Quantum Science and Technology

RECEIVED
13 May 2019

REVISED
2 September 2019

ACCEPTED FOR PUBLICATION
25 September 2019

PUBLISHED
15 October 2019

PAPER

Asymmetric cryptography with physical unclonable keys

Ravitej Uppu[1,2], Tom A W Wolterink[1,3,8], Sebastianus A Goorden[1,9], Bin Chen[4,5], Boris Škorić[6], Allard P Mosk[1,7] and Pepijn W H Pinkse[1]

[1] Complex Photonic Systems (COPS), MESA+ Institute for Nanotechnology, University of Twente, PO Box 217, 7500 AE Enschede, The Netherlands

[2] Center for Hybrid Quantum Networks (Hy-Q), Niels Bohr Institute, University of Copenhagen, Blegdamsvej 17, DK-2100, Copenhagen, Denmark

[3] Laser Physics and Nonlinear Optics (LPNO), MESA+ Institute for Nanotechnology, University of Twente, PO Box 217, 7500 AE Enschede, The Netherlands

[4] Department of Electrical Engineering, Eindhoven University of Technology, PO Box 513, 5600 MB Eindhoven, The Netherlands

[5] School of Computing and Information, Hefei University of Technology, Hefei, People's Republic of China

[6] Department of Mathematics and Computer Science, Eindhoven University of Technology, PO Box 513, 5600 MB Eindhoven, The Netherlands

[7] Nanophotonics, Debye Institute for Nanomaterials Research, Center for Extreme Matter and Emergent Phenomena, Utrecht University, PO Box 80000, 3508 TA Utrecht, The Netherlands

[8] Present address: Center for Nanophotonics, AMOLF, Science Park 104, 1098XG Amsterdam, The Netherlands.

[9] Present address: ASML Netherlands B.V., De Run 6501, 5504 DR Veldhoven, The Netherlands.

E-mail: ravitej.uppu@nbi.ku.dk **and** p.w.h.pinkse@utwente.nl

Keywords: light scattering, quantum cryptography, physical unclonable functions, wavefront shaping, quantum secure

Supplementary material for this article is available online

Abstract

Secure communication is of paramount importance in modern society. Asymmetric cryptography methods such as the widely used RSA cryptosystem allow secure exchange of information between parties who have never previously shared keys. However, the existing asymmetric cryptographic schemes rely on unproven mathematical assumptions for security. Further, the digital keys used in their implementation are susceptible to copying that might remain unnoticed. Here, we introduce a secure communication method based on Physical Unclonable Keys (PUKs), which we call PUK-Enabled Asymmetric Communication (PEAC). PEAC uses physical keys and thus overcomes the problem of unnoticed copying. As all the information about the PUK is allowed to be public, PEAC does not require the safekeeping of any digital information. Using optical PUKs realized in opaque scattering materials, we transmit messages in an error-corrected way employing off-the-shelf equipment. Information is transmitted as patterned wavefronts of few-photon wavepackets which can be successfully decrypted only with the receiver's PUK. The security of PEAC assumes technological constraints in distinguishing between different few-photon wavefronts. A heuristic argument for the security of PEAC is outlined focusing on a specific attack, namely state estimation. We demonstrate secure transmission of messages over a 2 m free-space line-of-sight quantum channel. PEAC enables new directions for physical key based cryptography.

1. Introduction

Secure communication has become of paramount importance in the internet era. The security is based on techniques that encrypt private messages from a sender (Alice) which can only be decrypted by the receiver (Bob) and not by any adversary (Eve). Symmetric cryptographic methods need an *a priori* exchange of secrets such as encryption keys and authentication keys between Alice and Bob [1]. Asymmetric cryptography has been a major revolution in cryptography by overcoming the key distribution problem and allowing the encryption of messages to Bob with whom Alice does not yet share a secret. Asymmetric cryptography methods such as RSA and Diffie–Hellman key exchange use secret private keys (known only to its owner) together with public keys and thus overcome the necessity of *a priori* sharing a secret [2, 3].

