entropy

IMPACT FACTOR 2.0

Indexed in: PubMed

CITESCORE 5.2

Article

Semi-Device-Independent Randomness Expansion Using $n \to 1$ Parity-Oblivious Quantum Random Access Codes

Xunan Wang, Xu Chen, Mengke Xu, Wanglei Mi and Xiao Chen

Special Issue

Quantum Probability and Randomness V

Edited by

Prof. Dr. Andrei Khrennikov and Prof. Dr. Karl Svozil

MDPI

https://doi.org/10.3390/e27070696

entropy

MDPI

Article

Semi-Device-Independent Randomness Expansion Using $n \to 1$ Parity-Oblivious Quantum Random Access Codes

Xunan Wang [1], Xu Chen [2], Mengke Xu [1], Wanglei Mi [1] and Xiao Chen [1,*]

[1] College of Information Engineering, China Jiliang University, Hangzhou 310018, China; xunan@cjlu.edu.cn (X.W.); xmk22@cjlu.edu.cn (M.X.); 22h034160135@cjlu.edu.cn (W.M.)
[2] College of Computer Science and Technology, Nanjing University of Aeronautics and Astronautics, Nanjing 211106, China; bx2416012@nuaa.edu.cn
* Correspondence: 230208705@seu.edu.cn

Abstract

Quantum mechanics enables the generation of genuine randomness through its intrinsic indeterminacy. In device-independent (DI) and semi-device-independent (SDI) frameworks, randomness generation protocols can further ensure that the output remains secure and unaffected by internal device imperfections, with certification grounded in violations of generalized Bell inequalities. In this work, we propose an SDI randomness expansion protocol using $n \to 1$ parity-oblivious quantum random access code (PO-QRAC), where the presence of true quantum randomness is certified through the violation of a two-dimensional quantum witness. For various values of n, we derive the corresponding maximal expected success probabilities. Notably, for $n = 4$, the expected success probability obtained under our protocol exceeds the upper bound reported in prior work. Furthermore, we establish an analytic relationship between the certifiable min-entropy and the quantum witness value, and demonstrate that, for a fixed witness value, PO-QRAC–based protocols certify more randomness than those based on standard QRACs. Among all configurations satisfying the parity-obliviousness constraint, the protocol based on the $3 \to 1$ PO-QRAC achieves optimal randomness expansion performance.

Keywords: Bell inequality; randomness expansion; parity-obliviousness; min-entropy

Academic Editors: Andrei Khrennikov and Karl Svozil

Received: 23 May 2025
Revised: 26 June 2025
Accepted: 26 June 2025
Published: 28 June 2025

Citation: Wang, X.; Chen, X.; Xu, M.; Mi, W.; Chen, X. Semi-Device-Independent Randomness Expansion Using $n \to 1$ Parity-Oblivious Quantum Random Access Codes. *Entropy* **2025**, *27*, 696. https://doi.org/10.3390/e27070696

1. Introduction

Random numbers serve as indispensable resources in various technological domains, including cryptography, secure computation, and quantum protocols [1]. In classical cryptographic frameworks, foundational protocols such as the Data Encryption Standard (DES) and Rivest–Shamir–Adleman (RSA) cryptosystems require random bit generation for cryptographic key establishment. In quantum cryptography, the BB84 quantum key distribution protocol relies critically on perfect random bits for secure basis selection and state encoding [2]. However, conventional random number generators (RNGs) produce only pseudorandom sequences whose security fundamentally relies on trust assumptions regarding device integrity [3]. Quantum mechanics provides a solution through its inherent non-determinism, enabling provably unpredictable randomness generation [4]. Consequently, device-independent (DI) and semi-device-independent (SDI) quantum RNGs have emerged as transformative paradigms in quantum information science [5–8].

The DI framework, formally established by Ac'in and Colbeck [9,10], guarantees security based solely on observed measurement statistics (e.g., Bell inequality violations)

without device characterization. In contrast, SDI protocols relax these requirements by assuming prior knowledge of the system dimension while remaining agnostic to other device specifications [11]. Notably, the dimensionality of quantum systems can be experimentally determined through quantum dimension witnessing protocols [12,13]. This hierarchy of trust assumptions enables flexible implementations balancing security and practicality for next-generation randomness expansion protocols. Randomness expansion is a protocol that utilizes a small amount of initial randomness to generate a larger sequence of certified random numbers. In recent years, significant progress has been made in both DI and SDI frameworks. In the DI framework, pioneering work includes Colbeck's genuine randomness expansion protocols based on GHZ tests for different randomness sources [14,15], and Pironio et al.'s protocol utilizing Bell inequality violations for randomness certification [16]. Coudron et al. presented a method achieving unbounded randomness expansion [17]. The development of SDI protocols has opened new research directions. Li et al. first proposed quantum random access code (QRAC)-based randomness expansion protocols in the SDI framework, rigorously proving that perfect random seeds can generate fresh randomness [18,19]. Zhou et al. subsequently extended this work by investigating protocols with partially free randomness sources under the SDI framework [20–23].

QRAC is a crucial tool in studying SDI quantum randomness expansion protocols. The study of QRACs in higher-dimensional Hilbert spaces and sequential QRACs have propelled the development of multi-party quantum randomness expansion protocols [24–29]. As a specialized variant of QRAC, parity-oblivious QRAC (PO-QRAC) introduces a critical constraint: the encoded quantum states must conceal parity information of the input classical bits, thereby addressing vulnerabilities in conventional QRACs that inadvertently leak global properties such as parity checks [30]. In a conventional $n \to 1$ RAC, Alice can effectively leak one of her input bits in clear form by embedding it directly into the transmitted state, allowing Bob to recover that bit with certainty. To eliminate this trivial information pathway, the parity-oblivious constraint demands that no parity of Alice's input string may be learned from the communicated quantum states [31]. This requirement ensures that, regardless of Bob's measurement strategy, the transmitted system carries no information about any parity bit—thereby precluding any classical "backdoor" and sharpening the focus on genuinely nonclassical, preparation-contextual advantages [32].

In quantum randomness expansion protocols, employing PO-QRACs prevents collusion among the parties and thereby enables the extraction of greater amounts of certifiable randomness. We introduce a randomness expansion based on the $n \to 1$ PO-QRAC and, for $n = 2, 3, 4$, explicitly construct the corresponding two-dimensional quantum witnesses that certify quantum advantage. Finally, we derive an analytic relation between the quantum witness and the certifiable min-entropy, quantifying how the degree of witness violation translates into fresh randomness.

The remainder of this paper is organized as follows. In Section 2, we present the formal model of the proposed $n \to 1$ PO-QRAC protocol and define the parity-obliviousness constraint. Section 3 derives the optimal classical success probability under this model and identifies the best parity-oblivious classical codes. In Section 4, we compute the maximum expected success probability in the quantum scenario for each n and verify when a quantum witness violation occurs. Section 5 analyzes the relationship between quantum witness and the certifiable randomness in the resulting randomness-expansion protocol, comparing our PO-QRAC–based schemes against standard QRAC–based approaches. Finally, we present our conclusion in Section 6.

