Quantum and semi-quantum lottery: strategies and advantages

Sandeep Mishra · Anirban Pathak

Received: 30 March 2022 / Accepted: 29 June 2023 / Published online: 18 July 2023
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2023

Abstract
Lottery is a game in which multiple players take chances in the hope of getting some rewards in cash or kind. In addition, from the time of the early civilizations, lottery has also been considered as an opposite method to allocate scarce resources. Technically, any scheme for lottery needs to be fair and secure, but none of the classical schemes for lottery are unconditionally secure and fair. As fairness demands complete unpredictability of the outcome of the lottery, it essentially requires perfect randomness. Quantum mechanics not only guarantees the generation of perfect randomness, it can also provide unconditioned security. Motivated by these facts, a set of strategies for performing lottery using different type of quantum resources (e.g., single photon states, and entangled states) are proposed here, and it’s established that the proposed strategies lead to unconditionally secure and fair lottery schemes. A scheme for semi-quantum lottery that allows some classical users to participate in the lottery involving quantum resources is also proposed and the merits and demerits of all the proposed schemes are critically analysed. It is also established that the level of security is intrinsically related to the type of quantum resources being utilized. Further, it is shown that the proposed schemes can be experimentally realized using currently available technology, and that may herald a new era of commercial lottery.

Keywords Quantum lottery · Semi-quantum lottery · Fair and secure quantum lottery

1 Introduction
Lottery is a game of chances where multiple players hope for getting the rewards. The use of lotteries has been prevalent since the time of early human civilizations. For example, during the Roman empire, lotteries were used as a form of amusement for giving gifts to the guests [1]. The first commercial application of the lottery was
done by Roman Emperor Augustus Caesar as an alternative to increase in taxes for the purpose of funding the infrastructure projects of the city [2]. In the modern history, the first officially recorded state controlled lottery was organized by Queen Elizabeth I in 1556–59 for the purpose of funding a set of projects [3]. In this particular case, 40,000 tickets of 0.5 pound each were issued with a reward of 5000 pounds to the winner. Since then, the lotteries have globally evolved as a mechanism that states can adopt to collect money (without levying higher taxes) required for various people-centric projects. Thus, the lottery is historically used for socially meaningful purposes, but it has close resemblance with the gambling and it can always be viewed as a kind of gambling. Consequently, nowadays commercial lottery with financial rewards is not considered righteous in many countries.