The existing asymmetric cryptography methods face two issues. Firstly, their security relies on unproven mathematical assumptions such as the hardness of factorization or computing discrete logarithms. Secondly, digitally stored private keys are prone to stealthy copying (which is not detected by the key owner). Over the last three decades, quantum physics has been exploited to create unconditionally secure cryptography methods such as Quantum Key Distribution [4–6], Quantum Key Recycling [7–9] and Quantum Secret Sharing [10]. These methods utilize entanglement or the unclonability of unknown quantum states to avoid leakage of information to Eve or to detect Eve's actions. Nevertheless, the practical implementation of these quantum methods again requires an authentication mechanism on the communication channel between Alice and Bob to prevent Eve from impersonating the legitimate parties. The standard approach for authentication is still *a priori* sharing of a secret key, which to some extent defies the purpose of a key exchange method. Indeed, public keys based on quantum states have been proposed as a way to fulfill all the security criteria [11, 12]. However, the use of quantum states as public keys is highly impractical, since it requires long-term quantum storage, and has limited scalability in the number of keys [11]. Hence, there is still a need for a practical asymmetric cryptographic method that overcomes the challenges of the existing classical and quantum cryptography methods.

Recently physical unclonable keys (PUKs), also known as physical unclonable functions (PUFs), have been introduced as a new security technology [13–16]. A PUK is a physical object with complex internal structure that is infeasible to copy due to the massive number of degrees of freedom that strongly affects its response to stimuli. PUKs that can be read out optically are readily realized in opaque scattering media (e.g. white paint, teeth and paper), which consists of vast numbers of randomly positioned particles. A recent development, Quantum Secure Authentication (QSA), verifies the authenticity of an optical PUK by querying it at the few-photon level [16, 17]. The security of QSA relies only on the hardness of building a device that has the same physical challenge-response behavior as the PUK.

Here we combine PUKs and quantum cryptography: We introduce 'PUK-Enabled Asymmetric Communication' (PEAC) that allows Alice to quantum-encrypt a message, which can be decrypted only with Bob's PUK. The security of PEAC does not rely on mathematical assumptions or on the secure storage of secrets, but -so we argue- only on the technological difficulty in distinguishing complicated high-dimensional quantum states [17–20]. Thus, PEAC is based on a *physical* assumption instead of a *mathematical* assumption. This augments the arsenal of security mechanisms and constitutes an independent approach that will not be broken together with the existing cryptography protocols. PEAC uses a (two-pixel) detector on Bob's side. PEAC has a practical advantage over QSA: PEAC requires photons to travel between Alice and Bob only once, i.e. PEAC requires only a one-way quantum channel, whereas in QSA the photons need to go back and forth and need spatial light modulation twice. This significantly reduces the transport losses [21]. The one-way quantum channel from Alice to Bob can be authenticated as follows: Alice sends a random bit string S and Bob cryptographically proves his knowledge of S, thereby confirming the possession of the PUK. An adversary cannot successfully pretend to be Bob without cloning the PUK.

2. PEAC: the protocol and its implementation

Similar to many asymmetric cryptography methods, PEAC works with a public-private key pair. The private key is the infeasible-to-copy PUK held by Bob. The completely classical optical challenge-response characteristics of Bob's PUK are the digital public key. The public key is generated through a one-time optical characterization of the PUK, e.g. as follows. Coherent light from a laser source is delivered to the digital Spatial Light Modulator (SLM) using a single-mode optical fiber with collimation optics that illuminates the SLM with a Gaussian intensity profile. The incident light is programmed with the SLM using complex wavefront shaping or digital phase conjugation in a setup illustrated in figure 1 [22–25]. The SLM offers K degrees of freedom in shaping the wavefront, i.e. K independent phases can be programmed. Using a CCD camera in the transmission of the PUK, wavefronts are constructed such that the transmitted light focuses to different locations on the camera, illustrated as the grid in the right panel of figure 1 (see section 1 and figures S1 and S2 of the supplementary material available online at stacks.iop.org/QST/4/045011/mmedia for details on experimental methods). Each distinct focus corresponds to a linearly independent incident field (wavefront) composed of K phases on the SLM. We separate the V incoming wavefronts into two sets, each focusing to one of the highlighted regions in figure 1, and assign them as the bases H_0 and H_1 for transmitting classical bits '0' and '1', respectively. The basis H_b consists of $V/2$ wavefronts, each of which is a $K-$element vector of phases programmed on the SLM. The two sets H_0 and H_1 together constitute the public key. The public key with $V \equiv |H_0 \bigcup H_1|$ column vectors, each of length K is made public as a binary file. The values of this $K \times V$ array are phases $[0, 2\pi)$, typically digitized as 8-bit integers. In our implementation, there are 350 spots per detector, leading to $V = 700$ and the SLM has

