npj | Quantum Information

www.nature.com/npjqi

ARTICLE OPEN

Check for updates

Probabilistic one-time programs using quantum entanglement

Marie-Christine Roehsner[1,6]✉, Joshua A. Kettlewell[2,3,4], Joseph Fitzsimons[5] and Philip Walther[1]✉

Quantum technology allows for unparalleled levels of data and software protection. Probabilistic one-time programs harness these capabilities for quantum-assisted classical computations by encoding classical software in small quantum states resulting in computer programs that can be used only once. Such self-destructing one-time programs facilitate a variety of applications reaching from software distribution to one-time delegation of signature authority. Whereas previous experiments demonstrated the feasibility of such schemes, the practical applications were limited. Here we present an improved protocol for one-time programs that resolves major drawbacks of previous schemes, by employing entangled qubit pairs. This results in four orders of magnitude higher count rates and the ability to execute a program long after the quantum information exchange has taken place. We implement a one-time delegation of signature authority over an underground fiber link between university buildings in downtown Vienna, emphasizing the compatibility of our scheme with prepare-and-measure quantum internet networks.

npj Quantum Information (2021)7:98 ; https://doi.org/10.1038/s41534-021-00435-w

INTRODUCTION

Computational algorithms touch almost every aspect of modern life. In light of continuous data breaches and increasingly stricter legislation on data protection, it would be desirable to reduce the amount of private user data leaked in a computation without forcing software owners to completely reveal their source code. Quantum computers have been shown to offer significant advantages in this area. A prominent example is blind quantum computation, where an almost classical client can delegate a quantum computation such that the quantum server cannot learn any information regarding the input, output and algorithm of the quantum computation.[1–5] While protocols such as this clearly demonstrate that quantum systems can provide powerful enhancements to the privacy of computations, full scale quantum computers still present significant technical challenges. Thus, it is of particular interest to investigate hybrid quantum-classical solutions which might allow for quantum enhancements of classical technology as well.

A promising direction of investigation is to use small quantum systems (such as single photons, which can be readily generated and manipulated by state-of-the-art quantum technology) to augment classical computers, and in particular to use them as a resource to increase the privacy of computations. A well-known example of such hybrid systems are quantum key distribution protocols.[6,7] Recently, another such hybrid system was demonstrated for probabilistic one-time programs.[8] One-time programs are a cryptographic primitive for performing secure computation in which a server provides a client with a software in such a way that the client can obtain only one input-output pair (x, $f(x)$) before the program is destroyed. Both the input of the client and the software of the server remain private (up to the information that is leaked by the input-output pair). One-time programs are considered as a powerful building block for many cryptographic tasks and could be used for applications such as software licensing, one-time delegation of signing abilities and electronic voting schemes. It has, however, been shown that perfect information theoretically secure quantum and classical one-time programs are impossible to implement without the use of one-time self-destructing hardware (hardware which is automatically destroyed after a single use).[9–11] These no-go results can be circumvented by allowing for the possibility of error in the program outcome resulting in probabilistic one-time programs.[8]

Probabilistic one-time programs encode classical software onto single-qubit quantum states which are then sent to a client for evaluation. The client can choose the input to the program by choosing the basis they measure the qubit in using a measurement operator taken from a set of anti-commuting operators. Thus, evaluation for one input prevents them from gaining information about a complimentary input. The output of the measurement will be the output of the gate. While demonstrating the implementability of probabilistic one-time programs the protocol presented in[8] faced a number of challenges with respect to theory and technological requirements that limit the practical implementation.

One of the most important challenges in the practical implementation of any quantum communication protocol is loss tolerance. As no real-life quantum channel is without loss, in order for a protocol to be practical, it must allow for a certain level of loss of information. While the previous scheme could achieve loss tolerance, this came at the price of a sub-routine that required the program sender and receiver to implement classical back-and forth communication after the exchange of each individual qubit. Furthermore, it required the receiver of the one-time program to immediately execute the program unless they had access to a non-demolition measurement of the photon number (to perform the loss-tolerance sub-routine) and a quantum memory. Finally, the gate rates of the scheme were limited by the mentioned need for a large amount of classical communication as well as the need of active polarization switches, resulting in a gate rate of about 0.7 Hz.

Here we present an improved protocol that exploits quantum entanglement to overcome the aforementioned limitations. We further demonstrate the enhanced practicality for real-life scenarios by using OTPs to digitally sign a message protocol using an underground fiber link that connects two buildings of the University in Vienna. Experimentally, our protocol is based on sharing a

[1]Vienna Center for Quantum Science and Technology, Faculty of Physics, University of Vienna, Vienna, Austria. [2]Singapore University of Technology and Design, Singapore, Singapore. [3]Centre for Quantum Technologies, National University of Singapore, Singapore, Singapore. [4]Staple AI, Singapore, Singapore. [5]Horizon Quantum Computing, Singapore, Singapore. [6]Present address: QuTech & Kavli Institute of Nanoscience, Delft University of Technology, Delft, The Netherlands. ✉email: m.roehsner@tudelft.nl; philip.walther@univie.ac.at

Published in partnership with The University of New South Wales

npj nature partner journals

maximally entangled qubit pair, a so-called Bell state,[12] among the software provider (Alice) and the client (Bob), who shall use the software only once. Alice performs random measurements on her half of the Bell state that lead to the remote preparation of four different states, covering all possible one-bit software gate operations, on Bob's side. Bob randomly chooses his measurement basis which defines input 0 or input 1. This leads to a shared table of randomly prepared input-output pairs. Now, when Alice and Bob keep their lists of respective outcomes, then Alice and Bob can use classical communication only to select the required gates for implementing the program with the corresponding input. Here it is important to point out that the execution of the program can happen long after the quantum information exchange and without any need for long-term quantum memories. From a technological point of view this scheme allows for a strongly improved gate rate for the transmission of gates as this protocol relies only on passive optical elements. This is demonstrated by achieving gate rates of about 10 kHz after a transmission via a 650 m of fiber link that runs partially through Vienna's underground sewer system; corresponding to an increase in gate rate of four orders of magnitude when being compared to previous schemes that had to use active state preparation for each gate. Besides the demonstration of delegated probabilistic one-time programs by making use of a previously established commodity table, we show that low-noise applications are possible via the implementation of one-time delegation of signature authority. We achieve success probabilities of >99% for having Bob, as client, signing a message in Alice's (the program provider's) name.