2. Model Description

We begin by introducing the SDI randomness expansion model. The SDI framework requires that the quantum system be entanglement-free and imposes no assumptions on any parameters beyond the Hilbert space dimensionality. Our model is based on the $n\to1$ QRAC in a two-dimensional Hilbert space C^2, which comprises two black-boxes: the preparation party (Alice) and the measurement party (Bob). As shown in Figure 1, Alice randomly selects a bit string $x = \{x_1, x_2, \ldots, x_n\} \in \{0,1\}^n$, encodes it into a quantum state ρ_x, and transmits it to Bob. Upon receiving ρ_x, Bob performs a measurement defined by the POVM measurement $\{\hat{M}_y^b\}_{b=0}^1$ where $y \in \{1, \ldots, n\}$, and subsequently outputs the measurement result $b \in \{0,1\}$.

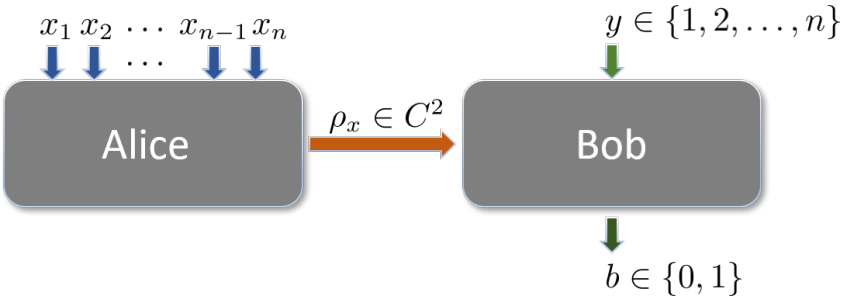

Figure 1. Semi-device-independent randomness expansion using $n\to1$ QRAC involves two parties, Alice and Bob. Alice encodes a quantum state ρ_x based on her input $x = \{x_1, x_2, \ldots, x_n\} \in \{0,1\}^n$. Bob subsequently performs a quantum measurement on ρ_x according to his input $y \in \{1, 2, \ldots, n\}$. The outcome of Bob's measurement is a single bit $b \in \{0,1\}$, which serves as the model's output. The implementation employs two protected black-box devices residing in the same secure space. The protocol operates under a semi-device-independent framework, where the internal workings of the devices are unknown, but the dimensions of the quantum systems are certified.

Through multiple repetitions of the procedure, we evaluate the expected success probability

$$E = \frac{1}{n \cdot 2^n} \sum_{x \in \{0,1\}^n} \sum_{y=1}^{n} p(b = x_y \mid x, y), \tag{1}$$

where success is defined as the event that Bob employs the y-th measurement $\{\hat{M}_y^b\}_{b=0}^1$ and obtains an outcome b matching the y-th bit of the input string x. We construct the two-dimensional quantum witness using the expected success probability.

The expected success probabilities, denoted as E_c (classical) and E_q (quantum), characterize the performance bounds in the respective scenarios. When the experimentally observed success probability $\hat{E}$ exceeds the classical upper bound $E_c^{\max}$, this provides a statistical proof of the system's ability to generate certified quantum randomness. The output sequence $\{b\}$ can then undergo quantum-proof entropy distillation to extract randomness that is information-theoretically secure. In this paper, we use the min-entropy function to quantify the randomness:

$$H_\infty(B \mid X, Y) = -\log_2[\max_{x,y,b} p(b \mid x, y)]. \tag{2}$$

We now introduce the concept of PO-QRAC in detail. The parity-obliviousness constraint enforces that Bob cannot obtain any parity information about the input bit string $x \in \{0,1\}^n$. Following reference [30], we define the parity-oblivious constraint set as

$$\mathcal{S}_n := \{\boldsymbol{S} \mid \boldsymbol{S} = \{S_1, S_2, \ldots, S_n\} \in \{0,1\}^n, \sum_i^n S_i \geqslant 2\}. \tag{3}$$

This leads to the quantum state constraint:

$$\forall \boldsymbol{S} \in \mathcal{S}_n : \quad \sum_{x\in\{0,1\}^n} (-1)^{\oplus_i S_i x_i} \rho_x = 0, \tag{4}$$

where $\bigoplus$ denotes modulo-2 summation.

3. The Maximum Expected Success Probabilities for the $n\to1$ PO-RACs

In this section, we analyze the maximum expected success probability $E_c^{\max}$ for classical $n\to1$ parity-oblivious random access codes (PO-RAC). For the classical standard $n\to1$ RAC, the optimal encoding scheme $\mathcal{E} : \{0,1\}^n \to \{0,1\}$ is given by the Hamming threshold function:

$$\mathcal{E}(x) = \begin{cases} 0, & \mathrm{wt}(x) \leqslant \lfloor n/2 \rfloor, \\ 1, & \mathrm{wt}(x) > \lfloor n/2 \rfloor, \end{cases} \tag{5}$$

where $\mathrm{wt}(x)$ denotes the Hamming weight of x. The corresponding optimal decoding scheme is characterized by the identity decoding strategy. According to [33], the maximum expected success probability for classical standard $n\to1$ RAC is given by

$$E_c^{\max} = \frac{1}{2} + \frac{1}{2^n} \begin{pmatrix} n-1 \\ \lfloor (n-1)/2 \rfloor \end{pmatrix}. \tag{6}$$

The incorporation of the parity-obliviousness constraint necessitates modifications to the optimal encoding scheme for standard $n\to1$ RAC. For $n = 2$, the parity-oblivious set is defined as $\mathcal{S}_2 = \{11\}$. This imposes the following linear constraint on the encoding function: $\mathcal{E}(00) + \mathcal{E}(11) = \mathcal{E}(01) + \mathcal{E}(10)$. A valid resolution satisfying this constraint is $\mathcal{E}(00) = \mathcal{E}(01) = 0$, $\mathcal{E}(10) = \mathcal{E}(11) = 1$. Remarkably, this constrained encoding preserves the maximum expected success probability $E_c^{\max} = 3/4$, identical to the standard $2\to1$ RAC.

For $n > 2$, the parity-obliviousness constraint alters the maximum expected success probability of RACs compared to their standard counterparts.

In the case of $n = 3$, the parity-oblivious set is defined as $\mathcal{S}_3 = \{011, 101, 110, 111\}$, corresponding to all non-trivial parity functions over three-bit strings. To satisfy this constraint while maintaining near-optimal performance, we refine the encoding scheme in Equation (5) through strategic input reclassification, i.e., $\mathcal{E}(011) = 0$ and $\mathcal{E}(100) = 1$, while preserving the Hamming weight threshold rule for other inputs. The computational result demonstrates that the $3\to1$ PO-RAC achieves a maximum expected success probability of $2/3$, which is less than the $E_c^{\max}$ of the standard $3\to1$ RAC.

In the case of $n = 4$, the parity-oblivious set is defined as $\mathcal{S}_4 = \{0011, 0101, 0110, 0111, 1001, 1010, 1011, 1100, 1101, 1110, 1111\}$. To reconcile this constraint with near-optimal performance, we encode the four-bit strings based on the value of the leading bit x_1. Then, the maximum expected success probability for the $4\to1$ PO-RAC is $5/8$.

