PNAS RESEARCH ARTICLE | PHYSICS OPEN ACCESS

Device-independent quantum randomness–enhanced zero-knowledge proof

Cheng-Long Li[a,b,c,1,2], Kai-Yi Zhang[d,1], Xingjian Zhang[e], Kui-Xing Yang[f], Yu Han[e,g], Su-Yi Cheng[a,b,c], Hongrui Cui[d], Wen-Zhao Liu[a,b,c], Ming-Han Li[a,b,c], Yang Liu[h], Bing Bai[a,b,c], Hai-Hao Dong[a,b,c], Jun Zhang[a,b,c], Xiongfeng Ma[c,e], Yu Yu[c,d], Jingyun Fan[c,f], Qiang Zhang[a,b,c,h], and Jian-Wei Pan[a,b,c]

Edited by Gilles Brassard, Universite de Montreal, Montreal, Canada; received March 29, 2022; accepted September 18, 2023

Zero-knowledge proof (ZKP) is a fundamental cryptographic primitive that allows a prover to convince a verifier of the validity of a statement without leaking any further information. As an efficient variant of ZKP, noninteractive zero-knowledge proof (NIZKP) adopting the Fiat–Shamir heuristic is essential to a wide spectrum of applications, such as federated learning, blockchain, and social networks. However, the heuristic is typically built upon the random oracle model that makes ideal assumptions about hash functions, which does not hold in reality and thus undermines the security of the protocol. Here, we present a quantum solution to the problem. Instead of resorting to a random oracle model, we implement a quantum randomness service. This service generates random numbers certified by the loophole-free Bell test and delivers them with postquantum cryptography (PQC) authentication. By employing this service, we conceive and implement NIZKP of the three-coloring problem. By bridging together three prominent research themes, quantum nonlocality, PQC, and ZKP, we anticipate this work to inspire more innovative applications that combine quantum information science and the cryptography field.

device-independent quantum cryptography | Bell nonlocality | zero-knowledge proof | postquantum cryptography

From bank loans to adding friends on social networks, while sharing our personal data to validate ourselves, we might raise the following question: Is it really necessary to share so much information? To unveil nothing more than what is exactly required by the tasks, we can use zero-knowledge proof (ZKP) (1, 2). In the original format of ZKP, a prover needs to interact with a verifier for many rounds of challenges. Unfortunately, in multiparty applications, such a one-to-one highly interactive protocol becomes impractical or even unrealizable. In comparison, noninteractive zero-knowledge proof (NIZKP) sends a one-round message to convince multiple verifiers; hence, it is favorable in real-life applications.

NIZKP typically relies on the Fiat–Shamir heuristic that is instantiated in the random oracle model. Bellare and Rogaway (3) introduced the random oracle methodology, which is shown to be useful for obtaining efficient designs of cryptosystems. A random oracle is a (virtual black-box realization of a) random function that responds to every distinct query with a (truly) random response. Hence, a random oracle cannot be efficiently implemented by requiring an unrealistic amount of randomness. But a random oracle requires an unrealistic amount of randomness and thus cannot be efficiently implemented. In practice, such a fully randomized object is typically instantiated by a deterministic cryptographic hash function. However, outputs of cryptographic hash functions, such as SHA2 and SHA3 (4, 5), are used as cryptographic random numbers in the random oracle model with known inputs. Although the hash functions based on high computational complexity make the pseudorandom numbers practically hard to guess, the hashing process is essentially deterministic and no intrinsic randomness can be produced from a deterministic function. This raises controversy over the security of the practically realized cryptosystems model. For example, Canetti et al. (6) showed that "there exist signature and encryption schemes that are secure in the random oracle model, but for which any implementation of the random oracle results in insecure schemes." Besides, the belief in computational complexity is challenged by emerging quantum computing technology, which promises unprecedented computing power (7, 8). Therefore, designing cryptosystems that do not depend on the random oracle heuristic is not only of theoretical value but also of security significance.

Here, we show that quantum physics provides a solution to the problem—we construct an NIZKP protocol inspired by the principle of quantum nonlocality (9). Specifically, in this work, we report on the construction of a randomness service consisting of a quantum randomness beacon and a timestamp server. The randomness beacon

Significance

The noninteractive zero-knowledge proof (NIZKP) is underlying a broad spectrum of applications. The major categories of NIZKP are instantiated with deterministic hash functions in the real world. However, the outputs of deterministic hash functions are modeled as truly random. Thus, this unrealizable assumption potentially undermines the security of the protocol. In this work, we bring quantumness to the table: We remove the assumption in NIZKP by implementing a quantum randomness service. We demonstrate the service in a proof-of-principle experiment, which publicly broadcasts random numbers based on quantum nonlocality and signed by postquantum cryptography (PQC). By bridging together quantum nonlocality, PQC, and Zero-knowledge proof, we anticipate this work to inspire more innovative applications that combine quantum information and cryptography.

The authors declare no competing interest.

This article is a PNAS Direct Submission.

[1] C.-L.L. and K.-Y.Z. contributed equally to this work.

[2] To whom correspondence may be addressed. Email: lcl123@mail.ustc.edu.cn.

This article contains supporting information online at https://www.pnas.org/lookup/suppl/doi:10.1073/pnas.2205463120/-/DCSupplemental.