Despite the above issue, we are interested in the lottery as the use of lottery is not restricted to gambling and collection of funds by the states. In fact, lotteries have many other applications in the diverse fields [4]. In the modern theory of allocation of resources, there are primarily four ways of allocation namely merit, queue, auction and lotteries. In “merit”, the persons are allotted points based on many parameters and the entity with maximum points get the first preference. In “queue”, the entity which has submitted the application first gets the reward. In “auction”, one who is willing to pay the maximum gets the rights. Of all the above, lotteries do a randomization and the entity gets hold of the resource purely by luck. In fact, lottery is the only method which is free from any type of inherent bias. Debates are going on to find an optimum method for the allocation of resources [5], but the lottery is often considered as a better and fairer way of allocating the scarce resources among the large number of applicants [6, 7]. Specially, if the number of indivisible goods (k) is lesser than the number of applicants (n) then lottery is considered as a suitable way for the allocation. Tracing down in history, the lottery has been used by governments for the allotment of lands to the farmers. Even nowadays lotteries are used for the allocation of low cost houses by many governments across the world. Lotteries are prevalent medium in many countries for fair grant of admission to the students in the elementary schools. Lotteries are also used to grant work permits from the pool of eligible applicants. Lotteries are considered as a good way of placing the teams in various groups of major sporting events such as Olympics and the events organized by FIFA, NBA, etc. Even there is a recorded history of use lottery in the legal system where punishment to the accused was delivered via use of lottery in a situation where the act of crime was committed by a mob and it was difficult to trace out the right person who dealt the fatal blow [8]. With respect to technology, lottery-based CPU scheduling among the various competing processes has been proposed and used for instantaneous fair CPU allocation [9]. Indeed, recently, lottery ticket hypothesis for graph theory has been proposed for training of the neural networks [10]. Nowadays, serious debate is also going on for the use of lotteries for the funding of the research projects as the prevalent medium of the peer review process has many intrinsic biases [11]. In fact, many funding agencies such as the Health Research Council of New Zealand, Volkswagen Foundation in Germany and the Swiss National Science Foundation are using the lotteries to fund the research projects after the initial screening of the eligible projects [12, 13].
As described above, lottery is an integral part of many important processes that are associated with our daily life. However, not all forms of lottery can be considered as fair. To understand this point, we first need to understand the meaning of a fair lottery. A lottery is considered as fair if and only if all the participants have an equal chance of winning. Thus, it requires perfect randomness. Further, once the results are announced then no one should be able to forge the ticket and claim to be the winner. Moreover, every participant should be able to verify the outcome of the process. An important point of concern is that the fairness of the lottery is inherently dependent upon the security of the lottery scheme being used. Thus, randomness and security are the primary concerns associated with the schemes of the lottery. Currently, the lottery schemes being used depend upon the credibility of the trusted authorities or security based on some mathematical complexities. Security derived in such a way is conditional. In fact, an unconditional security cannot be obtained in the classical world. Further, randomness used in classical schemes is weak compared to the randomness that can be generated quantum mechanically. Naturally, often issues have been raised regarding the fairness of the lottery schemes and such things will come up again and again until and unless we have an unconditionally secure lottery scheme. By unconditionally secure, we mean that any potential adversary even with the unlimited resources would not be able to manipulate the outcome. Such issues were raised for the classical cryptographic schemes, too, but the advent of quantum cryptography [14] provided a new way forward for unconditionally secure cryptography [15–17]. The use of quantum states is currently being explored for providing unconditional security in various applications such as bit commitment [18–20], auctions [21, 22], voting [23–26], multi-party computation [27]. Lottery is inherently related to quantum states as quantum mechanics has intrinsic randomness and lottery demands a complete randomization of the outcome [28].

Quantum strategies for fair and unconditionally secure lottery is a demand of the time. A step in this direction was provided by Sun et al. [29], where they proposed the schemes for lottery and auction on the backbone of the quantum blockchain. However, the mentioned protocol was not mature as it was based on quantum bit commitment which still does not provide unconditional security. Further, it used the elementary idea of quantum blockchain where communication between nodes was done via the QKD protocol for which trust between the nodes would have been required at the forefront. However, the blockchain requires consensus on the contents of the decentralized data between non-trusting parties. Barring this work, the field for use of quantum systems in implementing lottery schemes has remained largely untouched till now. Hence, we try to explore the use of quantum resources towards the development of fair and unconditionally secure lottery schemes which can be implemented via the currently available quantum hardware.

The rest of the paper is structured as follows. In Sect. 2, we introduce some of the basic ideas and nomenclature required for better understanding of the article with specific attention to the requirements that a good scheme of lottery should satisfy. Subsequently, a set of schemes for quantum and semi-quantum lottery are proposed in Sect. 3. This is followed by security analysis of the proposed schemes in Sect. 4. Finally, the paper is concluded in Sect. 5.
Fig. 1 (Color online) Schematic of the quantum lottery scheme with solid lines denoting quantum channels while dashed lines denoting classical channels.

2 Basic notations and definitions

The basic requirements to be satisfied by a lottery scheme can be briefly mentioned as follows:

(i) *Eligibility* Only the registered and legitimate entities can take part in the lottery with the eligible entities forming a set \( \mathcal{P} \).

(ii) *Equi-probability* All the entities have equal probability to win the lottery. Thus, if there are \( n \) participants, then the probability of winning for every participant \( (p_i) \) must be the same (complete randomization) and the total probability should be equal to unity. i.e.,

\[
p_1 = p_2 = p_3 = \cdots = p_n = \frac{1}{n}, \quad \text{s.t.} \quad \sum_{i=1}^{n} p_i = 1.
\]  

(iii) *Binding* No one can change the lottery ticket after it has been issued.

(iv) *Verifiability* Anyone can verify the outcome of the process.

(v) *Secure* An adversary even with unconditional computational power cannot manipulate the outcome.