4. The Maximum Expected Success Probabilities for the $n\to1$ PO-QRACs

This section establishes the theoretical maximum of the expected success probabilities for $n\to1$ PO-QRACs. Within the quantum information framework, the encoding states employed in our protocol must rigorously adhere to the parity-oblivious constraint, ensuring that no measurable information about parity correlations can be extracted through quantum measurements.

For $n = 2$, the parity-oblivious constraint manifests as $\rho_{00} + \rho_{11} = \rho_{01} + \rho_{10}$. Remarkably, the optimal standard 2→1 QRAC satisfies this condition through its symmetric encoding. We implement the following quantum scheme:

$$\rho_{00} = |+\rangle\langle+|, \rho_{11} = |-\rangle\langle-|, \rho_{01} = |0\rangle\langle 0|, \rho_{10} = |1\rangle\langle 1|, \tag{7}$$

and

$$\hat{M}_1^0 = \begin{pmatrix} \frac{1}{2} + \frac{\sqrt{2}}{4} & \frac{\sqrt{2}}{4} \\ \frac{\sqrt{2}}{4} & \frac{1}{2} - \frac{\sqrt{2}}{4} \end{pmatrix}, \hat{M}_1^1 = \begin{pmatrix} \frac{1}{2} - \frac{\sqrt{2}}{4} & -\frac{\sqrt{2}}{4} \\ -\frac{\sqrt{2}}{4} & \frac{1}{2} + \frac{\sqrt{2}}{4} \end{pmatrix}, \tag{8}$$

$$\hat{M}_2^0 = \begin{pmatrix} \frac{1}{2} - \frac{\sqrt{2}}{4} & \frac{\sqrt{2}}{4} \\ \frac{\sqrt{2}}{4} & \frac{1}{2} + \frac{\sqrt{2}}{4} \end{pmatrix}, \hat{M}_2^1 = \begin{pmatrix} \frac{1}{2} + \frac{\sqrt{2}}{4} & -\frac{\sqrt{2}}{4} \\ -\frac{\sqrt{2}}{4} & \frac{1}{2} - \frac{\sqrt{2}}{4} \end{pmatrix}. \tag{9}$$

We obtain the expected success probability as follows:

$$\begin{aligned} E_q &= \tfrac{1}{8} \sum_{x \in \{0,1\}^2} \sum_{y=1}^{2} \mathrm{tr}(\rho_x \hat{M}_y^{x_y}) \\ &= \tfrac{1}{2} + \tfrac{\sqrt{2}}{4}. \end{aligned} \tag{10}$$

This scheme is also optimal for 2→1 PO-QRAC, establishing the maximum expected success probability as $1/2 + \sqrt{2}/4$.

For $n = 3$, the parity-oblivious constraint corresponding to $S = 011$ is satisfied if $\rho_{000} + \rho_{011} + \rho_{100} + \rho_{111} = \rho_{001} + \rho_{010} + \rho_{101} + \rho_{110}$. Similarly, three conditions can be obtained for $S = 101$, $S = 110$, and $S = 111$. We represent the pure quantum state ρ_x as a linear combination of Pauli matrices:

$$\rho_x = \frac{1}{2}(\mathbb{I} + \boldsymbol{r}_x \cdot \boldsymbol{\sigma}), \tag{11}$$

where $\boldsymbol{r}_x$ is the Bloch vector for ρ_x, and $\boldsymbol{\sigma} = \{\sigma_x, \sigma_y, \sigma z\}$. Each pure state corresponds to a Bloch vector on the unit sphere, enabling the success probability to be expressed in terms of vector inner products. To maximize the expected success probability, the Bloch vectors must satisfy the antipodal condition: $\boldsymbol{r}_x = -\boldsymbol{r}_{\bar{x}}$, where $\bar{x}$ denotes the bitwise negation of x. The parity-oblivious constraint translates into solving the following system of equations:

$$\boldsymbol{r}_{000} + \boldsymbol{r}_{011} + \boldsymbol{r}_{100} + \boldsymbol{r}_{111} = \boldsymbol{r}_{001} + \boldsymbol{r}_{010} + \boldsymbol{r}_{101} + \boldsymbol{r}_{110}, \tag{12}$$

$$\boldsymbol{r}_{000} + \boldsymbol{r}_{010} + \boldsymbol{r}_{101} + \boldsymbol{r}_{111} = \boldsymbol{r}_{001} + \boldsymbol{r}_{011} + \boldsymbol{r}_{100} + \boldsymbol{r}_{110}, \tag{13}$$

$$\boldsymbol{r}_{000} + \boldsymbol{r}_{001} + \boldsymbol{r}_{110} + \boldsymbol{r}_{111} = \boldsymbol{r}_{010} + \boldsymbol{r}_{011} + \boldsymbol{r}_{100} + \boldsymbol{r}_{101}, \tag{14}$$

$$\boldsymbol{r}_{000} + \boldsymbol{r}_{011} + \boldsymbol{r}_{101} + \boldsymbol{r}_{110} = \boldsymbol{r}_{001} + \boldsymbol{r}_{010} + \boldsymbol{r}_{100} + \boldsymbol{r}_{111}. \tag{15}$$

Given the antipodal condition, we only need to consider Equation (15), reducing the constraint to $\boldsymbol{r}_{000} + \boldsymbol{r}_{011} = \boldsymbol{r}_{001} + \boldsymbol{r}_{010}$. The Bloch vector parameterization for quantum state preparation in the 3→1 PO-QRAC is expressed as

$$\boldsymbol{r}_{000} = (\sin\theta_1 \cos\varphi_1, \sin\theta_1 \sin\varphi_1, \cos\theta_1), \boldsymbol{r}_{001} = (\sin\theta_2 \cos\varphi_2, \sin\theta_2 \sin\varphi_2, \cos\theta_2), \tag{16}$$

$$\boldsymbol{r}_{010} = (\sin\theta_3 \cos\varphi_3, \sin\theta_3 \sin\varphi_3, \cos\theta_3), \boldsymbol{r}_{011} = (\sin\theta_4 \cos\varphi_4, \sin\theta_4 \sin\varphi_4, \cos\theta_4), \tag{17}$$

with angular parameters constrained by $\theta_i \in [0, \pi]$ and $\varphi_i \in [0, 2\pi)$ for $i = 1, 2, 3, 4$. The parity-oblivious condition imposes the following nonlinear constraints:

$$\begin{cases} \sin\theta_1 \cos\varphi_1 + \sin\theta_4 \cos\varphi_4 = \sin\theta_2 \cos\varphi_2 + \sin\theta_3 \cos\varphi_3, \\ \sin\theta_1 \sin\varphi_1 + \sin\theta_4 \sin\varphi_4 = \sin\theta_2 \sin\varphi_2 + \sin\theta_3 \sin\varphi_3, \\ \cos\theta_1 + \cos\theta_4 = \cos\theta_2 + \cos\theta_3. \end{cases} \tag{18}$$