Published November 2, 2023.

generates random numbers from loophole-free Bell tests (10–14), namely device-independently, and broadcasts them to the public with postquantum-cryptography (PQC)-based algorithms. As an entropy source, the device-independent quantum random number generation (DIQRNG) does not require any prior characterization of quantum devices to guarantee security (15–19). For the delivery of random numbers, we apply a hash-based signature algorithm that is secure against known quantum algorithms and independent of all random oracles. We also provide a timestamp server, which signs the digital messages on requirement with PQC-based algorithms (20). The combination of DIQRNG and PQC signature algorithms brings a high level of security to this public randomness service. With the aid of this service, we conceive and experimentally demonstrate a secure NIZKP of the NP-complete three-coloring problem (21) without resorting to the random oracle model. In the following, we first present our protocol, then introduce its experimental realization, central to which is the preparation of a quantum randomness service, and finally analyze the security of the whole protocol.

Results

Graph coloring is a problem famously believed to be computationally intractable. Formally, a graph, $G(V, E)$, with vertices V connected by edges E is three-colorable if there exists a mapping, $\phi : V \to \{1, 2, 3\}$, such that every two adjacent vertices connected by an edge have different colors, i.e., $\forall(u, v) \in E, \phi(u) \neq \phi(v)$. Three-coloring is NP-complete (22). That is, each NP problem instance corresponds to an instantiation of a particular three-colorable graph; hence, a secure and efficient protocol to prove the three-colorability is of fundamental interest. In our NIZKP of the three-coloring problem, the prover can convince the verifier that he has a solution to the problem without revealing the specific coloring assignments.

NIZKP Protocol for Three-Coloring. Our protocol for the three-coloring problem is compiled from the basic sigma protocol for the classic three-coloring protocol (1). Different from the standard NIZKP protocol, apart from the prover and the verifier, we introduce a third element, a randomness service, as shown in Fig. 1. With the aid of the service, the prover and the verifier maintain the capability to generate a noninteractive proof directly, while they no longer need to resort to the random oracle assumption. The randomness service is essentially composed of a randomness beacon (23) and a timestamp server. The randomness service must be secure and the prover needs to show that the challenge from the beacon is generated after the commitment is published. With a trusted timestamp server, the commitment can be certified at the time of the event.

Initially, the timestamp server and the beacon each generate a pair of a public key and a secret key with PQC denoted by (pk_{ts}, sk_{ts}) and (pk_{bc}, sk_{bc}), respectively, keep the secret key and share the public key with all participants. Then, we execute the following protocol:

1. The prover prepares an assignment of coloring denoted by ϕ. The prover repeats this step κ times: For the i-th time, it chooses a permutation $\pi_i \overset{\$}{\leftarrow} S_3$ uniformly, commits $\pi_i(\phi(v))$ for all vertices $v \in V$ that are denoted by c_i, $c_i \leftarrow \{\mathrm{Com}(\pi_i(\phi(v)))\}$.[*] Finally, the prover sends $c = \{c_i\}$ to the timestamp server.
2. The timestamp server signs c and the received time t on signature σ_t, $\sigma_t \leftarrow \mathrm{Sign}(sk_{ts}, (t, c))$, and sends σ_t and t to the prover.
3. The beacon broadcasts random bits $r_{t'}$ with signature $\sigma_{t'}$, $\sigma_{t'} \leftarrow \mathrm{Sign}(sk_{bc}, (t', r_{t'}))$ at time t'. Note that step 2 and step 3 are executed only once.
4. The prover repeats this step κ times: For the i-th time, the prover chooses a random edge, $e_i = (j, k) \overset{\$}{\leftarrow} E$, according to $r_{t'}$, and decommits the commitments, $c_{i,j}$ and $c_{i,k}$, to obtain $d_{i,j}$, $d_{i,k}$, respectively. Let e be $\{e_i\}$ and d be $\{(d_{i,j}, d_{i,k})\}$.
5. The prover sends the final proof $(c, \sigma_t, t, t', r_{t'}, \sigma_{t'}, e, d)$ to the verifier.
6. The verifier checks whether the commitments, the random bits, and the signature are correct, the colors of the two vertices are different, and $t < t'$.

We claim that our protocol is noninteractive. Although the prover has to interact with the randomness service, the verifier is still noninteractive, i.e., the verifier can verify the statement even if the prover is offline.

Completeness of this protocol follows from inspection. For protocol soundness, if the graph is not three-colorable, then at least one edge has the same color on both vertices. Therefore, the probability that the verifier catches cheating is at least $1/|E|$ when $\kappa = 1$[†]. Since the random bits broadcast by the beacon are independent and identically distributed (24), the repetitions over κ times are independent and the probability of successfully cheating is at most $((|E| - 1)/|E|)^{\kappa}$. The zero-knowledge property follows from the hiding property of the commitment protocol.

Randomness Service. We implement the randomness-service-enhanced NIZKP protocol with the flowchart shown in Fig. 2*A*. In this proof-of-principle experiment, the randomness beacon continuously broadcasts blocks of fresh public random numbers and its generation timestamp, with each block being generated every minute. A block, called a "beacon pulse," contains 512 fresh random bits that are time-stamped, signed, and hash-chained (25). The timestamp server keeps waiting for the requirement of signing the commitment. The prover sends the proof to the verifier. Then, the verifier opens the signature and the commitment and checks whether the conditions are satisfied.