3 Quantum lottery schemes

The proposed lottery schemes consist of the following stakeholders (see Fig. 1):

1. *Lottery Authority* The lottery authority \( (LA) \) is responsible for the conduct of lottery. Further, it will consist of multiple personnels but for the sake of simplicity, we can consider it to be consisting of three agents only, namely ‘lottery authority for registration’ \( (LAR) \), ‘lottery authority for ticketing 1’ \( (LAT_1) \) and ‘lottery authority for ticketing 2’ \( (LAT_2) \). The role of \( LAR \) is to register the interested parties and record their details. The role of \( LAT_1 \) and \( LAT_2 \) is to generate the lottery tickets for every eligible participant. Further, they cooperate with each other to declare the winning lottery ticket. In addition to this, we assume that the personnel of the \( LA \) are semi-honest. i.e., they faithfully follow all the steps of the protocol, but they may try to cheat without modifying the steps.
2. Participants Participants ($P_i$) consist of the set of people who are interested to participate in the lottery. It is to be mentioned that the proposed lottery scheme provides a method by which every participant can verify the winning lottery ticket.

3.1 BB84-based quantum lottery scheme

It has always been an endeavour since ages to develop a scheme by which secret messages can be sent from one party to another with minimum number of assumptions. The classical schemes were basically based on the assumption of trust that the encryption key is available to only authorized people or that some problems are too complex to be solved in polynomial time [30]. However, the advent of quantum cryptography in 1984 [i.e., the introduction of BB84 protocol for quantum key distribution (QKD)] [14] altogether changed the rules of the game by providing a scheme for unconditionally secure distribution of keys. Further, Ekert showed that the unconditional secure distribution of keys can be done via the use of entanglement [31] and the presence of unauthorized interceptor can be detected by checking the correlations between entangled particles. This lead to two different ways of secure key distribution and each has its own advantages and disadvantages. Currently, this field of unconditional secure cryptography is quite mature to be used in practical situations and scenarios [15, 16, 32, 33]. Parallel to the development of quantum key distribution technology, researchers have been working on the development of true random number generators whose outputs are completely non-deterministic as well as private. Since quantum mechanics has intrinsic randomness associated with it [34], so the quantum systems can be used to generate truly random numbers [35]. Currently, the quantum technology is quite mature that we can generate very high quality random numbers at great speeds [36–39] for a wide variety of applications including secure communication, e-commerce, multi-party computations and lottery. In fact, there are many commercial quantum random number generator (QRNG) devices available in the market such as ID Quantique [40], Toshiba [41], PicoQuant [42], MPD [43] etc.

Taking inspiration from quantum cryptographic protocols, and the availability of the required hardware, we will first propose a lottery strategy based on BB84 states [44] and then briefly elaborate about its physical implementation. BB84 states are one of the most important and widely studied set of states studied in context of quantum key distribution. These states can be experimentally produced in a wide variety of physical systems, but it is more useful when implemented using photonic systems. In photonics, BB84 states are essentially polarization-encoded qubits or equivalently a sequence of photons which are randomly polarized in horizontal, vertical, $45^\circ$ or $-45^\circ$ which respectively correspond to the states $|0\rangle$, $|1\rangle$, $|+\rangle$ and $|−\rangle$ [45]. These states can be easily generated by passing the photons from a laser diode source to an attenuator (neutral density filter) or by performing heralding on the output of certain spontaneous parametric down conversion process, and then passing the single photon through the relevant polarizer [46]. The lottery scheme using BB84 states involves the following three stages:
3.1.1 Registration phase

This phase is required for the registration of every participant with the \( LA \) and generation of unique digital signatures similar to that proposed by Wallden et al. [47] for every participant \( P_i \). The steps involved in the process can be enumerated as follows:

Step 1  The participant \( P_i \) will first register with the \( LA \) by sending the documents to \( LAR \) for purchasing the lottery ticket.

Step 2  \( LAR \) will verify the credentials of the \( P_i \) with the help of own or any third party database and then use a QRNG to issue a unique 256-bit participant’s identity \( PID_i \) for the participant \( P_i \). \( PID_i \) will be sent to \( P_i \) using the classical public key cryptosystems. Further, \( LAR \) keeps a record of all the allocated \( PID_i \)s to form a set of eligible participants \( \mathcal{P} \). The purpose of generation of \( PID_i \) for every participant is to maintain the privacy of the participants as from here on the participant will only be using \( PID_i \)s in all the subsequent steps. Because of the use of QRNG by \( LAR \), the probability of \( PID_i \) collision for two participants will be asymptotically very small. However, if the \( PID_i \) generated for a new participant collides with the existing set of allocated \( PID_i \)s, then the QRNG is used again to generate a new \( PID_i \).