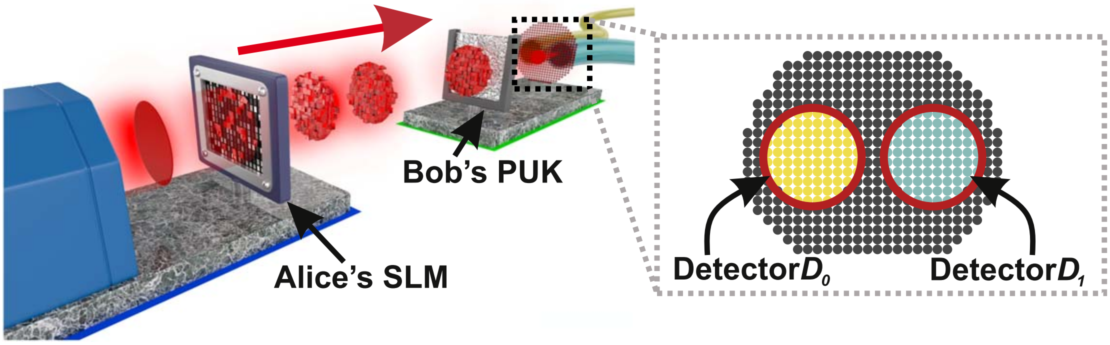

Figure 1. Using a spatial light modulator (SLM), Alice creates a few-photon wavefront that focuses to one of the highlighted regions in the transmission of Bob's PUK. The wavefront is constructed as a superposition of wavefronts known to focus to a spot in the detector area. The detector area is indicated as gray dots. Photons in the highlighted yellow or blue areas are collected by a multimode fiber (core diameter indicated by the red circle) and detected on an avalanche photodiode D0 ('0') or D1 ('1'), respectively. The received bit value is decided based on the difference in the number of photodetections in the two detectors.

$K = 900$ independent phases, which results in a public key file of size ~615 kB. An example of the public key used in our implementation can be found in Dataset1 ([26]). In a full-scale deployment of PEAC, this digital file can be shared through a certification authority to any number of users on the network.

When any sender (for instance, Alice) wants to send a bit b to Bob, they run the following procedure. Alice chooses a random subset of columns of H_b $(b \in \{0, 1\})$ and constructs the superposition ψ by adding the complex amplitudes in each of the K rows, i.e. argument of the segment-wise complex addition on the SLM. This superposition ψ is programmed to the SLM. A pulse of weak coherent light with low mean photon number $\langle n \rangle$ is patterned by the SLM and transmitted over the quantum channel to Bob. The quantum channel from Alice to Bob should be multimodal, with a capability to transmit K spatial modes. The requirement of low $\langle n \rangle$ provides the security from eavesdropping thanks to quantum physical principles (discussed below; see supplemental document section 22). Bob uses two single-pixel detectors D0 and D1 that register the integrated photodetections over the areas. The value of the received bit corresponds to the region with the most photodetections. The process is repeated with a different superposition on the SLM to transmit several bits. The rate of bit transmission is limited by the switching speed of the SLM, which can reach up to 50 kHz using off-the-shelf devices. Ideally, the contrast between the signal in the detectors is high with a perfect concentration of light into the chosen area. However, practical limitations such as the noise in the source and the detectors and an incomplete control of the transmitted field result in a reduced contrast. Further, the partial transmission of the incident light by the PUK (≈10%) leads to photon loss. The noise and losses lead to errors in the transmission of symbols from Alice to Bob, which necessitates error correction to make PEAC a functional communication scheme.