For the security of the protocol, the randomness beacon needs to satisfy a set of properties required for a high level of trust: 1) Unpredictability: The values of random bits cannot be predicted before their generation; 2) Autonomy: The source is resistant to any outside attempt to alter the distribution of random bits; 3) Consistency: A set of users can receive the same random bit-strings from the broadcast (25).

In constructing the randomness beacon, we adopt the DIQRNG as the entropy source, with its device-independent feature guaranteeing the requirement of unpredictability. We implement a Clauser–Horne–Shimony–Holt-type Bell-test experiment for randomness generation and subsequently perform a randomness extraction procedure under the security assumptions listed in Box 1. If we observe a nonlocal behavior in the fashion of a Bell inequality violation, we can certify the generation of intrinsic randomness from the Bell-test outputs without relying on a priori quantum device characterization. Then, the randomness extraction procedure removes the potential information leakage and extracts near-uniformly distributed random numbers.

[*] Following the conventions in cryptography, we use the symbol "$x \overset{\$}{\leftarrow} X$" to denote sampling an element x from the uniform distribution over an efficiently sampleable set X.

[†] We note that the cheating probability is a little better than $1/|E|$ when taking into account the cheating probability of the commitment scheme.

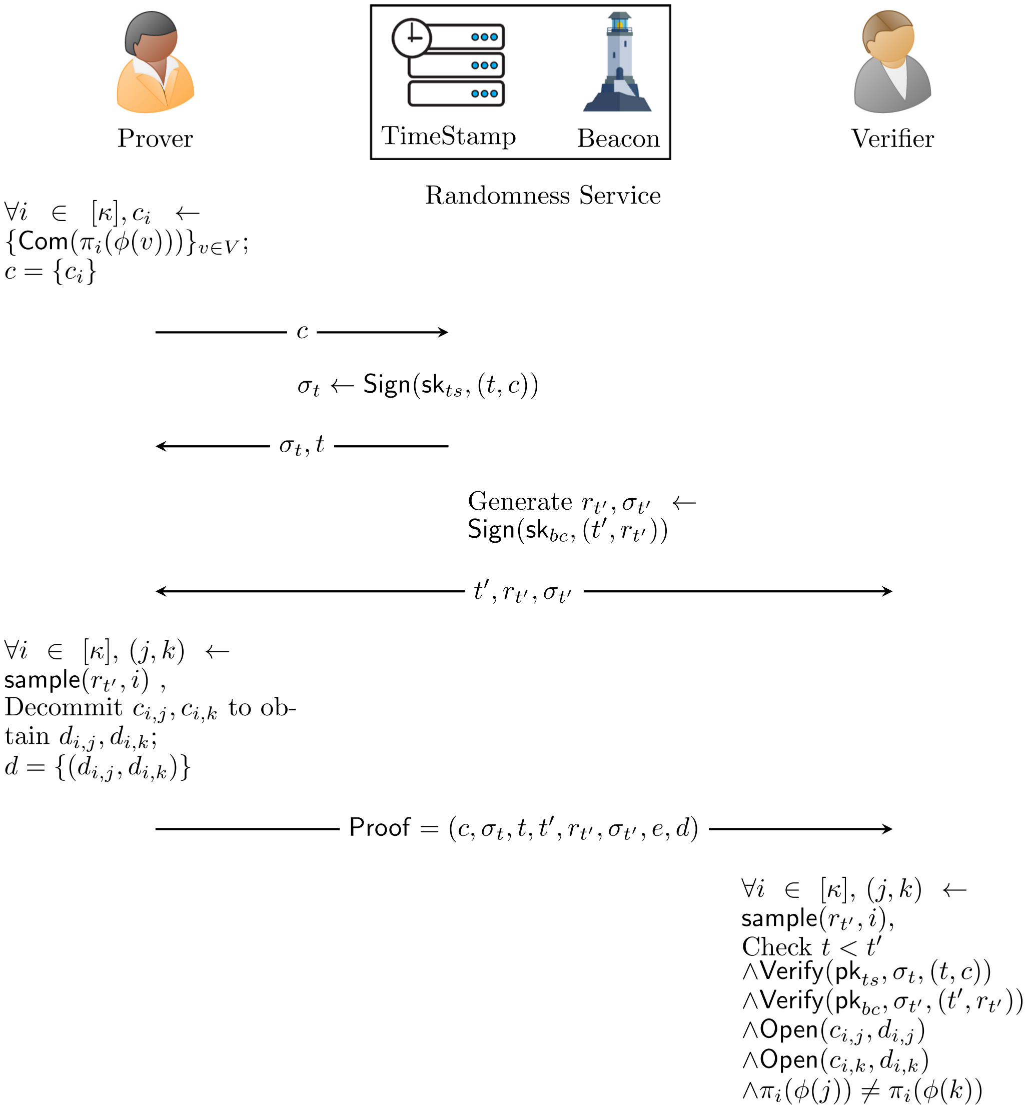
Prover
TimeStamp
Beacon
Randomness Service
Verifier
$\forall i \in [\kappa], c_i \leftarrow \{\mathsf{Com}(\pi_i(\phi(v)))\}_{v\in V}; c = \{c_i\}$
c
$\sigma_t \leftarrow \mathsf{Sign}(\mathsf{sk}_{ts}, (t, c))$
σ_t, t
Generate $r_{t'}, \sigma_{t'} \leftarrow \mathsf{Sign}(\mathsf{sk}_{bc}, (t', r_{t'}))$
$t', r_{t'}, \sigma_{t'}$
$\forall i \in [\kappa], (j, k) \leftarrow \mathsf{sample}(r_{t'}, i)$, Decommit $c_{i,j}, c_{i,k}$ to obtain $d_{i,j}, d_{i,k}$; $d = \{(d_{i,j}, d_{i,k})\}$
$\mathsf{Proof} = (c, \sigma_t, t, t', r_{t'}, \sigma_{t'}, e, d)$
$\forall i \in [\kappa], (j, k) \leftarrow \mathsf{sample}(r_{t'}, i)$, Check $t < t'$ $\wedge \mathsf{Verify}(\mathsf{pk}_{ts}, \sigma_t, (t, c))$ $\wedge \mathsf{Verify}(\mathsf{pk}_{bc}, \sigma_{t'}, (t', r_{t'}))$ $\wedge \mathsf{Open}(c_{i,j}, d_{i,j})$ $\wedge \mathsf{Open}(c_{i,k}, d_{i,k})$ $\wedge \pi_i(\phi(j)) \neq \pi_i(\phi(k))$