RESULTS

Theory

We define a one-time program as follows: a sender or provider, Alice, supplies resources related to a function $f(\cdot)$ to a receiver or client, Bob, which allow him to evaluate $f(x)$ while gaining no knowledge of $f(x')$, for any $x' \neq x$, other than what is directly implied by $f(x)$. Alice in turn obtains no information regarding Bob's input x. As it was shown that perfect, information theoretically secure OTPs in the classical and quantum case are impossible without further assumptions on hardware or abilities of an adversary[9,10,13] we allow for a bounded probability of error in the program output when encoding classical software onto quantum states[8] yielding probabilistic one-time programs. To achieve these probabilistic OTPs we start with the most basic logical gates which map a single input bit to a single output bit. We will refer to these gates as $\mathcal{G}_1$ gates. Alice will encode her choice of gate onto a quantum state (typically a qubit) while Bob's input will correspond to his measurement basis. We choose to encode Bob's input as measurement in σ_Z for an input of 0 and a measurement in σ_X for an input of 1. This allows Alice to, probabilistically, encode the four possible $\mathcal{G}_1$ gates (Identity, NOT, Constant-Zero and Constant-One) as one of the following four single-qubit quantum states (truth tables of the gates and Bloch-sphere representation of the states are shown in Fig. 1a):

$$|\Psi_0\rangle = \frac{1}{\sqrt{2+\sqrt{2}}}(|0\rangle + |+\rangle) \tag{1}$$

$$|\Psi_1\rangle = \frac{1}{\sqrt{2+\sqrt{2}}}(|1\rangle - |-\rangle) \tag{2}$$

$$|\Psi_{\mathrm{Id}}\rangle = \frac{1}{\sqrt{2+\sqrt{2}}}(|0\rangle + |-\rangle) \tag{3}$$

$$|\Psi_{\mathrm{not}}\rangle = \frac{1}{\sqrt{2+\sqrt{2}}}(|1\rangle + |+\rangle) \tag{4}$$

where $|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)$.

It has been shown[8] that these four basic gates allow for universal classical computing when being combined with a larger classical circuit in a fixed configuration. Remarkably, the circuit arrangements can be public as only the basic gate operations need to be secret to hide the implemented software.

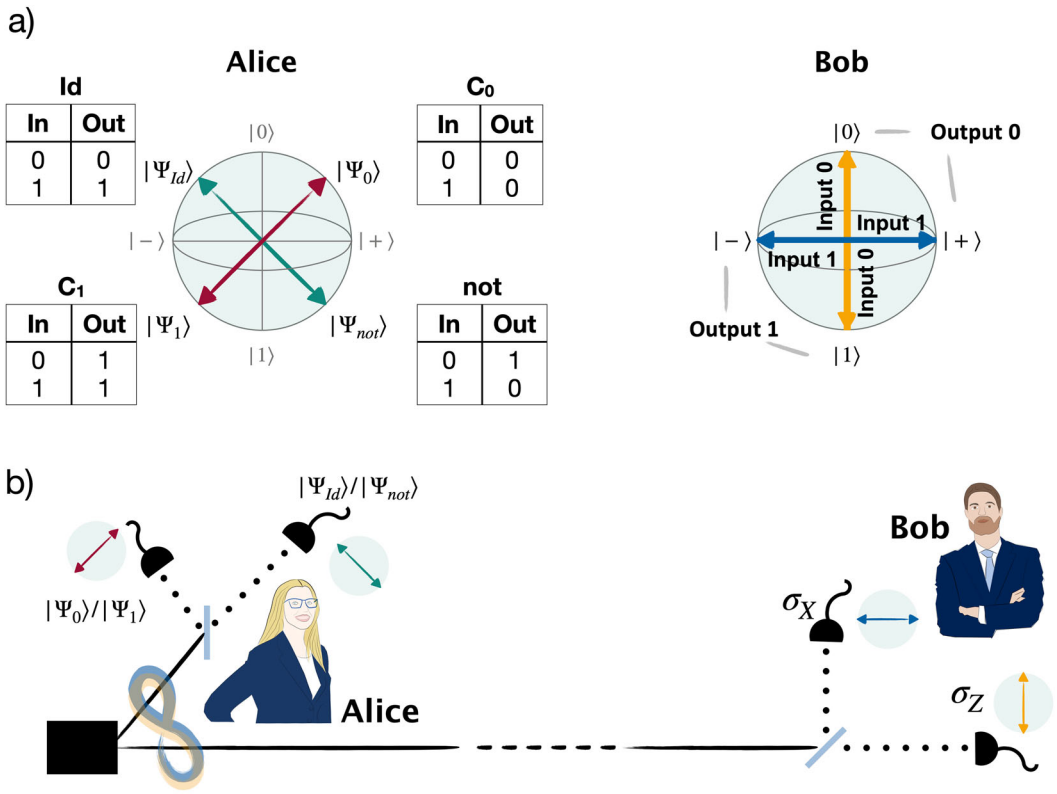
In the original OTP scheme the basic gates were consecutively mapped onto quantum states, realized as single photons, and then send to a receiver that had to measure them in the same exact order for implementing the function (software). The scheme presented here exploits quantum entanglement to create randomness as a resource for an enhanced protocol that allows to share OTPs that can be used at any time.

The protocol is composed of two distinct parts: a quantum part in which Alice sends a random sequence of gate-OTPs which Bob measures in a random basis and a classical part where classical communication is used to implement a OTP using the previously shared information from the quantum part. To randomly prepare one of the gate states ($|\Psi_0\rangle, |\Psi_1\rangle, |\Psi_{\mathrm{Id}}\rangle, |\Psi_{\mathrm{not}}\rangle$) Alice generates a maximally entangled Bell-state, measures it randomly in one of two bases ($|\Psi_0\rangle/|\Psi_1\rangle$) or ($|\Psi_{\mathrm{Id}}\rangle/|\Psi_{\mathrm{not}}\rangle$) which leads to a remote state generation on the other qubit that is sent to Bob. Thus, Bob will receive a random gate-OTP which he will randomly measure in σ_Z (input 0) or σ_X (input 1). Alice notes the gates sent while Bob records the input-output pairs, and both keep their results private. The remaining events make up a table of imperfectly correlated results where the percentage of correct input-output pairs is given by $P_1 = \frac{1}{2\sqrt{2}} + \frac{1}{2} \approx 0.85$. This is referred to as a *shared table* and will later be used as classical commodity or resource to perform a program. Alice and Bob repeat this process until they have constructed a shared table of sufficient length for the program(s) they want to perform. Note that this results in the sequence of gates being independent and identically distributed.