3. Results and discussion

3.1. Error-correction over noisy transmission channels

Our choice of error correction is guided by the level of channel noise. This can be quantified by the channel parameters shown in figure 2(a). The parameters α and ϵ characterize the bit-flip and bit-loss probabilities of the channel. The probability for a bit to be transmitted correctly is $(1 - \epsilon)(1 - \alpha)$. At $\langle n \rangle = 33$ photons per wavefront with $K = 900$ degrees of freedom on the SLM, we find $\alpha = 0.43 \pm 0.01$ and $\epsilon = 0.59 \pm 0.01$. These channel parameters were estimated by transmitting 2^{15} known pseudo-random bits from Alice to Bob. The error rate α is plotted as the red star in figure 2(b). To overcome the channel noise, we employ polar codes, which have been proven to be capacity-achieving [27]. Conceptually, polar codes can reliably transmit M bits of data by encoding them into a codeword of N bits $(N > M)$. The other $N - M$ bits in the codeword are preassigned to a known value and encoded with M data bits into an N bit codeword. The operation of polar codes can be formulated through the construction of N virtual channels with M of them carrying data reliably. The ratio $R \equiv M/N$, called the code rate, quantifies the amount of information that can be transmitted. The achievable R for a given channel is upper bounded by the channel capacity. Polar codes comprise an encoder-decoder system, which polarizes the M data channels to have a vanishingly small error rate. This improvement of the error rate in the data channels occurs at the cost of an increased error in the $N - M$ constructed noisy channels. Increasing the codeword length N for a fixed M improves the error rate of data channels, but results in a lower communication speed, i.e. smaller R. Figure 2(b) shows the maximum error rate of the virtual channels with

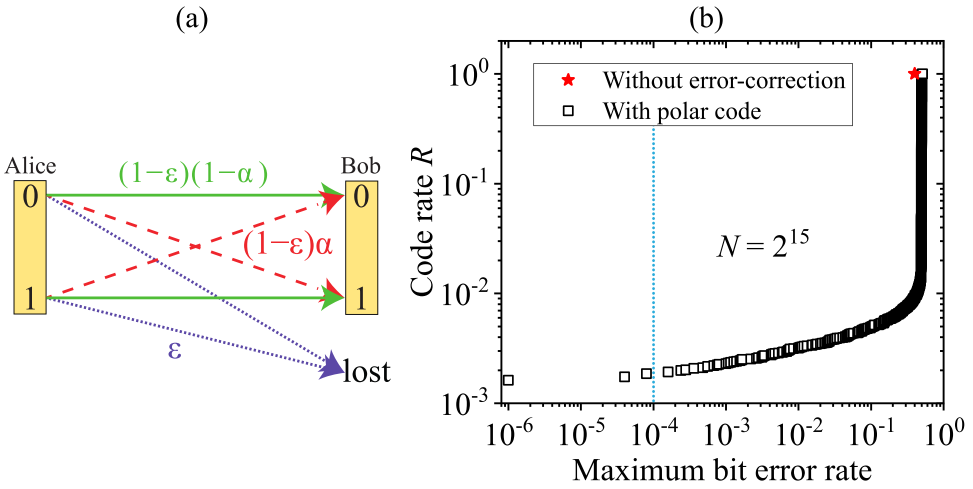

Figure 2. (a) Possible bit transmission outcomes: Correct transmission (solid green), loss (dotted purple) or flip of the bit (dashed red) are quantified by the two variables ϵ and α, which correspond to bit loss and flip probabilities respectively. (b) shows the code rate R calculated using density evolution simulations as a function of the maximum Alice → Bob bit error rate after application of the polar code (black squares right and left of the star). The channel bit error rate is estimated by transmitting and measuring 2^{15} bits, each carrying data, i.e. code rate $R = 1$, over a channel with $\epsilon = 0.59$ and $\alpha = 0.43$ (red star). We design an error-correcting polar code for a codeword of length $N = 2^{15}$ transmitted over N virtual channels. Simulations confirm the possibility to achieve bit error rate $<10^{-4}$ for a code rate $R \approx 0.002$, i.e. $M = R \cdot N = 2^6$ low-error decoded bits.

$N = 2^{15}$ (shown as black squares) estimated using simulations based on density evolution methods [28]. A code rate $R = 2^{-9} \approx 0.002$ can be used with this codeword length to maintain a practical limit of bit error rate (BER) $<10^{-4}$ (blue dashed line) for message transmission using polar coding (see supplemental document; figure S4).

An alternative way of dealing with photon loss (symbol erasures) could be implemented as follows. Instead of putting a message into the quantum states, Alice sends random bits using the quantum states. Bob receives the bit string with erasures and informs Alice which positions in the bit string were erased. The leftover bits constitute a random noisy secret shared between Alice and Bob. By applying information reconciliation and privacy amplification just as in QKD [29–34], a fully secret key is generated. The secret key is used as a one-time pad for transmitting the message. The difference with respect to QKD is that Bob is authenticated by the possession of the PUK. The advantage over the PEAC protocol described in section 2 is that more photon loss can be tolerated; a disadvantage is the increased communication complexity.