Fig. 1. NIZKP of three-colorability based on a randomness service. With the aid of the randomness service that is equipped with a beacon and timestamp, the prover aims to prove the knowledge of three-colorability to the verifier in the fashion of NIZKP. We depict the computation and communication steps in time order. Notations are defined as follows. sample algorithm on the inputs of randomness and index, outputs a random edge. A commitment scheme consists of two algorithms, Com and Open (*SI Appendix*, section 2). Com on the inputs of a message, outputs a commitment from a hash function, and is independent of the random oracle model in this experiment. Open on the inputs of a commitment and a decommitment, outputs false or true, corresponding to whether the commitment and the decommitment are consistent. Sign on the inputs of a secret key and a message, outputs a signature. Verify on the inputs of public keys, a signature, and a message, outputs false or true, corresponding to whether the message is signed by the owner of the public key. Proof contains all the information that is required for the verification.

Note that we need to take trusted random inputs for the Bell test. To ensure randomness, we use practical quantum random number generators based on phase fluctuations for the input settings (26). Ideally, we expect randomness expansion for a practical randomness service, where the DIQRNG produces more random bits than those consumed. However, due to the current experimental limitations, it is difficult to realize stable real-time device-independent randomness expansion that meets the requirements for a practical beacon service, where we need to finish all the procedures of DIQRNG and expand 512 bits of near-uniform random numbers in 1 min. Here, we perform two separate experiments. For the current online beacon service, we neglect the consumption of input randomness and carry out a real-time DIQRNG. For a prototype of a more practical service, we carry out a tabletop device-independent randomness expansion experiment and broadcast the random numbers in an offline manner. For both experiments, we assume secure data storage before broadcasting, while the second experiment requires a practically stronger assumption as it takes a longer time for secure storage.

In the first experiment, we establish a spacelike separation between the nonlocal parties in the Bell test to guarantee a nonsignaling condition. As shown in Fig. 2*B*, an entanglement source in Building 1 emits a pair of photons in the Einstein–Podolsky–Rosen (EPR) state and delivers one photon to Alice at a distance of 93 m to the west and another photon to Bob at a distance of 90 m to the east. The spatial separations are sufficiently large to close the locality loophole. In Fig. 2*C*, we show the time-space coordinates of the relevant events. The system achieves an 81% total efficiency for photon delivery and detection, which is sufficient to close the detection loophole (17, 19). We use the quantum probability estimation method to evaluate the