In case of channel losses Alice and Bob will exchange information about when they have sent and received qubits, respectively. Only the results of events in which both parties agree that a qubit was sent and measured will be kept, and all other results should be discarded. Thus, channel losses do not affect the security of the protocol, as only coincidence events generate entries in the shared table. All other lines of the shared table are not used for any evaluation of logic gates, and are each randomly generated from the set of possible states. These states thus provide no information to Bob regarding the program. The quantum states Bob utilizes for the evaluation of the protocol are identical to those given in previous schemes.[8] With the addition of quantum memories and heralded photon arrival the protocol may become non-interactive. The current interactive portion of the protocol may then instead be viewed as a transmission control step, which is followed by classical communication to distribute the one-time program to Bob.

The shared table created by the measurement of the quantum states is analogous exactly to noisy versions of Beaver triples, which are known to be sufficient for secure computation.[14]

After the distribution the shared table can be used to run an OTP (see flow chart in Fig. 2). To execute a gate Alice will first generate a random bit r. If $r = 0$ she looks at her part of the shared table and finds a line with the desired gate, if $r = 1$ she finds a line with the opposite gate (i.e., the gate for which all outputs are flipped). Lines she skips over while looking for an appropriate gate will be deleted from the table. She will then ask Bob if he can use this line. If Bob's desired input is equal to the (random) input in that line of the table, he will accept. Otherwise he will decline the use of the line and they will repeat the process (using a newly generated r). Only when Bob accepts to use a line Alice will reveal the corresponding value of r. If $r = 1$ Bob will have to flip the result of the gate used. Once a line is used (accepted or declined) it will be deleted from the shared table. Alice and Bob will iterate this process until the desired circuit is completed. The use of the random one-time-pad (r) to



Run #	Gate Alice projects on	Gate sent to Bob	Measurement Basis Bob	Input	Output
1	C_0	**C_1**	σ_X	**1**	**1**
2	Id	**not**	σ_Z	**0**	**1**
3	not	**Id**	σ_Z	**0**	**0**
4	C_1	**C_0**	σ_X	**1**	**0**

Fig. 1 Illustration of the scheme for implementing probabilistic one-time programs. In **a**, we show the truth tables defining all possible 1-bit logic gates together with the quantum states representing the different $\mathcal{G}_1$ gates on the Bloch-sphere. In **b**, we give the mapping of Bob's binary inputs to a measurement basis. An input of 0 maps to a measurement in the σ_Z (Z) basis while an input of 1 maps to a measurement in the σ_X (X) basis. Outputs are defined to be 0 if Bob projects onto the positive eigenstate and 1 for the negative eigenstate. The success probability of the gates is given by $P_S = \frac{1}{2\sqrt{2}} + \frac{1}{2} \approx 0.85$. **b** Establishing the shared table: Alice randomly prepares one of the four possible 1-bit gate-OTPs by randomly measuring her $|\Psi^-\rangle$ Bell-state in one of the two bases given by $|\Psi_0\rangle/|\Psi_1\rangle$ and $|\Psi_{Id}\rangle/|\Psi_{not}\rangle$. This collapses Bob's qubit into the orthogonal state which is sent over a quantum channel to Bob. He will randomly measure in σ_Z or σ_X, corresponding to a random input of 0 or 1 to the gate. Alice notes the gates sent (blue shaded column) and Bob the inputs and outputs of the gate (red shaded columns). These (classical) records form the shared table which will later be used to execute a program. Alice and Bob repeat this procedure until a sufficient amount of gate-OTPs has been exchanged. To increase clarity of the illustrations the gates are shown here with a 100% success probability. In a real implementation Bob will receive the correct output with a probability of $P_S \approx 0.85$.

encrypt Bob's output prevents information leakage in the case that Bob chooses to not use any given line (honestly or dishonestly) as without the line's pad value he gains no information. If the individual gates are used as building blocks for a larger circuit Alice might be concerned about Bob learning the intermediate results of this circuit. She can prevent this by randomly inserting pairs of NOT gates, with a probability of 1/2, between the gates and subsequently absorbing them into the neighboring gates as described in[8]. This will not alter the outcome of the overall program but effectively apply a one-time pad on the intermediate results of the circuit.

Remarkably, the quantum channel connecting Alice and Bob only needs to be maintained for the period required to generate the shared table. Thus, the creation of the shared table may occur long before the classical communication to execute a program and a large shared table might be used to execute several programs.

Finally, we would like to note that our OTPs are similar to noisy examples of random $\binom{2}{1}$-oblivious transfer (OT), a versatile cryptographic resource allowing a user to access a subset of database entries or messages a sender transmits without the sender knowing which entry was accessed. OT is known to be sufficient for many secure multi-party processes[14–16] such as homomorphic encryption[17] and bit commitment.[18] Classically, OT may only be performed with assumptions on the computational power of the parties[19] and is known to be impossible to implement even with quantum computers when information theoretic security is required.[13]