Step 3  For the generation of digital signatures, the participant \( P_i \) will generate two large identical, but random sequences \( (S_1, S_2) \) of BB84 states \( (|0\rangle, |1\rangle, |+\rangle, |−\rangle) \) in accordance with the output generated by QRNG. \( P_i \) will first send the \( PID_i \) to \( LAT_1 \) and \( LAT_2 \). Both \( LAT_1 \) and \( LAT_2 \) will verify the identity of \( P_i \) by checking if \( PID_i \in \mathcal{P} \). After the successful verification of participant, the \( P_i \) will send the first \( (S_1) \) and second \( (S_2) \) sequence respectively to \( LAT_1 \) and \( LAT_2 \) via the use of quantum channel.

Step 4  \( LAT_1 \) (\( LAT_2 \)) will randomly choose to either forward the element of sequence \( S_1 \) (\( S_2 \)) to \( LAT_2 \) (\( LAT_1 \)) or keep it with themselves to directly measure it. Further, in either case the position of the elements in the sequence is recorded.

Step 5  \( LAT_1 \) (\( LAT_2 \)) measures the states that they have directly received from \( P_i \) or through \( LAT_2 \) (\( LAT_1 \)) by randomly choosing either the rectilinear basis \( (|0\rangle, |1\rangle) \) or diagonal basis \( (|+\rangle, |−\rangle) \). In this way, after the measurements, both \( LAT_1 \) and \( LAT_2 \) exclude at least one of the four possible states and generate an eliminated signature for the sequence. e.g., if the measurement result is \( |0\rangle \) then the participant must have never sent \( |1\rangle \). So, \( LAT_1 \) and \( LAT_2 \) do not know the states sent by \( P_i \) in the sequence \( S_1 \), \( S_2 \), but are sure of at least one state that \( P_i \) must not have sent for every element present in the sequence \( S_1 \), \( S_2 \). The eliminated signature (see Table 1) will serve as the quantum digital signature for the participant \( P_i \) to be used in the ticketing phase. These signatures are called as eliminated signatures as the receiver excludes the possibility of states sent by the sender.

Similarly, unconditionally secure digital signatures are generated for every participant \( P_i \). The registration phase in only meant for the generation of signatures for every participant that will be used in the next phase for the authentication of the participants before the generation of the tickets.
Table 1  Table for generation of eliminated signatures

| $P_i$ state | LAT1/2 Measurement basis | Measurement outcome | Eliminated signature |
|-------------|---------------------------|---------------------|---------------------|
| $|0\rangle$ | $\{ |0\rangle, |1\rangle \}$ | $|0\rangle$ | $|1\rangle$ |
| $|0\rangle$ | $\{ |+\rangle, |−\rangle \}$ | $|+\rangle$ | $|−\rangle$ |
| $|1\rangle$ | $\{ |0\rangle, |1\rangle \}$ | $|1\rangle$ | $|0\rangle$ |
| $|1\rangle$ | $\{ |+\rangle, |−\rangle \}$ | $|+\rangle$ | $|−\rangle$ |
| $|+\rangle$ | $\{ |0\rangle, |1\rangle \}$ | $|0\rangle$ | $|1\rangle$ |
| $|+\rangle$ | $\{ |+\rangle, |−\rangle \}$ | $|+\rangle$ | $|−\rangle$ |
| $|−\rangle$ | $\{ |0\rangle, |1\rangle \}$ | $|0\rangle$ | $|1\rangle$ |
| $|−\rangle$ | $\{ |+\rangle, |−\rangle \}$ | $|−\rangle$ | $|+\rangle$ |

3.1.2 Ticketing phase

In this phase, lottery ticket numbers are generated by every participant. The steps involved in this phase are as follows:

Step 1  Participant $P_i$ will first send the $PID$ to both $LAT1$ and $LAT2$. After that, $P_i$ will reveal the states sent by him corresponding to the BB84 sequence ($S_1, S_2$) used in the registration stage.