3.2. Secure transmission of data

Eve knows everything about the PUK but does not possess the PUK itself. She intercepts the light pulse that Alice sends. Her aim is to learn the bit b by inspecting the pulse. The security of PEAC relies only on one assumption: Eve's (technological) difficulty of determining the used subspace H_0 or H_1. If we do not make this security assumption then PEAC is trivially broken. The subspaces H_0 and H_1 are mutually orthogonal, and hence a simple-to-formulate projective measurement suffices to determine the bit b. Despite the conceptual simplicity of this attack, it is difficult in practice to implement this projective measurement as it requires to: (a) clone the PUK or (b) realize an optical device that performs the PUK's operation with perfect fidelity [17–20].

The PUK used in our implementation is made up of a multitude ($\approx 10^{12}$) of randomly positioned zinc oxide nanoparticles (diameter $= 20 \pm 10$ nm). Cloning this PUK requires first a mapping of the exact position of the scatterers and then a precise nanofabrication of the map. Imprecision in the clone linearly decreases the fidelity of the PUK's operation on the incident light field and thereby increases the bit-flip error α. The clone should replicate the original with >86% similarity (of the optical transmission matrix) to ensure $\alpha < 0.5$. Assuming that the mapping and nanofabrication only results in on-average random perturbations of the nanosphere positions, light scattering theory imposes an error of $\ll 1$ nm per particle to achieve this similarity [35]. In comparison, state of the art 3D nanofabrication can only achieve a resolution of 10–50 nm, thus making it infeasible to clone a PUK in the foreseeable future [36, 37]. An alternative way of mimicking the operation of the PUK would be to create an optical device that emulates the PUK's scattering matrix. In our implementation, this method of attack requires a $K = 900$ mode interferometer, which has to be fully tunable to ensure a high fidelity copy of the PUK's scattering matrix. A K-mode programmable interferometer has $K(K - 1)/2$ beamsplitters and an equal number of phase shifters, i.e. >800 000 optical elements for $K = 900$. The largest programmable optical interferometer to date has ≈100 optical elements [38] and faces challenges in scaling up due to the required component density, programming tolerance of elements, and efficient methods to program such a

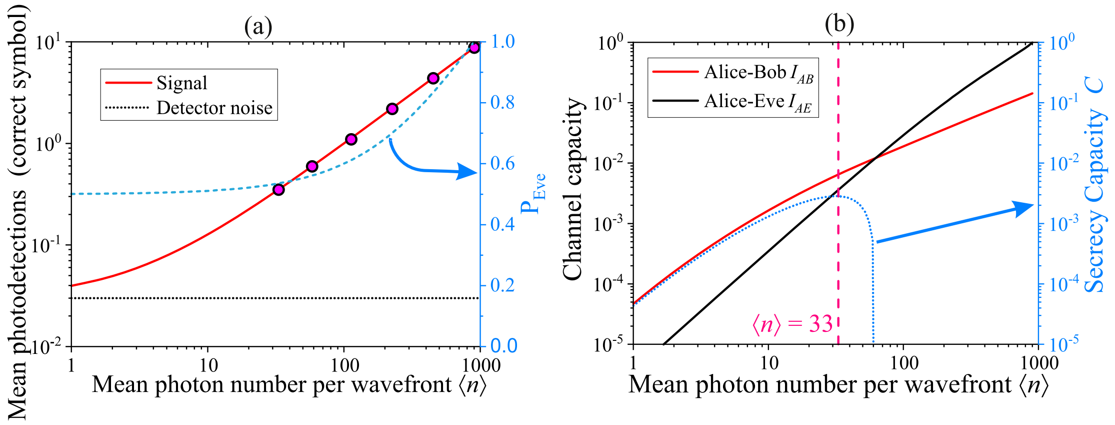

Figure 3. (a) Measured mean number of photodetections per millisecond in the correct symbol with varying mean photon number $\langle n\rangle$ (magenta circles). There were $K = 900$ degrees of freedom on the SLM in our experiment. The measured mean number of photodetections (error smaller than the circle size) agrees well with the estimated number of photodetections for an incident Poisson source with $\langle n\rangle$ photons (red curve). We operate well above the detector dark counts (black dotted curve). Eve's probability P_{Eve} to guess the correct bit value is depicted as the blue dashed curve. Lower P_{Eve} results in a higher level of security. (b) depicts the channel capacity between Alice and Bob I_{AB} (red curve) and between Alice and Eve I_{AE} (black curve) as a function of $\langle n\rangle$. The secrecy capacity $C = I_{\mathrm{AB}}$–I_{AE} is also plotted (blue dotted curve) and reaches its maximum at $\langle n\rangle = 33$.