For the measurement operators, we parameterize the POVM measurements through their Bloch vectors

$$\boldsymbol{m}_i^0 = (\sin\eta_i \cos\phi_i, \sin\eta_i \sin\phi_i, \cos\eta_i), \eta_i \in [0, \pi], \phi_i \in [0, 2\pi), \tag{19}$$

where $i = 1, 2, 3$. Under the conventional coordinate alignment, we let $\eta_1 = 0$, then $\boldsymbol{m}_1^0 = (1, 0, 0)$. This choice establishes the reference frame without loss of generality, simplifying the subsequent optimization problem. More precisely, the maximum expected success probability E_q for the 3→1 PO-QRAC is formally characterized by the following constrained optimization problem:

$$\begin{aligned} &\text{Maximize:} && E_q, \\ &\text{Subject to:} && E_q = \tfrac{1}{2} + \tfrac{1}{24}(\boldsymbol{r}_{000} \cdot \boldsymbol{m}_1^0 + \boldsymbol{r}_{000} \cdot \boldsymbol{m}_2^0 + \boldsymbol{r}_{000} \cdot \boldsymbol{m}_3^0 \\ &&& \quad + \boldsymbol{r}_{001} \cdot \boldsymbol{m}_1^0 + \boldsymbol{r}_{001} \cdot \boldsymbol{m}_2^0 + \boldsymbol{r}_{001} \cdot \boldsymbol{m}_3^1 \\ &&& \quad + \boldsymbol{r}_{010} \cdot \boldsymbol{m}_1^0 + \boldsymbol{r}_{010} \cdot \boldsymbol{m}_2^1 + \boldsymbol{r}_{010} \cdot \boldsymbol{m}_3^0 \\ &&& \quad + \boldsymbol{r}_{011} \cdot \boldsymbol{m}_1^0 + \boldsymbol{r}_{011} \cdot \boldsymbol{m}_2^1 + \boldsymbol{r}_{011} \cdot \boldsymbol{m}_3^1), \\ &&& \boldsymbol{r}_{000} + \boldsymbol{r}_{011} = \boldsymbol{r}_{001} + \boldsymbol{r}_{010}. \end{aligned} \tag{20}$$

Through numerical optimization using semidefinite programming, we determine that $E_q^{\max} = 0.7887$. Under this configuration, where $\boldsymbol{m}_2^0 = (0, 1, 0)$, $\boldsymbol{m}_3^0 = (1, 0, 0)$, and

$$\boldsymbol{r}_x = \frac{\sqrt{3}}{3} \sum_{i=1,2,3} \boldsymbol{m}_i^{(-1)^{x_i}}, \tag{21}$$

the theoretical upper bound of E_q is achieved. The three POVM measurements correspond to three mutually orthogonal pairs of antipodal Bloch vectors. This arrangement achieves the fundamental geometric limit for two-dimensional quantum systems. Specifically, in any qubit Hilbert space, the orthogonality-dimension complementarity principle dictates that no more than three mutually orthogonal vector pairs can coexist.

For $n = 4$, the parity-oblivious constraint set $\mathcal{S}_4$ comprises 11 elements, each corresponding to a distinct non-trivial parity function. Under the antipodal condition, the analysis reduces to considering only those parity constraints with elements of $\mathcal{S}_4$ satisfying $\mathrm{wt}(S)$ is odd. We thus define a refined parity-oblivious constraint set $\mathcal{S}_4'$, specifically comprising 0111, 1011, 1101, and 1110. Then, the parity-oblivious constraint translates into solving the following system of equations:

$$\boldsymbol{r}_{0000} + \boldsymbol{r}_{0011} + \boldsymbol{r}_{0101} + \boldsymbol{r}_{0110} = \boldsymbol{r}_{0111} + \boldsymbol{r}_{0100} + \boldsymbol{r}_{0010} + \boldsymbol{r}_{0001}, \tag{22}$$

$$\boldsymbol{r}_{0000} + \boldsymbol{r}_{0011} + \boldsymbol{r}_{0100} + \boldsymbol{r}_{0111} = \boldsymbol{r}_{0110} + \boldsymbol{r}_{0101} + \boldsymbol{r}_{0010} + \boldsymbol{r}_{0001}, \tag{23}$$

$$\boldsymbol{r}_{0000} + \boldsymbol{r}_{0010} + \boldsymbol{r}_{0101} + \boldsymbol{r}_{0111} = \boldsymbol{r}_{0110} + \boldsymbol{r}_{0100} + \boldsymbol{r}_{0011} + \boldsymbol{r}_{0001}, \tag{24}$$

$$\boldsymbol{r}_{0000} + \boldsymbol{r}_{0001} + \boldsymbol{r}_{0110} + \boldsymbol{r}_{0111} = \boldsymbol{r}_{0101} + \boldsymbol{r}_{0100} + \boldsymbol{r}_{0011} + \boldsymbol{r}_{0010}. \tag{25}$$

Following algebraic simplification of the constraint equations (Equations (22)–(25)), we derive the reduced system:

$$\boldsymbol{r}_{0000} + \boldsymbol{r}_{0111} = \boldsymbol{r}_{0001} + \boldsymbol{r}_{0110} = \boldsymbol{r}_{0010} + \boldsymbol{r}_{0101} = \boldsymbol{r}_{0011} + \boldsymbol{r}_{0100} = \boldsymbol{k}, \tag{26}$$

$$\boldsymbol{r}_{0000} + \boldsymbol{r}_{0011} = \boldsymbol{r}_{0001} + \boldsymbol{r}_{0010}, \tag{27}$$

where $\boldsymbol{k}$ denotes a fixed reference vector. Equations (26) and (27) reveal that the eight unit vectors geometrically constitute an equidiagonal parallelepiped, which is tangent to the unit Bloch sphere. $\boldsymbol{r}_{0000}$, $\boldsymbol{r}_{0010}$, $\boldsymbol{r}_{0110}$, and $\boldsymbol{r}_{0100}$ form a rectangle lying on a circle of the Bloch sphere, see Figure 2.

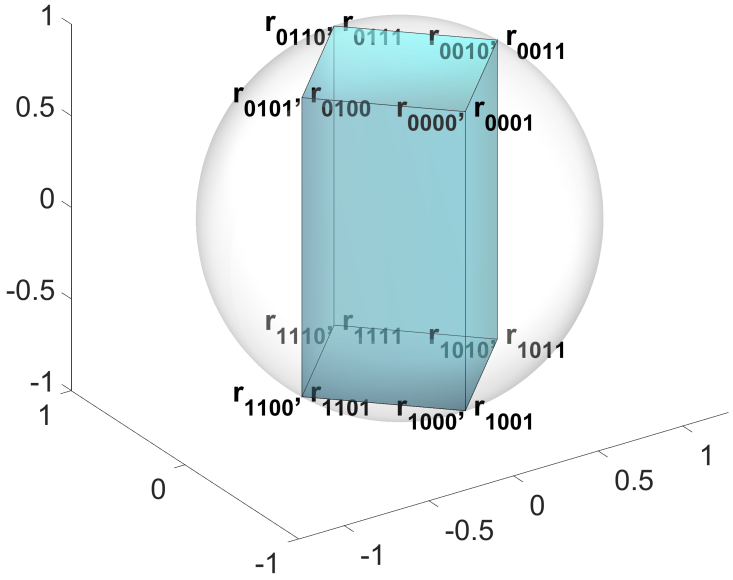

Figure 2. Geometric representation of encoded quantum states in the 4→1 PO-QRAC. The spatial distribution of Bloch vectors for the encoded states satisfies the symmetry constraints defined in Equations (26) and (27), forming the eight vertices of an equidiagonal parallelepiped on the Bloch sphere (rendered as a semitransparent gray sphere). This geometric configuration fundamentally differs from the tetrahedral arrangement characterizing the optimal 4→1 QRAC, highlighting the structural impact of parity-oblivious constraints on quantum state geometry.