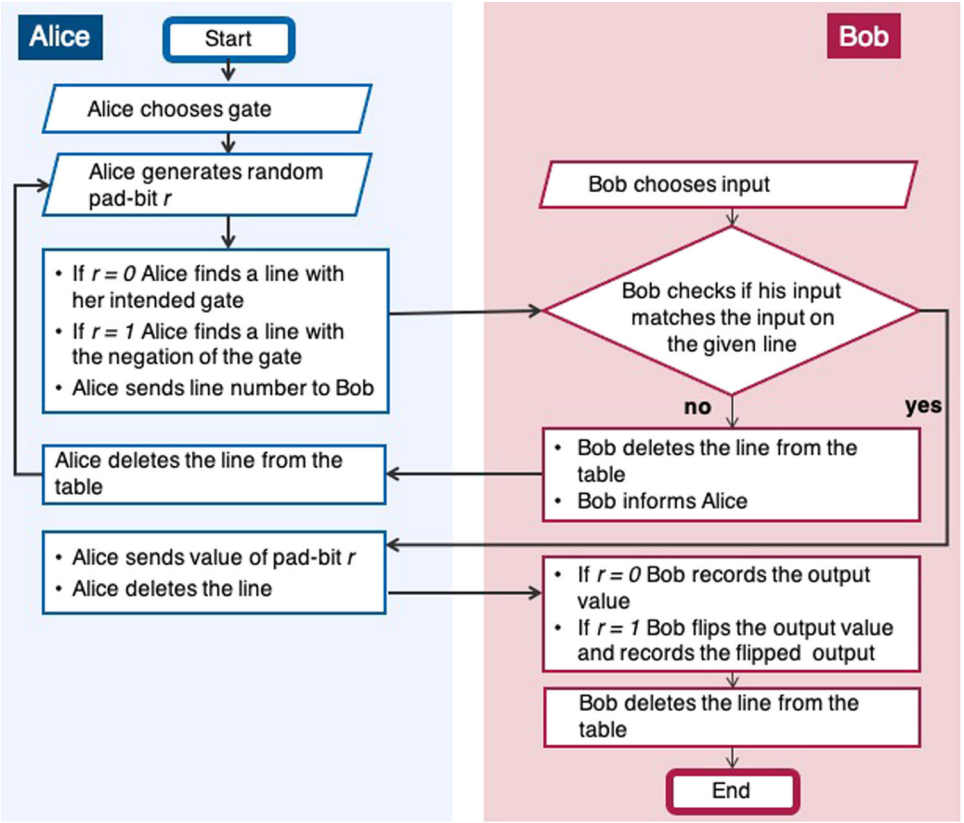


Fig. 2 Flow chat showing the instructions for Alice and Bob to securely evaluate a single $\mathcal{G}_1$ gate-OTP. The runtime of the classical part scales linearly with the complexity of function and latency between the parties as shown in the Mathods section.

Experimental implementation

We experimentally demonstrated our entanglement-based one-time programs between two university buildings separated by ~200 m air-line distance (~650 m in fiber) in down-town Vienna.

Alice initially prepares a maximally entangled Bell-state $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle|1\rangle - |1\rangle|0\rangle)$. She keeps one of the qubits in her local laboratory and sends it to a 50/50-beamsplitter. One output arm of the beamsplitter leads to a measurement device configured to measure in the basis spanned by $|\Psi_0\rangle$ and $|\Psi_1\rangle$, while qubits leaving the beamsplitter in the other output will be measured in the basis given by $|\Psi_{\mathrm{Id}}\rangle$ and $|\Psi_{\mathrm{not}}\rangle$. The second qubit is sent to Bob through a quantum channel, which is realized by a standard telecom fiber that is located partially in Vienna's sewer system. Bob uses a similar measurement apparatus as Alice, which also relies on a 50/50-beamsplitter leading to measurement devices projecting in σ_Z and σ_X bases. Both Alice and Bob record their measurement results and thus the gates send respectively the input and output of the program, which allows them to generate the shared table. A scheme of our set-up is shown in Fig. 3.

To prepare the Bell state Alice uses a dedicated photon source design (adapted from[20]) for generating entangled photon pairs with tailored wavelengths such that the transmitted photon faces minimal absorption loss in fiber and that the local photon can be efficiently detected with standard detector technology. This single-pass spontaneous parametric down conversion (SPDC) source emits highly non-degenerate polarization entangled photons pairs in the $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|H\rangle_s|V\rangle_l - |V\rangle_s|H\rangle_l)$ Bell state, where $|H\rangle$ corresponds to horizontal and $|V\rangle$ to vertical polarization and s and l denote the short (785 nm) and long (1498 nm) wavelength path. In our source two down-conversion processes are phase-matched in the same crystal yielding photon pairs of $|H\rangle_s|V\rangle_l$ as well as $|V\rangle_s|H\rangle_l$ polarization. These are superimposed to create a Bell-state of the form $\frac{1}{\sqrt{2}}(|H\rangle_s|V\rangle_l + e^{i\theta}|V\rangle_s|H\rangle_l)$. To ensure the spectral indistinguishably of these two processes a tunable narrow bandwidth-filter is inserted in the long wavelength path. A phase shifter is used to compensate for the varying time delays due to mismatched group velocities in the crystal and a liquid crystal retarder is used to set the phase angle θ of the produced Bell state. The pump-wavelength and crystal poling-period were chosen such that the source emits one photon in the Telecom range at 1498 nm (Telecom S-Band) and the other photon in the near-infrared range at 785 nm which is a standard wavelength for optical manipulation and in particular for efficient detection by using commercial Silicon Avalance Photo-Diodes. The Telecom (1498 nm) photon is sent through approximately 650 m of fiber to Bob's laboratory where they are detected by superconducting nano-wire detectors, as this wavelength suffers from low losses in fiber transmission. This results in a coincidence and thus gate rate of 10 kHz corresponding to an improvement in gate rate by four orders of magnitude compared to the previous implementation.[8]

Implemented program

We show the experimental implementation of a protocol for one-time delegation of signature authority in which Alice enables Bob to sign exactly one message in her name. While in general the complexity of programs that can be implemented by our approach is limited by their probabilistic nature, this protocol's success probability can be increased (in principle arbitrarily close to 1) without compromising the security.[8] Digital signatures are a widely employed technique used for contract signing, software distribution, e-mails and numerous other applications. Sometimes it is desirable to delegate these capabilities (e.g., to a lawyer), which classically corresponds to handing over one's private key. However, this enables the recipient to sign an unlimited number

