. Eng. **10771**, 102210F (2018).

[28] M. Thornton, H. Scott, C. Croal, and N. Korolkova, *Continuous-Variable Quantum Digital Signatures over Insecure Channels*, Phys. Rev. A **99**, 032341 (2019).

[29] C. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, *Continuous Variable Quantum Cryptography: Beating the 3 dB Loss Limit*, Phys. Rev. Lett. **89**, 167901 (2002).

[30] B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C* (John Wiley & Sons, New York, 1996).

[31] I. Kogias, Yu. Xiang, Q. He, and G. Adesso, *Unconditional Security of Entanglement-Based Continuous-Variable Quantum Secret Sharing*, Phys. Rev. A **95**, 012315 (2017).

[32] W. P. Grice and B. Qi, *Quantum Secret Sharing Using Weak Coherent States*, Phys. Rev. A **100**, 022339 (2019).

[33] I. Devetak and A. Winter, *Distillation of Secret Key and Entanglement from Quantum States*, Proc. R. Soc. A **461**, 207 (2005).

[34] P. Papanastasiou, C. Lupo, C. Weedbrook, and S. Pirandola, *Quantum Key Distribution with Phase-Encoded Coherent States: Asymptotic Security Analysis in Thermal-Loss Channels*, Phys. Rev. A **98**, 012340 (2018).

[35] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevX.11.011038 for a subset of raw measurement data. 10^4 heterodyne measurement samples are given for two different fiber links (2 and 20 km) which comprise a single Tx-Rx module. The data is sufficient to generate the top portion of Fig. 5.

[36] W. Hoeffding, *Probability Inequalities for Sums of Bounded Random Variables*, J. Am. Stat. Assoc. **58**, 13 (1963).

[37] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2010).

[38] R. J. Collins, R. Amiri, M. Fujiwara, T. Honjo, K. Shimizu, K. Tamaki, M. Takeoka, M. Sasaki, E. Andersson, and G. S. Buller, *Experimental Demonstration of Quantum Digital Signatures over 43 dB Channel Loss Using Differential Phase Shift Quantum Key Distribution*, Sci. Rep. **7**, 3325 (2017).

[39] A. Leverrier, *Security of Continuous-Variable Quantum Key Distribution via a Gaussian de Finetti Reduction*, Phys. Rev. Lett. **118**, 200501 (2017).

[40] Y.-B. Zhao, M. Heid, J. Rigas, and N. Lütkenhaus, *Asymptotic Security of Binary Modulated Continuous-Variable Quantum Key Distribution under Collective Attacks*, Phys. Rev. A **79**, 012307 (2009).

[41] K. Brádler and C. Weedbrook, *Security Proof of Continuous-Variable Quantum Key Distribution Using Three Coherent States*, Phys. Rev. A **97**, 022310 (2018).

[42] S. Ghorai, P. Grangier, E. Diamanti, and A. Leverrier, *Asymptotic Security of Continuous-Variable Quantum Key Distribution with a Discrete Modulation*, Phys. Rev. X **9**, 021059 (2019).

[43] J. Lin, T. Upadhyaya, and N. Lütkenhaus, *Asymptotic Security Analysis of Discrete-Modulated Continuous-Variable Quantum Key Distribution*, Phys. Rev. X **9**, 041064 (2019).