large interferometer. The orders of magnitude disparity in the state of the art and the requirements highlights the technological infeasiblity in breaking PEAC. The above arguments are not a formalisation of the security assumption 'Eve cannot implement the projective measurement', which we leave for future research. Instead, we provide a heuristic security argument by demonstrating security against one specific class of attacks based on state estimation. We suspect, but cannot prove, that Eve's problem of determining the subspace is as hard as state estimation.

Consider the above scenario where Eve knows Bob's public key and all the details of the symbol encoding scheme. One particular attack is to *estimate the state* ψ and then infer to which subspace ψ belongs. This makes sense given that Eve cannot perform the difficult subspace distinction measurement. We think that this attack is close to Eve's optimal strategy although, as mentioned above, we have no formal proof. The most powerful state estimation is based on universal cloning [18] and known to yield a fidelity $F = (\langle n\rangle + 1)/(\langle n\rangle + K)$ [20], from which we calculate the probability for Eve to correctly guess the subspace to be

$$P_{\mathrm{Eve}} \leqslant \frac{1}{q} + \frac{\langle n\rangle}{K}\frac{K-1}{K+\langle n\rangle}. \tag{1}$$

Here, q is the number of subspaces; in our implementation $q = 2$. In the limit $K/\langle n\rangle \to \infty$, i.e. $\langle n\rangle \ll K$, P_{Eve} goes to 1/2, which corresponds to a random guess. We use notation $S = K/\langle n\rangle$. The quantity S represents the security parameter of QSA [16]. Having $S > 1$ results in $P_{\mathrm{Eve}} < 1$. Figure 3 shows the measured photodetections in the correct detector with varying $\langle n\rangle$. The baseline photodetections are the detector dark counts which impede Bob's measurements at lower $\langle n\rangle$. At $\langle n\rangle = 33$, i.e. $S \approx 27$, the mean number of photodetections in the correct and wrong detector are 0.35 and 0.27, respectively. At $S \approx 27$, $P_{\mathrm{Eve}} = 0.53$, very close to a random guess. The information shared between Alice–Bob and Alice–Eve can be quantified in terms of the channel capacities for Alice–Bob, I_{AB}, and Alice–Eve, I_{AE}, as shown in figure 3(b) (see supplementary document for details). The secrecy capacity for the communication of information between Alice and Bob is $C = I_{\mathrm{AB}}$–I_{AE}. When $C > 0$, the information shared between Alice and Bob is higher than that between Alice and Eve. The error-correcting code has to be tuned such that the Alice → Bob noise is corrected but not the Alice–Eve noise. To ensure secure and error-free transmission of data between Alice and Bob, the designed polar codes should achieve a BER $<10^{-4}$ for the Alice → Bob channel and an extremely noisy Alice → Eve channel (ideally BER=0.5). In our implementation with $C = 0.003$, we succeeded in designing a polar code with $R \approx 0.002$ that concurrently achieves an Alice → Bob BER $<10^{-4}$ and Alice → Eve BER >0.12 (see supplemental document; figure S5). After the error correction step, Eve's partial information can be reduced to zero using privacy amplification techniques. Note that we assume the worst-case scenario in which Eve intercepts all signal photons from Alice with perfect detectors. In contrast, the BER for the Alice → Bob channel is estimated for the imperfect detection (54%) and collection (50%) efficiencies achieved in our setup.

3.3. Discussion

To put the novelty of PEAC in perspective, we compare various cryptography schemes in table 1. While the widely used RSA scheme is a prime example of asymmetric cryptography, it relies on the safekeeping of digital

Table 1. Comparison between different cryptography schemes. Legend: **QC**—Directionality of the Quantum Channel, **SA**—Security Assumption, **CP**—Channel Prerequsites, **KI**—Key Infrastructure, A → B—One-way channel from sender to receiver, A ↔ B—Two-way channel between sender and receiver.

