Device-independent quantum randomness–enhanced zero-knowledge proof

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

Edited by Gilles Brassard, Université de Montréal, 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)\textsuperscript{(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\textsuperscript{(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\textsuperscript{(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.\textsuperscript{(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\textsuperscript{(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\textsuperscript{(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

The authors declare no competing interest.

Copyright © 2023 the Author(s). Published by PNAS. This open access article is distributed under Creative Commons Attribution-NonCommercial-NoDerivatives License 4.0 (CC BY-NC-ND).

1 C.-L.L. and K.-Y.Z. contributed equally to this work.
2 To whom correspondence may be addressed. Email: lid123@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, \( \phi : V \rightarrow \{1,2,3\} \), 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 \( \phi \). The prover repeats this step \( k \) times: For the \( i \)-th time, it chooses a permutation \( \pi_i \leftarrow S_3 \) uniformly, commits \( \pi_i((\phi(v)) \) for all vertices \( v \in V \) that are denoted by \( c_i, c_i \leftarrow \{\text{Com}(\pi_i((\phi(v)))\}^* \). Finally, the prover sends \( e = \{c_i\} \) to the timestamp server.

2. The timestamp server signs \( c \) and the received time \( t \) on signature \( \sigma_i, \sigma_t \leftarrow \text{Sign}(sk_{ts}, (t, c)) \), and sends \( \sigma_t \) and \( t \) to the prover.

3. The beacon broadcasts random bits \( r_j \) with signature \( \sigma_j, \sigma_j \leftarrow \text{Sign}(sk_{bc}, (t', r_j)) \) at time \( t' \). Note that step 2 and step 3 are executed only once.

4. The prover repeats this step \( k \) times: For the \( i \)-th time, the prover chooses a random edge, \( e_i = (j, k) \leftarrow E \), according to \( r_i \), and decommits the commitments, \( c_{ij} \) and \( c_{jk} \), to obtain \( d_{ij}, d_{jk} \) respectively. Let \( e \) be \{\( e_i \}\) and \( d \) be \{\( d_{ij}, d_{jk} \)\}.

5. The prover sends the final proof \((e, \sigma_i, t, t', r_j, \sigma_j, c, e, d)\) 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 \( \frac{1}{|E|} \) when \( k = 1 \). Since the random bits broadcast by the beacon are independent and identically distributed (24), the repetitions over \( k \) times are independent and the probability of successfully cheating is at most \( \frac{(|E| - 1)}{|E|^x} \). 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. 2A. 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 ‘$X \xrightarrow{\$} X$’ to denote sampling an element $x$ from the uniform distribution over an efficiently sampleable set $X$.\footnote{We note that the cheating probability is a little better than $1/|E|$ when taking into account the cheating probability of the commitment scheme.}
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.

\[ \forall i \in [k], (j, k) \leftarrow \text{sample}(r_{t'}, i), \]

Decommit \( c_{1,j}, c_{1,k} \) to obtain \( d_{1,j}, d_{1,k} \);
\[ d = \{(d_{1,j}, d_{1,k})\} \]

\[ \text{Proof} = (c, \sigma_t, t', r_{t'}, \sigma_{t'}, e, d) \]

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. 2B, 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. 2C, 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
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 $5.66 \times 10^8$ 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. 2B.
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 \( k \) 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 \( k \log_2 |E| \). 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.
**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 (T1215010), the Chinese Academy of Sciences, the Anhui Initiative in Quantum Information Physics, Shanghai Municipal Science and Technology Major Project (2019SZDZX01), Innovation Program for Quantum Science and Technology (20212D0300804), the Tsinghua Student Program of Shandong Province, and the New Cornerstone Science Foundation through the XPLORER PRIZE.
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. G. 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. J. Katz, Y. Lindell, Introduction to Modern Cryptography (CRC Press, 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).