Under the above genetic conditions, we define the vector $\boldsymbol{r}_{0000}$ as

$$\boldsymbol{r}_{0000} = (\sin\theta_0 \cos\varphi_0, \sin\theta_0 \sin\varphi_0, \cos\theta_0), \tag{28}$$

where $\theta_0 \in [0, \pi]$ and $\varphi_0 \in [0, 2\pi)$. The other encoded quantum states are determined based on $\boldsymbol{r}_{0000}$.

Given the fundamental geometric constraint that a two-dimensional Hilbert space permits at most three mutually orthogonal measurement bases, our protocol strategically duplicates one measurement basis to accommodate the fourth required setting in the 4→1 PO-QRAC optimization. Following the optimal QRAC configuration framework, we intentionally align the fourth measurement basis with one of the three existing orthogonal pairs. Without loss of generality, we implement the following Bloch vector assignments:

$$\boldsymbol{m}_1^0 = (0,0,1), \boldsymbol{m}_2^0 = (0,1,0), \tag{29}$$

$$\boldsymbol{m}_3^0 = (1,0,0), \boldsymbol{m}_4^0 = (0,0,1). \tag{30}$$

The expected success probability E_q for the 4→1 PO-QRAC can be written as

$$E_q = \frac{1}{2} + \frac{1}{128} \sum_{x \in \{0,1\}^4} \boldsymbol{r}_x \cdot \Big(\sum_{i=1,2,3,4} \boldsymbol{m}_i^{x_i} \Big). \tag{31}$$

By varying the spherical coordinate parameters θ_0 and φ_0, we characterize the functional relationship between these angular variables and the expected success probability E_q of the 4→1 PO-QRAC. Numerical optimization reveals a global maximum of $E_q = 0.7165$ at $\theta_0 = \frac{5\pi}{16}$ and $\varphi_0 = \frac{\pi}{4}$, corresponding to a geometrically optimal Bloch vector configuration. The dependence of E_q on θ_0, and φ_0 is fully mapped in Figure 3.

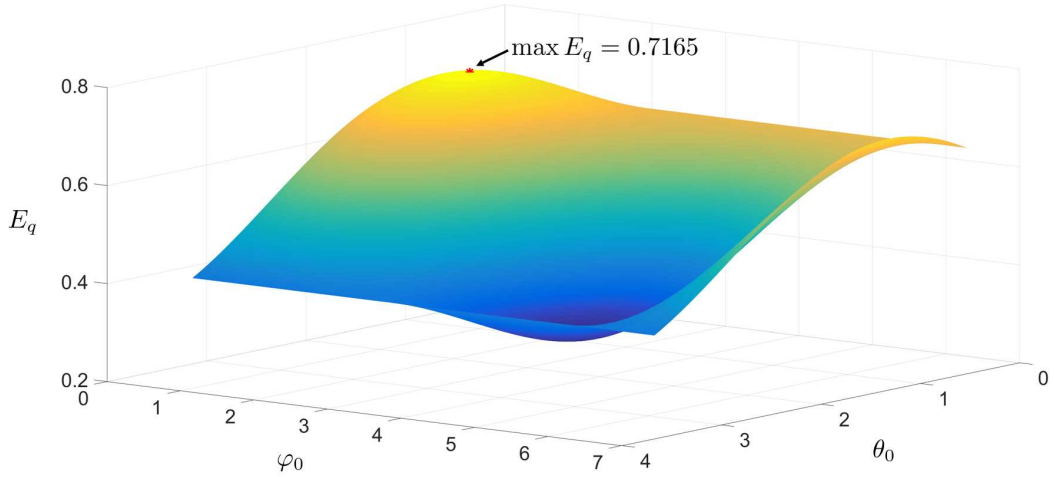

Figure 3. Relationship of the expected success probability E_q on spherical coordinates θ_0 and φ_0 for the 4→1 PO-QRAC. The maximum $E_q = 0.7165$ (marked by the red datapoint) is achieved at $\theta_0 = \frac{5\pi}{16}$ and $\varphi_0 = \frac{\pi}{4}$.

The above result demonstrates an enhancement over the previously reported bound of $1/2 + \sqrt{2}/8$ in [31], while rigorously satisfying the parity-obliviousness constraint. However, the result falls short of the theoretical upper bound $E_q = 0.75$ for the 4→1 PO-QRAC reported in [32]. Achieving that bound in a qubit system would require constructing four mutually complementary measurements, yet any qubit admits at most three such measurements, corresponding to the three Pauli matrices. To reach $E_q = 0.75$, one must upgrade the protocol to a four-dimensional Hilbert space, where the necessary observables can be built from the generalized Gell-Mann matrices. In that setting, the scheme becomes a 4→2 PO-QRAC and can attain the theoretical maximum.

5. Randomness Certification

Following the analytical determination of maximum success probabilities for n→1 PO-QRACs with $n = 2, 3, 4$, we now investigate the certifiable randomness generated by quantum randomness expansion protocols based on this family of quantum access codes. The two conditions that must be met in order to generate fresh randomness are as follows:

1. Violation of a quantum witness, i.e., $E_q > E_c^{\max}$, where E_q is the quantum expected success probability and $E_c^{\max}$ denotes the classical bound.
2. The min-entropy $H_\infty(B \mid X, Y)$ of the output bit must be strictly positive, i.e., $H_\infty(B \mid X, Y) > 0$.

As demonstrated in our prior analyses, the maximum expected success probabilities of n→1 PO-QRACs for $n = 2, 3, 4$ exceed their respective classical bounds, thereby satisfying the first criterion for randomness generation. We now characterize the parametric conditions under which the second critical requirement is fulfilled.