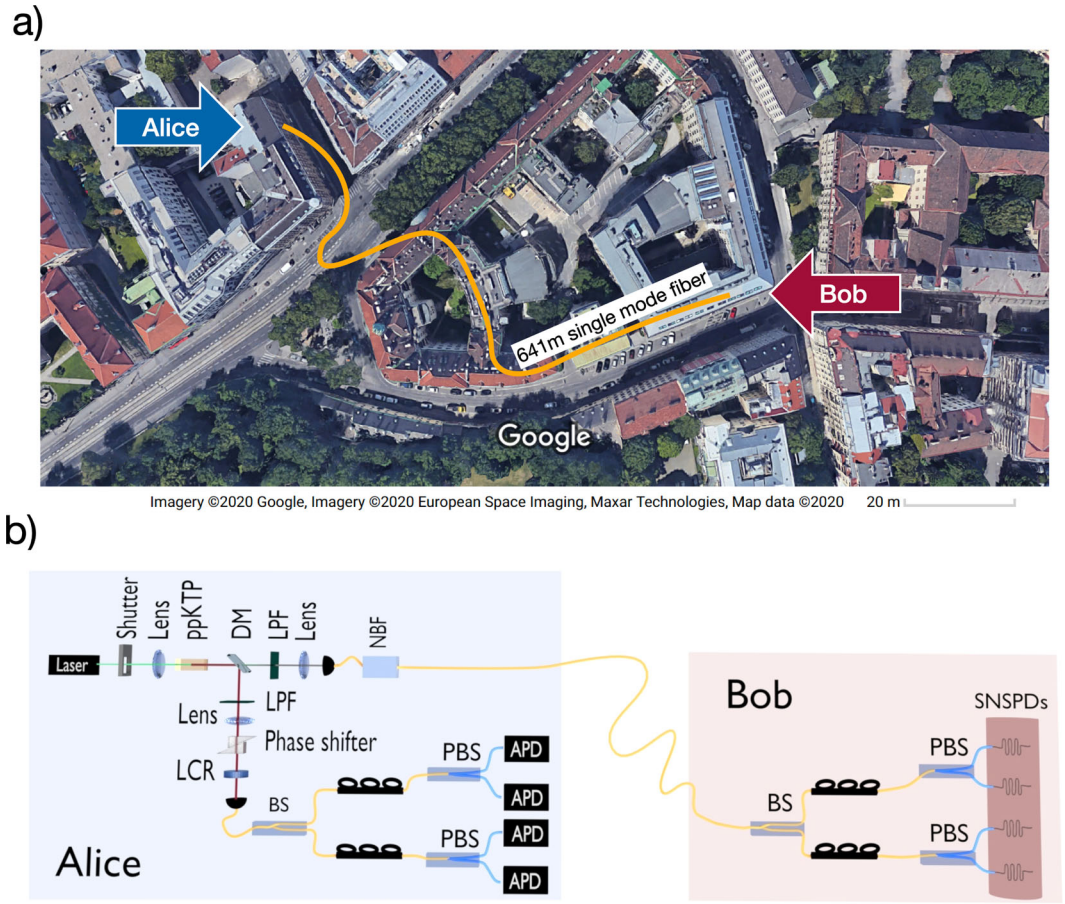


Fig. 3 Overview of the experimental setup. a The laboratories of Alice and Bob are located at different buildings of the University in Vienna, but connected by a quantum channel consisting of a single-mode fiber (Corning SMF-28) with a lenght of 641 m. **b** Polarization entangled photons are created via SPDC using a 515nm cw-pump-laser directed on to a ppKTP crystal, emitting polarization-entangled photon pairs in a $|\Psi^-\rangle = \frac{1}{\sqrt{2}}(|H\rangle_s|V\rangle_i + e^{i\theta}|V\rangle_s|H\rangle_i)$ Bell state with $\lambda_s = 785$ nm and $\lambda_i = 1498$ nm (Telecom S-Band). A dichroic mirror (DM) separates the photons by wavelength followed by a long-pass filter (LPF) to block the pump light in both arms and a narrow bandwidth filter (NBF), to ensure spectral indistinguishability of the *H* and *V* photons, in the long-wavelength arm. In the short-wavelength arm we use calcite wedges as phase shifters to compensate temporal walk-off and a liquid crystal retarder (LCR) to set precisely the phase θ in the Bell state. Alice uses a beam-splitter (BS) to randomly choose her measurement basis. The measurement is realized using in-fiber polarization control, two fiber-polarizing beam-splitters (PBS) and four Si-Avalanche-Photo-Diodes (APD). The second photon is transmitted through ≈ 650 m of standard Telecom fiber to Bob's laboratory. Bob uses one fiber-BS, in-fiber polarization control, two PBSs and four superconducting nanowire single-photon detectors (SNSPDs) to randomly measure the received photons in one of two bases σ_Z and σ_X corresponding to input 0 and 1, respectively.

of messages as the classical software used for signing can, in principle, always be copied. Thus, should one wish to limit the number of messages that can be signed, this cannot be done classically. OTPs on the other hand enable us to implement a one-time delegated signatures as introduced in[8] with information theoretic security following the described steps:

1. Encryption: Alice prepares a set of OTPs that will perform encryption with her private key(s). As the encryption will be done bitwise it is sufficient to use $\mathcal{G}_1$ gate-OTPs in this step. She sends these gate-OTPs over to Bob. For every bit that Bob wants to encrypt, Alice will send *N* independently encrypting gate-OTPs. These will result in multiple independent encryptions which will later allow her to achieve an increased probability of success.
2. Message: Bob chooses the message he wants to sign in Alice's name. As in classical digital signatures he takes the hash of this message which ensures that his input into the protocol will always be of the same length *m*.
3. Signing: Bob uses the bits of his hash as inputs into the gate-OTPs. The output of the gate-OTPs will form the delegated signature. As he receives *N* gate-OTPs per bit of the hash, the length of the signature will be $L = m{\cdot}N$.
4. Verification: Bob sends the signature together with the signed message back to Alice for verification. Alice will accept the signature as valid if the expected percentage of output bits is correct. Thus, she will define a lower bound or threshold τ on the probability of success she will accept for the encryption of every individual bit in the hash. Should one or more bits of the hash have been signed with a probability of success below her threshold she will abort the protocol (see also Fig. 4b).

Intrinsically the individual gate-OTPs have a success probability of $P_S = \frac{1}{2\sqrt{2}} + \frac{1}{2} \approx 0.85$. The overall success probability of the protocol is however increased by using multiple gate-OTPs per bit of the hash. In fact, by increasing *N* the probability that at least $\tau \cdot N$ evaluations are correct (i.e., the success probability of the signature) asymptotically approaches 1. It is important to note that in order to maintain the security of the protocol the *N* gate-OTPs that are used per bit of the hash are not mere copies of each other but encrypt the bit independently, i.e., with a different private key.