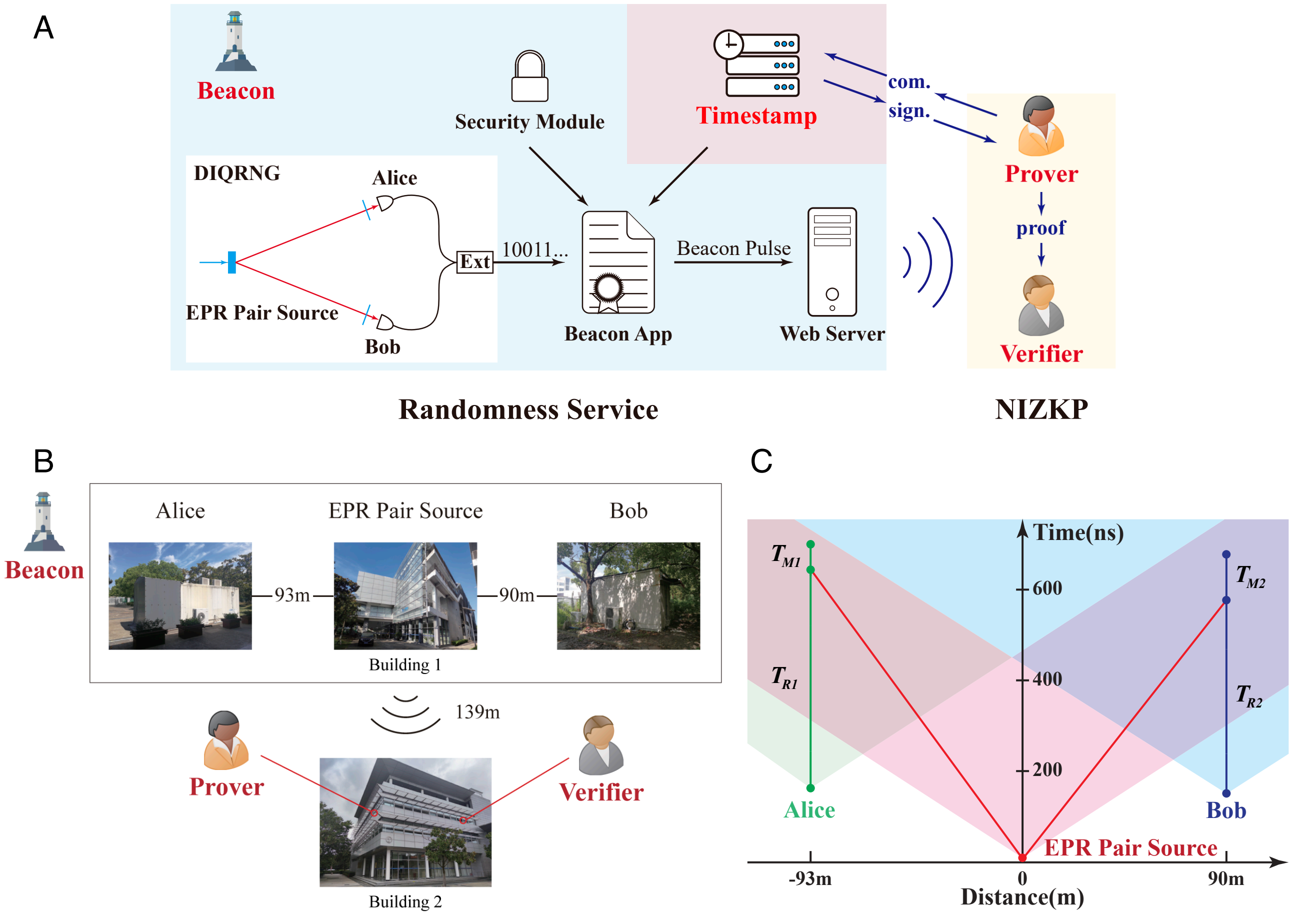

Fig. 2. Schematics of the experiment. (*A*) A flowchart demonstration of the experiment. The randomness service contains a randomness beacon and a timestamp server. The randomness beacon broadcasts random bits, and the timestamp server signs the commitment and the received time. To perform the NIZKP protocol, the prover and the verifier communicate with the beacon and the timestamp server. The timestamp server is synchronized with Coordinated Universal Time (UTC). The beacon contains a DIQRNG as the entropy source, a security module to provide the authenticity of signed beacon pulses, a beacon APP to process inputs from the DIQRNG, a timestamp from the timestamp server, and a web server to broadcast beacon pulses each minute containing 512 bits to the public. (*B*) Schematic diagram of the overall experimental setup. An EPR-pair source is located in Building 1, where pairs of entangled photons are transmitted through a fiber to the measurement stations in opposite directions with free-space distances of 93 m and 90 m, denoted as Alice and Bob, respectively. Other beacon components are located in the same lab as the EPR-pair source. The prover and the verifier are located in Building 2, 139 m from Building 1. (*C*) Spacetime diagram for the DIQRNG experimental configuration. The values $T_{R1,2}$ are the times for Pockels cells to get ready for state measurement and $T_{M1,2}$ are the times elapsed for the single-photon detectors to output an electronic signal. No signaling between relevant events is allowed in this configuration (*SI Appendix*, section 5.B.5).

amount of randomness generated in the Bell-test experiment (24) and utilize a quantum-proof strong randomness extractor (27) to extract uniformly distributed random bits. The Bell-test experiment generates 512 random bits in about 31.38 s and the randomness extraction takes approximately 1 s. The total soundness error for the DIQRNG is no larger than 2^{-64}.

To demonstrate a more practical beacon service, we perform a device-independent randomness expansion experiment on our upgraded tabletop platform (28). In this experiment, we make the shielding assumption, where we assume that the measurement device of each party is blocked from signals from the other party. The tabletop platform achieves higher detection efficiencies, reaching overall efficiencies of 87.40% for Alice and 86.31% for Bob. Consequently, this leads to a larger Bell inequality violation. We successfully achieved a randomness expansion of 5.66×10^8 bits more than the initial input randomness within approximately 38 h. Subsequently, we performed offline randomness extraction in 102 h.

To fulfill autonomy and consistency, in the authentication procedure, we apply a hash-based PQC signature algorithm (20) in the security module of the beacon to prove the identity of the randomness server. The hash-based signature algorithm is secure against all known quantum algorithms. It only relies on the collision-resistant property of the hash function rather than the random oracle model. The random numbers used to produce the public, and private keys in the hash-based PQC algorithms are derived from our previous DIQRNG experiment (19). The private key (sk_{bc}) is used to sign the message, and the public key (pk_{bc}) is broadcast to everyone. The double certification ensures the trust of the randomness beacon service.

In addition to the randomness beacon, our randomness service also provides a timestamp server that is synchronized to Coordinated Universal Time (UTC). The timestamp server applies a hash-based PQC signature algorithm to provide the public and private keys (pb_{ts}, sk_{ts}) upon request. In the implementation of our NIZKP protocol, the timestamp server authenticates the commitment of the prover in each round of the experiment.