We now proceed to establish a lower bound on the min-entropy conditioned on the expected success probability E_q of the $n\to1$ PO-QRAC, which can be obtained by solving the following optimization problem:

$$\begin{aligned} &\text{Minimize:} && H_\infty(B \mid X, Y), \\ &\text{Subject to:} && E_q = \tfrac{1}{n\cdot 2^n} \sum_{x\in\{0,1\}^n} \sum_{y=1}^{n} p(b = x_y \mid x, y), \\ & && \forall S \in \mathcal{S}_n : \quad \textstyle\sum_{x\in\{0,1\}^n} (-1)^{\oplus_{i\in S} x_i} \rho_x = 0. \end{aligned} \tag{32}$$

Following Equation (2), the optimization problem can be reformulated as maximizing the conditional probability $p(b = x_y \mid x, y)$ for a given target expected success probability E_q. In the optimization problem, the set of achievable pairs $(E_q, \max p(b = x_y \mid x, y))$ forms a concave region. Consequently, the function f that returns the maximal value of $\max p(b = x_y \mid x, y)$ for a fixed E_q coincides with the inverse mapping that returns the maximal E_q for a fixed $\max p(b = x_y \mid x, y)$. We then derive f^{-1} by solving the following optimization:

$$\begin{aligned} &\text{Maximize:} && E_q = \tfrac{1}{n\cdot 2^n} \sum_{x\in\{0,1\}^n} \sum_{y=1}^{n} p(b = x_y \mid x, y), \\ &\text{Subject to:} && \max_{x,y} p(b = x_y \mid x, y) = p, \\ & && \forall S \in \mathcal{S}_n : \quad \textstyle\sum_{x\in\{0,1\}^n} (-1)^{\oplus_{i\in S} x_i} \rho_x = 0, \end{aligned} \tag{33}$$

where p is the fixed maximum probability value.

For $n = 2$, we define $\boldsymbol{m}_1^0 = (1, 0, 0)$ and $\boldsymbol{m}_2^0 = (\cos\alpha, \sin\alpha, 0)$, $0 \leqslant \alpha \leqslant \pi$. Without loss of generality, let $p(b = 1 \mid 11, 1) = p$ and set the corresponding Bloch vector $\boldsymbol{r}_{11} = (-\cos\beta, -\sin\beta, 0)$, where $\beta = \arccos(2p - 1)$. To maximize the value of E_q, the optimal preparations for the remaining inputs are

$$\boldsymbol{r}_{01} = \frac{\boldsymbol{m}_1^0 + \boldsymbol{m}_2^1}{\| \boldsymbol{m}_1^0 + \boldsymbol{m}_2^1 \|}, \boldsymbol{r}_{10} = \frac{\boldsymbol{m}_1^1 + \boldsymbol{m}_2^0}{\| \boldsymbol{m}_1^1 + \boldsymbol{m}_2^0 \|}. \tag{34}$$

Finally, enforcing parity-obliviousness requires $\boldsymbol{r}_{00} = -\boldsymbol{r}_{11}$.

We derive the expected success probability E_q as

$$E_q = \frac{1}{2} + \frac{1}{8}(\sqrt{2 - 2\cos\alpha} + (2p - 1)(1 + \cos\alpha) + 2\sqrt{p^2 - p}\sin\alpha). \tag{35}$$

The inverse function $f^{-1}(p)$ is correspondingly given by

$$f^{-1}(p) = \frac{1}{2} + \frac{1}{8}(\sqrt{2 - 2\cos\alpha_p} + (2p - 1)(1 + \cos\alpha_p) + 2\sqrt{p - p^2}\sin\alpha_p), \tag{36}$$

where α_p denotes the critical point that extremizes f^{-1} with respect to α and $0 \leqslant \alpha_p \leqslant \pi$.

The relationship between the min-entropy bound $H_\infty^{E_q}$ and the expected success probability E_q for the $2\to1$ PO-QRAC is plotted in Figure 4. The result shows that the integration of parity-oblivious constraints into the randomness expansion protocol enables the generation of certifiable randomness at an enhanced rate.

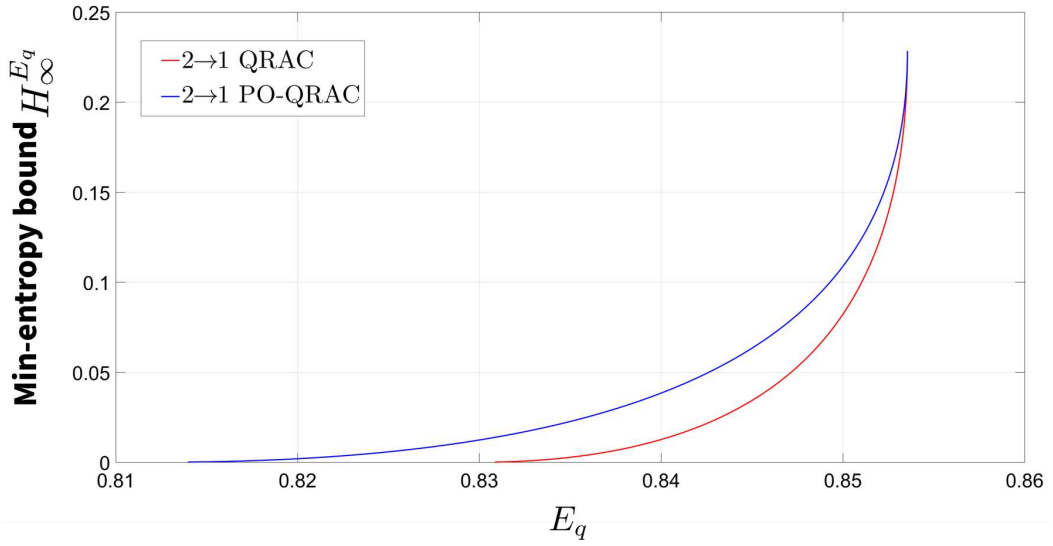

Figure 4. The relationship between the min-entropy bound $H_\infty^{E_q}$ and the expected success probability E_q for the 2→1 PO-QRAC. The red curve represents the randomness expansion protocol based on 2→1 QRAC, while the blue curve corresponds to the enhanced protocol utilizing 2→1 PO-QRAC. Comparative analysis demonstrates that the latter achieves a broader certifiable randomness range. Notably, when the min-entropy assumes positive values, the E_q consistently surpasses its classical counterpart $E_c = 3/4$.

For the case of $n = 3$, to ensure $\boldsymbol{m}_1^0\boldsymbol{m}_2^0 = \boldsymbol{m}_1^0\boldsymbol{m}_3^0 = \boldsymbol{m}_2^0\boldsymbol{m}_3^0$, the measurements are defined as

$$\boldsymbol{m}_1^0 = (1, 0, 0), \tag{37}$$
$$\boldsymbol{m}_2^0 = (\cos 2\alpha, \sin 2\alpha, 0), \tag{38}$$
$$\boldsymbol{m}_3^0 = (\cos\alpha \sin\beta, \sin\alpha \sin\beta, \cos\beta), \tag{39}$$

where $0 \leqslant \alpha \leqslant \pi/2$, $-\pi/2 \leqslant \beta \leqslant \pi/2$. Assuming that $p(b = 1 \mid 111, 3) = p$, the states can be defined as

$$\boldsymbol{r}_{111} = (-\cos\alpha \sin(\beta+\gamma), -\sin\alpha \sin(\beta+\gamma), -\cos(\beta+\gamma)), \tag{40}$$
$$\boldsymbol{r}_{000} = -\boldsymbol{r}_{111}, \tag{41}$$
$$\boldsymbol{r}_{x\neq 000,111} = \frac{\boldsymbol{m}_1^{x_1} + \boldsymbol{m}_2^{x_2} + \boldsymbol{m}_3^{x_3}}{\| \boldsymbol{m}_1^{x_1} + \boldsymbol{m}_2^{x_2} + \boldsymbol{m}_3^{x_3} \|}, \tag{42}$$