Experimentally we implemented a one-time delegated signature using $N = 1000$ and a SHA3-224 hash ($m = 224$), thus per signature we evaluate $L = N \cdot m = 224{,}000$ gate-OTPs. Due to experimental imperfections the probability of success is reduced to $P_S^{exp} = 0.831 \pm 0.013$. Given these values we analyzed the probability of success for a honest Bob, trying so sign one-and-only-one message, compared to a cheating Bob. To bound the probability of successful cheating we assume the smallest deviation and thus worst-case in which Bob tries to sign a second message that differs in just one bit of the hash from his first message. We consider his probability of success in dependence of Alice's threshold value τ. Furthermore, we assume that a cheating Bob can achieve the theoretical maximum for $P_S^{th} = \frac{1}{2\sqrt{2}} + \frac{1}{2} \approx 0.85$. Thus, unless Bob can exploit a collision in the classical hash, our values give an upper bound for his probability of success. Considering these numbers we choose $\tau = 0.776$ to maximize the difference in probability of success between an honest and a cheating Bob as shown in Fig. 4 where we plot the respective success probabilities in dependence of τ. At this value a cheating Bob has a probability of success of $P_{cheat} = 0.11\%$ while an honest Bob achieves $P_{hon} = 99.87\%$. The derivation for evaluating optimal values of τ to maximize the difference in probability of success of the different strategies has previously been shown.[8]

In Fig. 5 we show a histogram of the combined results of 50 (honest) delegated signatures (corresponding to 11,200,000 evaluated gate OTPs) where each bar is generated using the results of 1000 OTPs. It can be seen that due to experimental imperfections and drifts in the setup that the average success probability is lower than the theoretical maximum (green line) and has a larger standard deviation than expected by a binomial

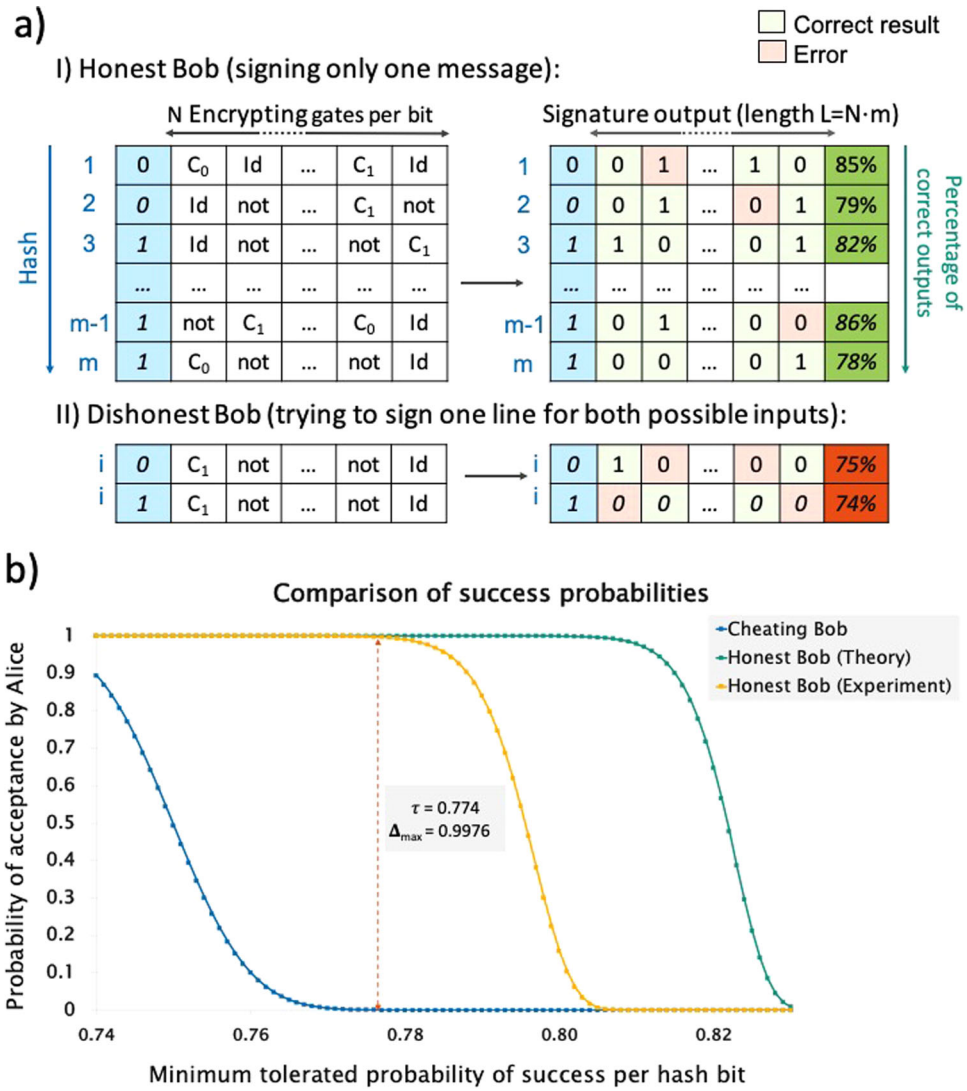


Fig. 4 Illustration of the delegated signature protocol. In **a**, we show the evaluation of a signature. Alice and Bob evaluate $L = N \cdot m$ lines from the shared table, according to the hash of Bobs messages. The signature produces a N bit string for each bit of the hash, each one required to be correct in $\tau \cdot N$ positions, where the correct output is defined as a ideal implementation of the gate. τ is chosen according to the length of N to maximize the difference between honest and dishonest probabilities. If Bob tries to cheat and sign two messages that differ in only one bit of the hash he has to obtain two sets of correct outputs for N gates (corresponding to one line). This will reduce his average success probability as shown in[8] and thus his probability to surpass Alice's threshold. The numbers shown in **a** are for explanatory purposes only and do not correspond to experimental data. **b** The probabilities of signing 1 (honest) or 2 (dishonest) messages using a signature length of $N = 1000$ and a hash output size of 224 bits. The difference between the honest (experimental) and dishonest probability of success depends on the chosen threshold value τ. This difference is maximized (at 0.9976) for the experimentally found values for a threshold value of 0.774 (indicated by the red dotted line) which corresponds to a success probability of 0.9987 and a cheating probability of 0.0011.