Experimental Demonstration. In implementing the NIZKP protocol, we located the prover and the verifier in Building 2. They received the random bits broadcast by the beacon and are 139 m away from Building 1, as shown in Fig. 2*B*.

Box 1. Security Assumptions

Security assumptions in DIQRNG:

1. *Quantum mechanics:* Quantum mechanics is correct and complete.
2. *Nonsignaling:* In each round of the Bell test, the measurement process of Alice/Bob is independent of the other party.
3. *Trusted inputs:* Alice and Bob each have trusted random input settings.[‡]
4. *Secure lab:* The devices cannot communicate to the outside to leak the experimental results before broadcasting public random numbers.
5. *Trusted postprocessors:* The classical postprocessing procedures for randomness evaluation and randomness extraction are trusted.

Security assumptions in NIZKP:

1. *Hash function:* The hash function used in the scheme is collision-resistant.
2. *Semihonest third parties:* Although the beacon and the timestamp server may attempt to gather information, they do not deviate from the protocol.

[‡] In the randomness expansion experiment, Alice and Bob only need a small amount of randomness to initialize the experiment. They keep the random input settings private until successfully implementing randomness expansion.

Our protocol supports any user-specified three-coloring instance that can represent any NP-problem instance. In general, it is hard in the average case to choose an efficiently sampleable set of instances. To the best of our knowledge, there is no provable solution for three-coloring problems (i.e., a worst-case-to-average-case reduction). Therefore, we used different sample spaces. Using the method in ref. 29, we generated the graphs as follows: 1. Randomly assign colors to each vertex; 2. for each pair $u, v \in V$ such that $\phi(u) \neq \phi(v)$, add this edge with probability p. Note that the generated graphs are not hard if p is either too high or too low (30), but the concrete range is difficult to analyze. Thus, we decided to demonstrate our experiments across multiple parameters. The number of vertices n was selected from 40 to 60. The probability p was selected from 0.1 to 0.9. For each graph, the repeated number of rounds κ was determined to reach a soundness error of 2^{-64} for ZKP (same with DIQRNG), and the experiment was finished in less than 37 s. With increasing numbers of runs, we also demonstrated that a widely accepted soundness error of 2^{-128} for ZKP can be reached in less than 54 s. The number of consumed random bits is $\kappa \log_2 |E|$. As the requirement of the standard format of the randomness beacon (31), 512 random bits were broadcast every minute. In Table 1, we list the experimental settings and the respective consumption of resources, including the runtimes of the commitment phase, the response phase, the verification phase, and the proof size, with the environment of both the prover and the verifier in OS Win10, CPU i7-9750H CPU @ 2.60 GHz, RAM 16.0 GB.

Security

In this task, which brings together DIQRNG, PQC, and ZKP, we can adopt an information-theoretic security definition and cryptographic analysis for DIQRNG and PQC. However, it is not obvious to establish a clear security argument for the entire task as a whole. The security of this composition remains an open problem. Nevertheless, a practically reasonable solution is to analyze the security of our whole scheme in a hybrid model, where we regard the randomness service as an idealized primitive. Such a modular method is widely adopted in ZKPs (32). Following this convention, we present the following theorem.

Table 1. Results of our noninteractive zero-knowledge proof

$\|V\|$	$\|E\|$	p	Commitment time/s	Response time/s	Verification time/s	Proof size/MB	Sec.	# of rounds κ
55	89	0.1	3.36	0.20	0.39	14.80	64	3,925
49	152	0.2	6.02	0.20	0.56	22.57	64	6,720
58	333	0.3	17.1	0.37	1.34	58.66	64	14,750
42	213	0.4	7.93	0.26	0.73	27.14	64	9,426
51	411	0.5	17.6	0.44	1.54	63.68	64	18,210
52	514	0.6	25.6	0.54	1.94	81.22	64	22,779
43	420	0.7	16.0	0.44	1.42	54.86	64	18,609
54	775	0.8	33.0	0.78	2.96	127.2	64	34,357
44	570	0.9	20.2	0.58	1.93	76.22	64	25,263
51	78	0.1	6.87	0.21	0.59	24.04	128	6,875
48	145	0.2	10.3	0.33	1.04	42.19	128	12,820
54	285	0.3	25.9	0.60	2.19	93.46	128	25,241
47	279	0.4	20.5	0.56	1.96	79.63	128	24,709
52	425	0.5	33.8	0.84	3.16	134.2	128	18,210
50	481	0.6	37.9	0.93	3.46	146.1	128	42,631
45	469	0.7	31.7	0.96	3.32	128.2	128	41,566
49	635	0.8	47.7	1.25	4.63	189.1	128	56,294
43	543	0.9	37.6	1.05	3.62	141.9	128	48,132

The commitment time is the time consumption of the prover in step 1. The response time is the time consumption of the prover in steps 2, 3, 4, and 5. The verification time is the time consumption of the verifier in step 6. Note that we count only the local computation time, except the communication time. The proof size is the disk and communication consumption of the proof in step 5. sec. is the negative base two logarithms of the soundness error. The number of rounds is the number of parallel repetitions. The consumption of random services is fairly small; thus, we omit it here.

Box 2. Randomness Service Functionality

Initialization. The prover and verifier set their identity as id_P and id_V, respectively.

Commitment. On receiving $(\mathrm{commit}, \mathrm{id}, c)$, the functionality generates randomness r and then sends (id_P, c, r) to the prover and (id_V, c, r) to the verifier.