Protocol	Private key	Asymmetric	QC	SA	CP	KI
PEAC	PUK	Yes	A → B	PEAC	Multimode	PUK-based
RSA [1, 3]	Digital	Yes	N/A	Factorization of large numbers	Classical channel	Digital certificates
QKD [4, 5]	Digital	No	A → B	Unconditional	Classical + Quantum channels	N/A
QSA-d [39]	PUK	Yes	A ↔ B	QSA	Multimode	PUK-based
QSA + QKD [40]	PUK	Yes	A ↔ B	QSA	Multimode	PUK-based

keys which are vulnerable to stealthy copying by an adversary. Recent attacks such as Spectre, Meltdown and Heartbleed, as well as high-profile attack tool leaks (Vault7, APT34/Oilrig leak), highlight the vulnerability of cryptographic keys [41]. Furthermore, RSA's reliance on the unproven complexity of factorisation has to be considered a vulnerability. When comparing PEAC to QKD, it is important to keep in mind that QKD achieves a limited goal: given that a symmetric (MAC) key already exists between Alice and Bob, QKD generates more key material. PEAC on the other hand allows Alice and Bob to send messages in an authenticated way, as described at the end of section 3A, even if they have never communicated in the past. This is a complementary functionality. By employing PUKs, the authentication of Bob by Alice using QSA was recently demonstrated [16]. The QSA-d scheme employs a modified QSA experiment to securely transmit data from Bob to Alice [39]. A combination of QSA and QKD realizes an asymmetric cryptography scheme, but at the cost of requiring a two-way channel similar to QSA and QSA-d [40]. With PEAC, we achieve a direct one-way communication channel from Alice to Bob (Alice → Bob). Therefore, PEAC for the first time enables asymmetric cryptography that promises to be as versatile as RSA and alleviates the necessity of storing secrets. The distribution and generation of PUKs can be managed by a central certification authority similar to the implementation of a Public Key Infrastructure for RSA public keys. The process of verifying a digital (RSA) certificate is replaced by the act of communicating with the certification authority in order to get the public key of any party. This is indicated as 'PUK-based' in table 1.

4. Outlook

We demonstrate an asymmetric encryption scheme that does not require storage of any digital secrets. Its security is based on one assumption: the technological infeasibility of distinguishing which subspace a complicated wavefront belongs to. PEAC can be deployed stand-alone or in tandem with classical cryptography; the latter case yields a strong multi-factor encryption with unprecedented security features. The proposed scheme can be readily implemented with available hardware, making it highly attractive for short-term realization. An important aspect in the physical realization of optical PUKs is the sensitivity of their optical response to environmental conditions. Optical PUKs that are robust against mechanical and thermal variations in the environment can be realized in ceramics, electrochemically-etched gallium phosphide and through laser micromachining of glass [42–44]. PEAC can be extended to non-line-of-sight communication, and possibly to distances of several kilometres, by utilizing multimode fibre networks [45] as transmission channels.

Acknowledgments

We thank Klaus Boller, Ad Lagendijk, Mehul Malik, and Willem Vos for discussions. We acknowledge funding from the European Research Council ERC (Grant No. ERC 279248) and the Netherlands Organisation for Scientific Research NWO (Vici Grant No. 680.47.614 and Grant No. 651.002.003).

ORCID iDs

Ravitej Uppu https://orcid.org/0000-0002-8052-9427

References

[1] Menezes A J, Van Oorschot P C and Vanstone S A 1996 *Handbook of Applied Cryptography* (Boca Raton, FL: CRC Press)
[2] Diffie W and Hellman M 1976 *IEEE Trans. Inf. Theory* **22** 644–54

[3] Rivest R L, Shamir A and Adleman L 1978 *Commun. ACM* **21** 120–6

[4] Bennett C H and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing *Int. Conf. Computers, Systems and Signal Processing (Bangalore, India)* pp 8–12

[5] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145–95

[6] Islam N T, Lim C C W, Cahall C, Kim J and Gauthier D J 2017 *Sci. Adv.* **3** e1701491

[7] Bennett C H, Brassard G and Breidbart S 2014 *Nat. Comput.* **13** 453–8

[8] Fehr S and Salvail L 2017 Quantum authentication and encryption with key recycling *Advances in Cryptology—EUROCRYPT 2017* ed J S Coron and J B Nielsen (Cham: Springer) pp 311–38