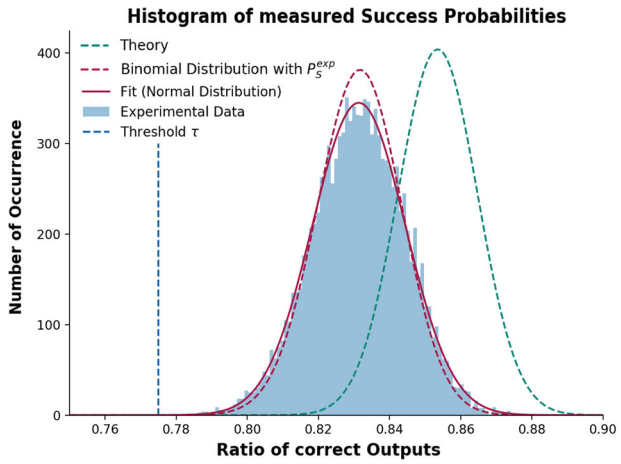


Fig. 5 Cumulative histogram of success probabilities. The light blue bars show the experimentally found probabilities of success per bit of the hash for 50 signatures with 224 hash-bits each, thus from 11200 evaluations (with $N = 1000$, thus 112, 000, 000 evaluated gate-OTPs). While due to experimental imperfections the probability of success is lower than the theoretical maximum, nevertheless Alice's acceptance threshold τ is passed every single time. To characterize the found distribution we compare it the theoretical (noiseless) prediction (dashed green line) as well as to a binomial distribution with the experimentally found mean $\mu^{\exp} = 0.831$ (red dashed line) and a fit to the histogram (normal distribution, red solid line, $\mu^{\exp} = 0.831, \sigma_{\exp} = 0.013$). We attribute the slightly increased standard deviation in the data compared to the binomial distribution to drifts in the set-up during data acquisition.

distribution of this mean (red line). Nevertheless, the protocol is successfully implemented and the threshold of acceptance by Alice is surpassed every single time.

The evaluation of L gate-OTPs would trivially require evaluating L rounds of communication to complete. However, as none of the gates in the signature scheme are causally connected, Alice and Bob may evaluate all of them concurrently, thus reducing the expected required rounds of communication to $\log_2(L)$ where L is the total number of gate-OTPs. Therefore, on average our example program could be implemented using only 18 rounds of classical communication. Should Alice and Bob be willing to use $O(\log_2(L))$ lines per input the amount of communication rounds can be made constant with a high probability.

DISCUSSION

We have presented a protocol for probabilistic one-time programs overcoming previous challenges in theory and experiment. Our implementation exploits quantum entanglement as a resource to achieve random remote state preparation resulting in a shared table of correlated input-output pairs between Alice and Bob. Through separating the quantum communication from the actual program execution, we enable client and sender to perform a one-time program at an arbitrarily later time only using classical communication. By deploying our experiment between two university buildings, connected by an underground quantum link we demonstrate the significant advantages of this method over the previous state of the art, allowing for four orders of magnitude higher gate-rates than in previous experiments. Additionally, the use of quantum entanglement enables the detection of an eavesdropper, attempting to steal the program. We believe that can be the basis for a wide field of further investigations including protocols and connections to known protocols like oblivious transfer and quantum money.[21–23] Further advances in source and detector technologies, would allow gate rates to be increased even further. We believe that this demonstration indicates the compatibility of our schemes with early quantum internet implementations and highlights the viability of quantum technologies using small quantum systems to enhance our current classical capabilities.

METHODS

$\mathcal{G}_k$ gate-OTPs

The presented protocol for $\mathcal{G}_1$ gates may be implemented as a subroutine to realize all possible $\mathcal{G}_k$ gate-OTPs with information-theoretic security in a similar fashion to the protocol of,[8] where subscripts 1 and k stand for gates with 1 and k inputs, respectively. All binary inputs to gates are mapped to anti-commuting measurement set $\{M_i\}$, such that each measurement is composed of separable qubit measurements. Specifically

$$M_i = \bigotimes_{j=1}^{2^k-1} \sigma_{ij} \ \forall\, i \tag{5}$$

where $\sigma_{ij} \in \{\sigma_X, \sigma_Z\}$. Thus all measurements are single qubit operations in one of two bases. Each gate-OTP may be written as

$$\rho_G = \frac{1}{Tr(\mathbb{I})}\left(\mathbb{I} + \frac{1}{\sqrt{2^k}}\sum_{i=1}^{2^k}(-1)^{G(i)}M_i\right) \tag{6}$$

$$= \sum_i \frac{1}{2^k}\rho_i \tag{7}$$

$$= \sum_i \frac{1}{2^k}\left(\bigotimes_{j=1}^{2^k-1}\tilde{G}_{ij}\right) \tag{8}$$

where ρ_i is a pure state formed from a tensor product of single qubit states $\tilde{G}_{ij}$. Remarkably, each $\tilde{G}_{ij}$ is a $\mathcal{G}_1$ gate-OTP[8] and via randomly selecting from the set of possible pure states, the state received by the client is equivalent to the mixed state ρ_G under all measurements. It is thus possible to implement a $\mathcal{G}_k$ gate-OTP using only $\mathcal{G}_1$ states. The probability of correctness P_k of such noisy logic gates is for all inputs

$$P_k = \frac{1}{2^{(1+k/2)}} + \frac{1}{2}. \tag{9}$$

The shared table records random implementations of $\mathcal{G}_1$ gates with measurements in both the σ_X and σ_Z basis. The protocol presented in the main text allows secure evaluation of the measurement of such states, and thus repeated applications may be used to construct measurement outcomes of $\mathcal{G}_k$ gate-OTPs. The evaluation of all such gates-OTPs may be performed concurrently as the corresponding measurements are separable. We therefore expect the implementation of any $\mathcal{G}_k$ gate-OTP to be completed within an average of $\log_2(2^k - 1)$ rounds of classical communication. A dishonest client, who has not made measurements and instead retained states in a quantum memory, will be in possession of exactly the quantum state intended and described by Eq. (6), the security of which has been previously shown.[8] Thus, the delaying of measurements does not allow Bob to obtain additional information regarding the one-time program.

Experimental details

A 515 nm cw-laser (Roithner RLTMGL-515-500-2) with a spectral bandwidth of 0.057 nm and a power of 40 mW is used to pump a 30mm periodically-poled KTP ($KTiOPO_4$) crystal with a poling period of 33.53 µm. This is phase-matched for two SPDC processes, one emitting $|H\rangle_s|V\rangle_l$ as well as $|V\rangle_s|H\rangle_l$ with $\lambda_s = 785$ nm and $\lambda_l = 1498$ nm. The two down-conversion processes have a different spectral width, thus we use a narrow bandwidth filter (0.45 nm) for the photons in the long-wavelength arm. It turns out that it is not necessary to filter the photons in the short-wavelength arm as only photons in the desired wavelength interval will cause coincidences. We found a coincidence rate between Alice and Bob of 10 kHz using a coincidence time window of 6ns. Transmission losses between Alice's and Bob's laboratory were measured to be $13 \pm 2\%$. Using the measured double clicks at one side as well as the detector efficiency and transmission losses we can estimate the percentage of times where more than one photon was emitted finding a value of 0.097%. Assuming Bob could use all of these events to improve his probability of success when cheating (i.e., for this percentage of events he has the honest probability of success even when signing two lines) this raises his overall probability of success for a

signature run from 0.107% to 0.112%. For further details see the Supplementary Information.