Theorem 1. *Under the security assumptions listed in Box 1, the protocol in Fig. 1 is a zero-knowledge proof in the randomness service hybrid model.*

Proof: **Completeness.** Given an honest implementation, the randomness service does not abort with high probability (*SI Appendix*, section 4). Based on a successful implementation of the randomness service, the prover would convince the verifier if the prover has a proper three-coloring.

Zero Knowledge. We adopt a hybrid model to describe the functionality of the randomness service, as shown in Box 2. Then, the zero-knowledge property can be proven by replacing the second interactive phase according to ref. 1.

Soundness. The overall soundness error of our protocol is the sum of 2^{-64} (randomness generation), 2^{-100} (randomness extraction), and 2^{-64} (ZKP). The soundness of ZKP has been stated above. (*SI Appendix*, section 5.A.3). □

Discussion

We propose an NIZKP protocol with the aid of a public randomness service, which removes the random oracle model. As a demonstration, we implement the protocol for the three-coloring problem. To implement the protocol, we construct a randomness beacon—the heart of our randomness service—utilizing a loophole-free DIQRNG and PQC signature algorithms. The framework of our randomness beacon forms a strong trust chain. Basic trust originates from the correctness of quantum mechanics, which guarantees the intrinsic unpredictability of random numbers. For the delivery of random numbers, thanks to the use of PQC authentication algorithms, the users can trust their access. The timestamps and the signatures can be used by legitimate users to confirm the broadcast random numbers. In the future, the trust chain can be further boosted. By combining various randomness beacon services owned by separate administrative identities and even more countries in a quantum network, the users can bypass the problem of one or a few malicious beacon services. Starting from the fundamental discussion on local realism and quantum nonlocality by Einstein et al. (33), continuous experimental and theoretical developments have innovated the most secure information-technology applications thus far, namely, the device-independent quantum cryptography. We anticipate there will be more device-independent quantum information processing applications.

Materials and Methods

Supporting Details. In *SI Appendix*, we present the details of ZKP for the three-coloring problem, commitment scheme from hash function, PQC signature algorithm, randomness service, and DIQRNG. In *SI Appendix*, section 1, we describe the details of zero-knowledge proof for the three-coloring problem and the Fiat–Shamir transformation. In *SI Appendix*, section 2, we construct a commitment scheme from a cryptographic hash function. In *SI Appendix*, section 3, we briefly introduce our hash-based PQC digital signature algorithm. In *SI Appendix*, section 4, we show the details of our randomness service. In *SI Appendix*, section 5, we introduce the details of the theory and experiment of our DIQRNG.

Data, Materials, and Software Availability. All study data are included in the article and/or *SI Appendix*. The code for the zero-knowledge proof, post-quantum cryptography and timestamp server has been deposited on GitHub (https://github.com/kzoacn/beacon) (34). The randomness beacon can be accessed on the website (https://randomnessbeacon.com) (35).

ACKNOWLEDGMENTS. This work was supported by the National Key Research and Development (R&D) Plan of China (2020YFA0309704), the National Natural Science Foundation of China (T2125010), the Chinese Academy of Sciences, the Anhui Initiative in Quantum Information Technologies, Shanghai Municipal Science and Technology Major Project (2019SHZDZX01), Innovation Program for Quantum Science and Technology (2021ZD0300804), the Taishan Scholar Program of Shandong Province, and the New Cornerstone Science Foundation through the XPLORER PRIZE.

Author affiliations: [a]Hefei National Research Center for Physical Sciences at the Microscale and School of Physical Sciences, University of Science and Technology of China, Hefei 230026, People's Republic of China; [b]CAS Center for Excellence in Quantum Information and Quantum Physics, University of Science and Technology of China, Shanghai 201315, People's Republic of China; [c]Hefei National Laboratory, University of Science and Technology of China, Hefei 230088, People's Republic of China; [d]Department of Computer Science, Shanghai Jiao Tong University, Shanghai 200240, People's Republic of China; [e]Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing 100084, People's Republic of China; [f]Department of Physics and Shenzhen Institute for Quantum Science and Engineering, Southern University of Science and Technology, Shenzhen 518055, People's Republic of China; [g]State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450001, People's Republic of China; and [h]Jinan Institute of Quantum Technology, Jinan 250101, People's Republic of China

Author contributions: X.M., Y.Y., J.F., Q.Z., and J.-W.P. designed research; C.-L.L., S.-Y.C., W.-Z.L., M.-H.L., Y.L., B.B., H.-H.D., J.Z., J.F., Q.Z., and J.-W.P. performed the experiment of DIQRNG; K.-Y.Z., H.C., and Y.Y. designed the algorithms of PQC and ZKP; K.-X.Y. and Y.H. established the randomness beacon service; and K.-Y.Z., X.Z., H.C., and M.X. analyzed the security of the protocol, all authors contributed to analyze data and write the paper.