Step 2  Both $LAT1$ and $LAT2$ will then match the set of states ($S_1, S_2$) revealed by $P_i$ with the corresponding eliminated signatures for every position. e.g. if $P_i$ has revealed the state $|0\rangle$ present at $j$th position of the sequence ($S_1, S_2$), then $|0\rangle$ should not be present in the eliminated signature as recorded by $LAT1$ and $LAT2$ for the $j$th position. If the number of mismatches as recorded by either of $LAT1$ and $LAT2$ is greater than a threshold limit, then the participant is not allowed to take part further. $P_i$ is allowed to participate only if he is authenticated by both $LAT1$ and $LAT2$.

Step 3  $P_i$ will use any of the experimentally available BB84-based QKD protocol to generate two keys, namely $K_{LAT1}^{P_i}$ and $K_{LAT2}^{P_i}$ corresponding to $LAT1$ and $LAT2$.

Step 4  $P_i$ will then generate a random 256-bit unique ticket ($TID_i$) via use of QRNG. These $TID_i$s will be used for the draw of lots. Also, the hash value of the $TID_i$ will be generated and publicly announced. The generation of $TID_i$ by the participant will prevent any kind of manipulation by the lottery authority during ticket allocation phase. Further, the public announcement of hash of $TID_i$ precludes any forging of the lottery ticket after the reward have been announced. Here, it is to be mentioned that any adversary can use the dictionary attack in which the publicly announced hash value of $TID_i$ can be compared with the pre-calculated hash value of all possible 256 bit $TID$s. But, such an attack is computationally impossible. Further, there are other possible attacks.
too on the hash functions [48–53], but still all of them are computationally intensive.

Step 5 \( P_i \) sends the \( TID_i \) to both \( LAT1 \) and \( LAT2 \) using the key \( K_{Pi} = K_{LAT1}^{LAT1} \oplus K_{LAT2}^{LAT2} \) (XOR of the keys \( K_{Pi}^{LAT1} \) and \( K_{Pi}^{LAT2} \)). So data sent to \( LAT1 \) and \( LAT2 \) is basically \( TID_i \oplus K_{Pi} \). In this way, the \( TID_i \) sent by \( P_i \) can be opened only if \( LAT1 \) and \( LAT2 \) cooperate with each other. As an alternative, \( P_i \) can use any other experimentally available quantum secret sharing protocol using BB84 states [54, 55] to send the \( TID_i \) to \( LAT1 \) and \( LAT2 \).

The same procedure will be repeated by every participant \( P_i \) to send the correspondingly generated \( TID_i \) to the \( LAT1 \) and \( LAT2 \). No lottery tickets will be accepted after the closing of the phase.

### 3.1.3 Rewards phase

The steps involved in this phase are as follows:

**Step 1** \( LAT1 \) and \( LAT2 \) cooperate with each other to open the tickets \( TID_i \).

**Step 2** The winning ticket is announced as the bit wise XOR of all the received \( TID_i \)s. i.e., \( T^W = \oplus TID_i \). In this way, the winning ticket is a true random function of all the eligible \( TID_i \)s.

**Step 3** The reward for every participant is calculated as proportional to the Hamming distance of the participants’ ticket (\( TID_i \)) from the winning ticket (\( T^W \)). Hamming distance between two strings basically corresponds to the number of positions in which two strings are different. For bit strings, it corresponds to the number of 1’s present in the XOR of the two strings. In the proposed scheme, there is finite possibility that two or more participants have the same \( TID_i \). For such an event, the rewards can be distributed equally to all participants having the winning ticket, but for most of the cases the specific scheme for the calculation of rewards will depend upon the particular application of the lottery scheme.

In this phase, our main focus is to just propose a method for generation of the winning ticket rather than commenting on a particular method for distribution of the rewards. The allocation of rewards will depend upon the application of lottery scheme and is thus left open to the potential users to develop their own methods. Further, such methods only constitute as a part of the post-processing techniques.