DATA AVAILABILITY

The datasets generated and analyzed during the current study are available from the corresponding authors upon reasonable request.

Received: 29 July 2020; Accepted: 19 May 2021;
Published online: 15 June 2021

REFERENCES

1. Broadbent, A., Fitzsimons, J. & Kashefi, E. Universal blind quantum computation. In *Proceedings of 50th Annual IEEE Symposium on Foundations of Computer Science, FOCS'09*. 517–526 (2009).
2. Dunjko, V., Fitzsimons, J. F., Portmann, C. & Renner, R. Composable security of delegated quantum computation. *Adv. Cryptol.—ASIACRYPT 2014* **8874**, 406–425 (2014).
3. Morimae, T. & Fujii, K. Blind quantum computation protocol in which alice only makes measurements. *Phys. Rev. A* **87**, 050301 (2013).
4. Barz, S. et al. Demonstration of blind quantum computing. *Science* **335**, 303–308 (2012).
5. Greganti, C., Roehsner, M.-C., Barz, S., Morimae, T. & Walther, P. Demonstration of measurement-only blind quantum computing. *New J. Phys.* **18**, 013020 (2016).
6. Bennett, C. H. & Brassard, G. Quantum cryptography: public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and signal processing*, vol. 175 (1984).
7. Ekert, A. K. Quantum cryptography based on bell's theorem. *Phys. Rev. Lett.* **67**, 661–663 (1991).
8. Roehsner, M.-C., Kettlewell, J. A., Batalhão, T. B., Fitzsimons, J. F. & Walther, P. Quantum advantage for probabilistic onetime programs. *Nat. Commun.* **9**, 1–8 (2018).
9. Broadbent, A., Gutoski, G. & Stebila, D. Quantum one-time programs. In *Proceedings of Advances in Cryptology—CRYPTO 2013. Part II* 344–360 (2013).
10. Goldwasser, S., Kalai, Y. T. & Rothblum, G. N. One-time programs. In *Proceedings of Advances in Cryptology—CRYPTO 2008*. 39–56 (2008).
11. Liu, Y.-K. Single-shot security for one-time memories in the isolated qubits model. In *Proceedings of Advances in Cryptology—CRYPTO 2014*. 19–36 (2014).
12. Nielsen, M. & Chuang, I. L. *Quantum Computation and Quantum Information*. (Cambridge University Press, New York, 2011).
13. Lo, H.-K. Insecurity of quantum secure computations. *Phys. Rev. A* **56**, 1154–1162 (1997).
14. Beaver, D. Precomputing oblivious transfer. In *Proceedings of Advances in Cryptology—CRYPTO'95*. 97–109 (1995).
15. Kilian, J. Founding crytpography on oblivious transfer. In *Proceedings of the Twentieth Annual ACM Symposium on Theory of Computing*, STOC'88, 20–31 (ACM, 1988).
16. Ishai, Y., Prabhakaran, M. & Sahai, A. Founding cryptography on oblivious transfer—efficiently. In *Proceedings ofAdvances in Cryptology—CRYPTO 2008*. 572–591 (2008).
17. Bendlin, R., Damgøard, I., Orlandi, C. & Zakarias, S. Semihomomorphic encryption and multiparty computation. In Paterson, K. G. (ed.) *Advances in Cryptology—EUROCRYPT 2011*, 169–188 (Springer Berlin Heidelberg, 2011).
18. Yao, A. C.-C. How to generate and exchange secrets. In *Proceedings of the 27th Annual Symposium on Foundations of Computer Science*, SFCS'86, 162–167 (IEEE Computer Society, 1986).
19. Impagliazzo, R. & Rudich, S. Limits on the provable consequences of one-way permutations. In *Proceedings of the Twenty-first Annual ACM Symposium on Theory of Computing*, STOC'89, 44–61 (ACM, 1989).
20. Laudenbach, F., Kalista, S., Hentschel, M., Walther, P. & Hübel, H. A novel single-crystal & single-pass source for polarisationand colour-entangled photon pairs. *Sci. Rep.* **7**, 7235 (2017).
21. Guan, J.-Y. et al. Experimental preparation and verification of quantum money. *Phys. Rev. A* **97**, 032338 (2018).
22. Bozzio, M. et al. Experimental investigation of practical unforgeable quantum money. *npj Quantum Inform.* **4**, 1–8 (2018).
23. Erven, C. et al. An experimental implementation of oblivious transfer in the noisy storage model. *Nat. Commun.* **5**, 1–11 (2014).

ACKNOWLEDGEMENTS

We thank Robert Peterson, Teodor Strömberg, Joshua A. Slater, Fabian Laudenbach, Stefan Zeppetzauer and Maxime Jacquet for discussions and Irati Alonso Calafell and Lee Rozema operating the superconducting detector units. M.-C.R. acknowledges support from the the uni:docs fellowship program of the University of Vienna. P.W. acknowledges support from the research platform TURIS, the Austrian Science Fund (FWF) through BeyondC (F7113-N38) and NaMuG (P30067-N36), through the European Commission via UNIQORN (no. 820474) and HiPhoP (no. 731473), the United States Air Force Office of Scientific Research via QAT4SECOMP (FA2386-17-1-4011) and Red Bull GmbH. J.A.K. and J.F.F. acknowledge support from the Singapore National Research Foundation under NRF Award No. NRF-NRFF2013-01.

AUTHOR CONTRIBUTIONS

M.-C.R. and P.W. designed the experiments. M.-C.R. built and performed the experiments and analyzed data. J.A.K. and J.F.F. developed the underlying theory including the security analysis. All authors contributed to writing the manuscript. The project was supervised by J.F.F. and P.W.

COMPETING INTERESTS

The authors declare no competing interests.

ADDITIONAL INFORMATION

Supplementary information The online version contains supplementary material available at https://doi.org/10.1038/s41534-021-00435-w.

Correspondence and requests for materials should be addressed to M.-C.R. or P.W.

Reprints and permission information is available at http://www.nature.com/reprints

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.