where $x \in \{0,1\}^3$. We can derive the inverse function $f^{-1}(p)$ as

$$\begin{aligned} f^{-1}(p) = \; & \tfrac{1}{2} + \tfrac{3}{8}\sqrt{3 - 2\cos 2\alpha_p} \\ & + \tfrac{1}{24}\left[(2p-1)(1 + 2\cos^2\alpha_p - 2) + 2\sqrt{(p-p^2)(5 - 4\cos^2\alpha_p - \tfrac{1}{\cos^2\alpha_p})}\right], \end{aligned} \tag{43}$$

where α_p denotes the extreme point of f^{-1} with respect to α and $0 \leqslant \alpha_p \leqslant \pi$. The optimization process must strictly maintain the balance equation $\boldsymbol{r}_{000} + \boldsymbol{r}_{011} = \boldsymbol{r}_{010} + \boldsymbol{r}_{001}$.

The relationship between the min-entropy bound $H_\infty^{E_q}$ and the expected success probability E_q for the 3→1 PO-QRAC is plotted in Figure 5. Our analysis reveals that the quantum randomness expansion protocol based on the 3→1 PO-QRAC achieves a higher certified randomness generation rate compared to its 2→1 PO-QRAC counterpart.

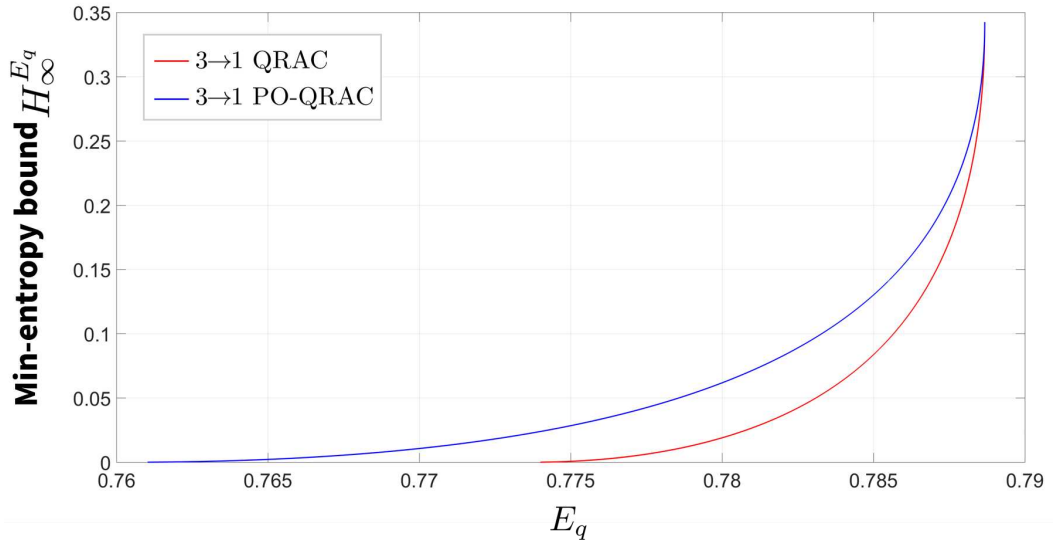

Figure 5. The relationship between the min-entropy bound $H_\infty^{E_q}$ and the expected success probability E_q for the 3→1 PO-QRAC. The red curve represents the randomness expansion protocol based on 3→1 QRAC, while the blue curve corresponds to the enhanced protocol utilizing 3→1 PO-QRAC. Comparative analysis demonstrates that the latter achieves a broader certifiable randomness range. Notably, when the min-entropy assumes positive values, the E_q consistently surpasses its classical counterpart $E_c = 2/3$.

The proposed $3 \to 1$ PO-QRAC-based randomness expansion protocol achieves a higher certified min-entropy compared to conventional QRAC implementations at identical quantum witness values E_q. Additionally, the results presented in Section 4 demonstrate that the $3 \to 1$ PO-QRAC achieves the maximum quantum success probability among all investigated configurations. This optimal performance simultaneously maximizes the certifiable min-entropy. Crucially, SDI randomness expansion protocols utilizing $3 \to 1$ PO-QRAC outperform both $2 \to 1$ and $4 \to 1$ variants in entropy generation efficiency, establishing it as the optimal protocol configuration for quantum randomness expansion under parity-oblivious constraints.

6. Conclusions

We have investigated randomness-expansion protocols based on the $n \to 1$ PO-QRACs. After introducing the protocol model, we derived tight upper bounds on the maximum success probability in both the classical and quantum settings. Our analysis shows that for $n = 2, 3, 4$, the PO-QRAC always outperforms its classical counterpart, making it a viable primitive for SDI randomness expansion. Remarkably, in the case of $n = 4$, the quantum bound under the parity-oblivious constraint even exceeds the limit reported in [31]. However, for $n > 3$, no two-dimensional PO-QRAC can attain the theoretical maximum of 0.75 derived by [32], since that bound demands the existence of n mutually unbiased bases in a qubit system, which is impossible. Finally, we established an analytic relation between the quantum witness E_q and the certifiable randomness (min-entropy) in these protocols. Numerically, we find that for $n = 2, 3$, PO-QRAC-based expansion certifies strictly more randomness than standard QRAC-based schemes at the same E_q value, demonstrating the advantage of enforcing parity obliviousness. The SDI randomness expansion protocol constructed using the 3→1 PO-QRAC represents the optimal implementation framework for quantum randomness expansion under parity-oblivious constraints.

Author Contributions: Conceptualization, X.W.; Methodology, X.C. (Xiao Chen); Investigation, X.C. (Xu Chen); Data curation, W.M.; Writing—original draft, X.W.; Writing—review & editing, M.X. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Natural Science Foundation of Zhejiang Province, China, (Grant No. Q24A050004).