Before, moving to the next lottery scheme, let us just briefly describe the physical implementation of the above mentioned scheme. Figure 2 shows the schematic of the resource requirements for the participants and the lottery authority to implement the BB84-based lottery scheme. We can see that the resource requirements at both the ends are symmetric in nature. Both of them require a QRNG to perform certain steps in the protocol and more so with respect to generation of \( TID_i \)s and \( PID_i \)s. As mentioned before, currently there are a wide variety of commercial QRNGs in the market, though the cost is a bit on the higher end. To reduce cost, the participants may use pseudo random number generators (PRNGs) which pass NIST test [56] but that may lead to a compromise with the security aspects. Other than QRNG, both
of them require set-up for the generation and the measurement of BB84 states. The current optical technology is quite mature enough to generate and measure BB84 states with very high fidelity. For photonics-based implementation, the qubits are encoded in the polarization states of the single photon with horizontal, vertical, $45^\circ$ or $-45^\circ$ respectively corresponding to the states $|0\rangle$, $|1\rangle$, $|+\rangle$ and $|−\rangle$ [45]. These BB84 states are used for both the authentication of the participants as well as sending of the $TID_i$s from the participants to the lottery authority. Further, the participants and lottery authority are connected to each other via bi-directional quantum as well as the classical authenticated channel. Current technology now allows us to send qubits from one party to another through free space communication as well as via use of optical fibres. So, the proposed lottery scheme seems feasible to be implemented via the use of currently available technology.

### 3.2 Entanglement-based quantum lottery scheme

Till now, we have proposed a lottery scheme based on BB84 states, but this is not the only quantum system that can used. In fact, we already know that for quantum cryptography, there are many entanglement-based protocols [31–33]. The use of entanglement brings altogether new features such as device independence [27, 57, 58]. i.e. we need not trust the devices used for the implementation. Similar to the use of entanglement in cryptography, here we will propose a lottery scheme by exploiting the feature of entanglement that can be found only in quantum systems. It is to be mentioned that quantum entanglement is a very costly resource which is very difficult to maintain. So, we will try to minimize the use of quantum entanglement in the proposed scheme. We will keep the registration phase and rewards phase same as that used in the already discussed scheme while using the entanglement only in the ticketing phase using schemes similar to that of quantum secret sharing [59–62].
This is done with the motivation that ticketing is the most important phase where tickets are generated by the participants and are sent to the lottery authority. The proposed scheme makes use of the Bell state $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle)$ and single qubit local unitary operators, namely $U_0 = |0\rangle\langle 0| + |1\rangle\langle 1|$, $U_1 = |0\rangle\langle 0| - |1\rangle\langle 1|$, $U_2 = |1\rangle\langle 0| + |0\rangle\langle 1|$, $U_3 = |0\rangle\langle 1| - |1\rangle\langle 0|$. In principle, the scheme can use any of the four Bell states $(|\psi^\pm\rangle, |\phi^\pm\rangle)^1$ but we will use only $|\psi^-\rangle$ in the scheme. The application of above single qubits operator transforms the Bell state $(|\psi^-\rangle)$ as follows: $U_0|\psi^-\rangle = |\psi^-\rangle$, $U_1|\psi^-\rangle = |\psi^+\rangle$, $U_2|\psi^-\rangle = |\phi^+\rangle$, $U_3|\psi^-\rangle = |\phi^-\rangle$. Further, the scheme will make use of the entanglement swapping for two Bell states [63, 64]. The steps involved in the ticketing phase while implementing entanglement-based lottery scheme are as follows:

Step 1 same as that of Sect. 3.1.2
Step 2 same as that of Sect. 3.1.2

Step 3 $P_i$ will prepare 256 pair of Bell states $|\psi^-\rangle$ and stores the first qubit of all 256 pairs with him. The sequence of second qubits of one set of 256 Bell states is sent to $LAT1$ while the sequence of second qubits of the other set of 256 Bell states is sent to $LAT2$. So, $P_i$ shares 256 Bell states with $LAT1$ (Set I) and another 256 Bell states with $LAT2$ (Set II). The combined state of $P_i$, $LAT1$ and $LAT2$ can be written as $[|\psi^-\rangle^1 \otimes |\psi^-\rangle^2 \otimes \cdots \otimes |\psi^-\rangle^{256}]_{LAT1} \otimes [|\psi^-\rangle^1 \otimes |\psi^-\rangle^2 \otimes \cdots \otimes |\psi^-\rangle^{256}]_{LAT2}$ (tensor product of 256 pair of Bell states shared between $P_i$ and $LAT1$ and 256 pair of Bell states shared between $P_i$ and $LAT2$).