1. S. Goldwasser, S. Micali, C. Rackoff, The knowledge complexity of interactive proof systems. *SIAM J. Comput.* **18**, 186–208 (1989).
2. G. Kappos, H. Yousaf, M. Maller, S. Meiklejohn, "An empirical analysis of anonymity in Zcash" in *27th USENIX Security Symposium (USENIX Security 18)*, W. Enck, A. P. Felt, Eds. (USENIX Association, Baltimore, MD, 2018), pp. 463–477.
3. M. Bellare, P. Rogaway, "Random oracles are practical: A paradigm for designing efficient protocols" in *Proceedings of the 1st ACM Conference on Computer and Communications Security*, D. E. Denning, R. Pyle, R. Ganesan, R. S. Sandhu, V. Ashby, Eds. (ACM Press, Fairfax, VA, 1993), pp. 62–73.
4. Fips Pub. Secure hash standard (shs). Fips pub, 180 (2012).
5. M. Dworkin, "Sha-3 standard: Permutation-based hash and extendable-output functions" (Tech. Rep. Federal Inf. Process. Stds. NIST FIPS-202, 2015-08-04, 2015).
6. R. Canetti, O. Goldreich, S. Halevi, The random oracle methodology, revisited. *J. ACM* **51**, 557–594 (2004).
7. F. Arute *et al.*, Quantum supremacy using a programmable superconducting processor. *Nature* **574**, 505–510 (2019).
8. H.-S. Zhong *et al.*, Quantum computational advantage using photons. *Science* **370**, 1460–1463 (2020).
9. J. S. Bell, On the Einstein Podolsky Rosen paradox. *Physics Physique Fizika* **1**, 195–200 (1964).
10. B. Hensen *et al.*, Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. *Nature* **526**, 682 (2015).
11. L. K. Shalm *et al.*, Strong loophole-free test of local realism. *Phys. Rev. Lett.* **115**, 250402 (2015).
12. M. Giustina *et al.*, Significant-loophole-free test of Bell's theorem with entangled photons. *Phys. Rev. Lett.* **115**, 250401 (2015).
13. W. Rosenfeld *et al.*, Event-ready Bell test using entangled atoms simultaneously closing detection and locality loopholes. *Phys. Rev. Lett.* **119**, 010402 (2017).
14. M.-H. Li *et al.*, Test of local realism into the past without detection and locality loopholes. *Phys. Rev. Lett.* **121**, 080404 (2018).
15. S. Pironio *et al.*, Random numbers certified by Bell's theorem. *Nature* **464**, 1021–1024 (2010).
16. P. Bierhorst *et al.*, Experimentally generated randomness certified by the impossibility of superluminal signals. *Nature* **556**, 223 (2018).

17. Y. Liu *et al*., Device-independent quantum random-number generation. *Nature* **562**, 548 (2018).
18. L. K. Shalm *et al*., Device-independent randomness expansion with entangled photons. *Nat. Phys.* **17**, 452–456 (2021).
19. M.-H. Li *et al*., Experimental realization of device-independent quantum randomness expansion. *Phys. Rev. Lett.* **126**, 050503 (2021).
20. J. Katz, Y. Lindell, *Introduction to Modern Cryptography* (CRC Press, 2020).
21. O. Goldreich, S. Micali, A. Wigderson, Proofs that yield nothing but their validity or all languages in NP have zero-knowledge proof systems. *J. ACM (JACM)* **38**, 690–728 (1991).
22. S. Arora, B. Barak, *Computational Complexity: A Modern Approach* (Cambridge University Press, 2009).
23. M. O. Rabin, Transaction protection by beacons. *J. Comput. Syst. Sci.* **27**, 256–267 (1983).
24. Y. Zhang, F. Honghao, E. Knill, Efficient randomness certification by quantum probability estimation. *Phys. Rev. Research* **2**, 013016 (2020).
25. M. J. Fischer, M. Iorga, R. Peralta, "A public randomness service" in *Proceedings of the International Conference on Security and Cryptography* (IEEE, 2011), pp. 434–438..
26. Y.-Q. Nie *et al*., The generation of 68 Gbps quantum random number by measuring laser phase fluctuations. *Rev. Sci. Instrum.* **86**, 063105 (2015).
27. X. Ma *et al*., Postprocessing for quantum random-number generators: Entropy evaluation and randomness extraction. *Phys. Rev. A* **87**, 062327 (2013).
28. W.-Z. Liu *et al*., Device-independent randomness expansion against quantum side information. *Nat. Phys.* **17**, 448–451 (2021).
29. J. S. Turner, Almost all *k*-colorable graphs are easy to color. *J. Algorithms* **9**, 63–82 (1988).
30. N. Alon, N. Kahale, A spectral technique for coloring random 3-colorable graphs. *SIAM J. Comput.* **26**, 1733–1748 (1997).
31. J. Kelsey, L. T. A. N. Brandão, R. Peralta, H. Booth, "A reference for randomness beacons: Format and protocol version 2" (Tech. Rep., National Institute of Standards and Technology, 2019).
32. Y. Ishai, E. Kushilevitz, R. Ostrovsky, A. Sahai, "Zero-knowledge from secure multiparty computation" in *Proceedings of the thirty-ninth annual ACM symposium on Theory of computing*, S. Johnson, U. Feige, Eds. (ACM Press, San Diego, CA, 2007), pp. 21–30.
33. A. Einstein, B. Podolsky, N. Rosen, Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.* **47**, 777–780 (1935).
34. C.-L. Li *et al*., Device-independent-quantum-randomness-enhanced zero-knowledge proof. GitHub. https://github.com/kzoacn/beacon. Deposited 12 October 2023.
35. Jinan Institute of Quantum Technology, Device independent quantum random number beacon service. Randomness Beacon. https://randomnessbeacon.com. Deposited 17 May 2023.