Institutional Review Board Statement: Not applicable.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Knuth, D.E. *The Art of Computer Programming, Volume 2: Seminumerical Algorithms*, 2nd ed.; Addison-Wesley: Reading, MA, USA, 1981.
2. Bouda, J.; Pivoluska, M.; Plesch, M.; Wilmott, C. Weak randomness seriously limits the security of quantum key distribution. *Phys. Rev. A* **2012**, *86*, 062308. [CrossRef]
3. Dhara, C.; De La Torre, G.; Acín, A. Can observed randomness be certified to be fully intrinsic? *Phys. Rev. Lett.* **2014**, *112*, 100402. [CrossRef] [PubMed]
4. Shen, Y.; Tian, L.; Zou, H.X. Practical quantum random number generator based on measuring the shot noise of vacuum states. *Phys. Rev. A* **2010**, *81*, 063814. [CrossRef]
5. Vallone, G.; Marangon, D.G.; Tomasin, M.; Villoresi, P. Quantum randomness certified by the uncertainty principle. *Phys. Rev. A* **2014**, *90*, 052327. [CrossRef]
6. Lunghi, T.; Brask, J.B.; Lim, C.C.W.; Lavigne, Q.; Bowles, J.; Martin, A.; Zbinden, H.; Brunner, N. Self-testing quantum random number generator. *Phys. Rev. Lett.* **2015**, *114*, 150501. [CrossRef]
7. Van Himbeeck, T.; Woodhead, E.; Cerf, N.J.; García-Patrón, R.; Pironio, S. Semi-device-independent framework based on natural physical assumptions. *Quantum* **2017**, *1*, 33. [CrossRef]
8. Liu, Y.; Yuan, X.; Li, M.H.; Zhang, W.; Zhao, Q.; Zhong, J.; Cao, Y.; Li, Y.H.; Chen, L.K.; Li, H.; et al. High-speed device-independent quantum random number generation without a detection loophole. *Phys. Rev. Lett.* **2018**, *120*, 010503. [CrossRef]
9. Acín, A.; Brunner, N.; Gisin, N.; Massar, S.; Pironio, S.; Scarani, V. Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.* **2007**, *98*, 230501. [CrossRef]
10. Colbeck, R. Quantum and Relativistic Protocols for Secure Multi-Party Computation. Ph.D. Dissertation, University of Cambridge, Cambridge, UK, 2007.
11. Pawłowski, M.; Brunner, N. Semi-device-independent security of one-way quantum key distribution. *Phys. Rev. A* **2011**, *84*, 010302(R). [CrossRef]
12. Teo, Y.S.; Shringarpure, S.U.; Jeong, H.; Prasannan, N.; Brecht, B.; Silberhorn, C.; Evans, M.; Mogilevtsev, D.; Sánchez-Soto, L.L. Evidence-based certification of quantum dimensions. *Phys. Rev. Lett.* **2024**, *133*, 050204. [CrossRef]
13. Håkansson, E.; Piveteau, A.; Seguinard, A.; Muhammad, S.; Bourennane, M.; Gühne, O.; Plávala, M. Experimental implementation of dimension-dependent contextuality inequality. *Phys. Rev. Lett.* **2025**, *134*, 200202. [CrossRef] [PubMed]
14. Colbeck, R.; Kent, A. Private randomness expansion with untrusted devices. *J. Phys. A Math. Theor.* **2011**, *44*, 095305. [CrossRef]
15. Colbeck, R.; Renner, R. Free randomness can be amplified. *Nat. Phys.* **2012**, *8*, 450–453. [CrossRef]
16. Pironio, S.; Acín, A.; Massar, S.; Boyer de la Giroday, A.; Matsukevich, D.N.; Maunz, P.; Olmschenk, S.; Hayes, D.; Luo, L.; Manning, T.A.; et al. Random numbers certified by Bell's theorem. *Nature* **2010**, *464*, 1021–1024. [CrossRef]
17. Coudron, M.; Yuen, H. Infinite randomness expansion with a constant number of devices. In Proceedings of the 46th Annual ACM Symposium on Theory of Computing, New York, NY, USA, 31 May–3 June 2014; pp. 427–436.
18. Li, H.W.; Yin, Z.Q.; Wu, Y.C.; Zou, X.B.; Wang, S.; Chen, W.; Guo, G.C.; Han, Z.F. Semi-device-independent random-number expansion without entanglement. *Phys. Rev. A* **2011**, *84*, 034301. [CrossRef]
19. Li, H.W.; Pawłowski, M.; Yin, Z.Q.; Guo, G.C.; Han, Z.F. Semi-device-independent randomness certification using $n \rightarrow 1$ quantum random access codes. *Phys. Rev. A* **2012**, *85*, 052308. [CrossRef]
20. Zhou, Y.Q.; Li, H.W.; Wang, Y.K.; Li, D.D.; Gao, F.; Wen, Q.Y. Semi-device-independent randomness expansion with partially free random sources. *Phys. Rev. A* **2015**, *92*, 022331. [CrossRef]
21. Zhou, Y.Q.; Gao, F.; Li, D.D.; Li, X.H.; Wen, Q.Y. Semi-device-independent randomness expansion with partially free random sources using $3 \rightarrow 1$ quantum random access code. *Phys. Rev. A* **2016**, *94*, 032318. [CrossRef]
22. Li, D.D.; Wen, Q.Y.; Wang, Y.K.; Zhou, Y.Q.; Gao, F. Security of semi-device-independent random number expansion protocols. *Sci. Rep.* **2015**, *5*, 15543. [CrossRef]

23. Wang, X.N.; Yuan, J.B.; Zhou, Y.Q.; Liu, Y.; Fan, L.L. Semi-device-independent randomness certification with partially free random sources using 4→1 quantum random access code. *Quantum Inf. Process.* **2022**, *21*, 38. [CrossRef]
24. Mohan, K.; Tavakoli, A.; Brunner, N. Sequential random access codes and self-testing of quantum measurement instruments. *New J. Phys.* **2019**, *21*, 083034. [CrossRef]
25. Tavakoli, A.; Marques, B.; Pawłowski, M.; Bourennane, M. Spatial versus sequential correlations for random access coding. *Phys. Rev. A* **2016**, *93*, 032336. [CrossRef]
26. Curchod, F.J.; Johansson, M.; Augusiak, R.; Hoban, M.J.; Wittek, P.; Acín, A. Unbounded randomness certification using sequences of measurements. *Phys. Rev. A* **2017**, *95*, 020102(R). [CrossRef]
27. Sasmal, S.; Das, D.; Mal, S.; Majumdar, A.S. Steering a single system sequentially by multiple observers. *Phys. Rev. A* **2018**, *98*, 012305. [CrossRef]
28. Wang, X.N.; Yuan, J.B.; Zhou, Y.Q.; Liu, Y.; Fan, L.L. Semi-device-independent randomness expansion using n→1 sequential quantum random access codes. *Quantum Inf. Process.* **2021**, *20*, 346. [CrossRef]
29. Xiao, Y.; Guo, F.Z.; Dong, H.F.; Gao, F. Expanding the sharpness parameter area based on sequential 3→1 parity-oblivious quantum random access code. *Quantum Inf. Process.* **2023**, *22*, 195. [CrossRef]
30. Spekkens, R.W.; Buzacott, D.H.; Keehn, A.J.; Toner, B.; Pryde, G.J. Preparation contextuality powers parity-oblivious multiplexing. *Phys. Rev. Lett.* **2009**, *102*, 010401. [CrossRef]
31. Mukherjee, S.; Pan, A.K. Semi-device-independent certification of multiple unsharpness parameters through sequential measurements. *Phys. Rev. A* **2021**, *104*, 062214. [CrossRef]
32. Ghorai, S.; Pan, A.K. Optimal quantum preparation contextuality in an n-bit parity-oblivious multiplexing task. *Phys. Rev. A* **2018**, *98*, 032110. [CrossRef]
33. Ambainis, A.; Leung, D.; Mancinska, L.; Ozols, M. Quantum random access codes with shared randomness. *arXiv* **2009**, arXiv:0810.2937.