[9] Škorić B and de Vries M 2017 *Int. J. Quantum Inf.* **15** 1750016

[10] Hillery M, Bužek V and Berthiaume A 1999 *Phys. Rev.* A **59** 1829–34

[11] Gottesman D and Chuang I L 2001 arXiv:quant-ph/0105032

[12] Nikolopoulos G M 2008 *Phys. Rev.* A **77** 032348

[13] Pappu R, Recht B, Taylor J and Gershenfeld N 2002 *Science* **297** 2026–30

[14] Buchanan J D R, Cowburn R P, Jausovec A V, Petit D, Seem P, Xiong G, Atkinson D, Fenton K, Allwood D A and Bryan M T 2005 *Nature* **436** 475–475

[15] Javidi B *et al* 2016 *J. Opt.* **18** 083001

[16] Goorden S A, Horstmann M, Mosk A P, Škorić B and Pinkse P W H 2014 *Optica* **1** 421–4

[17] Škorić B 2016 *Quantum Inf. Comput.* **16** 50–60

[18] Bruß D, Ekert A and Macchiavello C 1998 *Phys. Rev. Lett.* **81** 2598–601

[19] Derka R, Bužek V and Ekert A K 1998 *Phys. Rev. Lett.* **80** 1571–5

[20] Bruß D and Macchiavello C 1999 *Phys. Lett.* A **253** 249–51

[21] Brassard G, Lütkenhaus N, Mor T and Sanders B C 2000 *Phys. Rev. Lett.* **85** 1330–3

[22] Mosk A P, Lagendijk A, Lerosey G and Fink M 2012 *Nat. Photon.* **6** 283–92

[23] Rotter S and Gigan S 2017 *Rev. Mod. Phys.* **89** 015005

[24] Huisman T J, Huisman S R, Mosk A P and Pinkse P W H 2014 *Appl. Phys.* B **116** 603–7

[25] Wang D, Zhou E H, Brake J, Ruan H, Jang M and Yang C 2015 *Optica* **2** 728–35

[26] Uppu R, Wolterink T A W, Goorden S A, Chen B, Škorić B, Mosk A P and Pinkse P W H 2019 Public key of the zinc oxide PUK https://doi.org/10.6084/m9.figshare.7609136

[27] Arıkan E 2009 *IEEE Trans. Inf. Theory* **55** 3051–73

[28] Mori R and Tanaka T 2009 *IEEE Commun. Lett.* **13** 519–21

[29] Csiszár I and Körner J 1978 *IEEE Trans. Inf. Theory* **24** 339–48

[30] Bennett C H, Brassard G and Robert J M 1988 *SIAM J. Comput.* **17** 210–29

[31] Bennett C H, Bessette F, Brassard G, Salvail L and Smolin J 1992 *J. Cryptol.* **5** 3–28

[32] Maurer U M 1993 *IEEE Trans. Inf. Theory* **39** 733–42

[33] Deutsch D, Ekert A, Jozsa R, Macchiavello C, Popescu S and Sanpera A 1996 *Phys. Rev. Lett.* **77** 2818–21

[34] Renes J M and Renner R 2011 *IEEE Trans. Inf. Theory* **57** 7377–85

[35] Berkovits R 1991 *Phys. Rev.* B **43** 8638–40

[36] Soukoulis C M and Wegener M 2011 *Nat. Photon.* **5** 523

[37] Yamazaki K, Yamaguchi T and Namatsu H 2004 *Japan. J. Appl. Phys.* **43** L1111

[38] Carolan J *et al* 2015 *Science* **349** 711–6

[39] Škorić B, Pinkse P W H and Mosk A P 2017 *Quantum Inf. Process.* **16** 200

[40] Wolterink T A W 2016 Programmable quantum interference in massively multichannel networks *PhD Thesis* University of Twente

[41] Schwarz M, Weiser S, Gruss D, Maurice C and Mangard S 2017 Malware guard extension: using SGX to conceal cache attacks *Detection of Intrusions and Malware and Vulnerability Assessment* ed M Polychronakis and M Meier (Cham: Springer International Publishing) pp 3–24

[42] Schuurmans F J P, Vanmaekelbergh D, van de Lagemaat J and Lagendijk A 1999 *Science* **284** 141–3

[43] Matoba O, Kitamura Y, Manabe T, Nitta K and Watanabe W 2009 *Appl. Phys. Lett.* **95** 221114

[44] Zhang H and Tzortzakis S 2016 *Appl. Phys. Lett.* **108** 211107

[45] Bozinovic N, Yue Y, Ren Y, Tur M, Kristensen P, Huang H, Willner A E and Ramachandran S 2013 *Science* **340** 1545–8