Step 4 $P_i$ randomly picks half of his qubits, then choose to measure them either in the computational basis ($|0\rangle, |1\rangle$) or Hadamard basis ($|+\rangle, |-\rangle$) and publicly announce the basis used for measurement of his qubits. $LAT1$ and $LAT2$ will use the same basis as announced by $P_i$ to measure their corresponding qubits. If there is no adversary during the transmission phase, then the measurement outcomes of $P_i$ will be opposite to that of $LAT1$. E.g. If $P_i$ gets $|0\rangle$ ($|1\rangle$) then $LAT1$ will get $|1\rangle$ ($|0\rangle$) while if $P_i$ gets $|+\rangle$ ($|-\rangle$) then $LAT1$ will get $|-\rangle$ ($|+\rangle$). Similar is the case for measurement outcomes of $P_i$ and $LAT2$. If the error is below the threshold limit, then they proceed to next step else they abort the protocol. Further, they will rearrange the qubits to have the combined state as $[|\psi^-\rangle^1 \otimes |\psi^-\rangle^2 \otimes \cdots \otimes |\psi^-\rangle^{128}]_{LAT1} \otimes [|\psi^-\rangle^1 \otimes |\psi^-\rangle^2 \otimes \cdots \otimes |\psi^-\rangle^{128}]_{LAT2}$.

Step 5 $P_i$ will choose one qubit from Set I and another qubit from Set II. Further, $P_i$ will randomly choose one of the above qubits to apply any one of the operators $U_0, U_1, U_2, U_3$ to encode the bits 00, 01, 10, 11 respectively (see Table 2). $P_i$ will then perform a Bell measurement on the two qubits and then publicly announce the outcome. The same operation is performed for all the qubits of $P_i$ by taking one qubit from Set I while other from Set II. In this way, $P_i$ will send the encoded 256 bit $TID_i$ to $LAT1$ and $LAT2$. Further, the hash of the $TID_i$ is publicly announced.

---

1 $|\psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$ and $|\phi^\pm\rangle = \frac{1}{\sqrt{2}}(|00\rangle \pm |11\rangle)$
Table 2 Table of encoding using Bell state and entanglement swapping

| $P_i$ encoding | $P_j$ Operation | Initial state | Final state after entanglement swapping |
|----------------|----------------|---------------|----------------------------------------|
| 00             | $U_0 = |0\rangle\langle0| + |1\rangle\langle1|$ | $U_0|\psi^-\rangle_{LAT1}|\psi^-\rangle_{LAT2}$ = $\frac{1}{2}(|\psi^-\rangle_{P_j} |\psi^-\rangle_{LAT1} + |\phi^+\rangle_{P_j} |\phi^+\rangle_{LAT1} - |\psi^-\rangle_{P_j} |\psi^-\rangle_{LAT2} - |\phi^-\rangle_{P_j} |\phi^-\rangle_{LAT2})$ |
| 01             | $U_1 = |0\rangle\langle0| - |1\rangle\langle1|$ | $U_1|\psi^-\rangle_{LAT1}|\psi^-\rangle_{LAT2}$ = $\frac{1}{2}(|\psi^-\rangle_{P_j} |\psi^-\rangle_{LAT1} - |\psi^-\rangle_{P_j} |\psi^-\rangle_{LAT2} + |\phi^+\rangle_{P_j} |\phi^+\rangle_{LAT1} - |\phi^-\rangle_{P_j} |\phi^-\rangle_{LAT2})$ |
| 10             | $U_2 = |1\rangle\langle0| + |0\rangle\langle1|$ | $U_2|\psi^-\rangle_{LAT1}|\psi^-\rangle_{LAT2}$ = $\frac{1}{2}(|\phi^-\rangle_{P_j} |\psi^+\rangle_{LAT1} - |\psi^-\rangle_{P_j} |\psi^-\rangle_{LAT2} + |\phi^+\rangle_{P_j} |\phi^-\rangle_{LAT1} - |\phi^-\rangle_{P_j} |\phi^+\rangle_{LAT2})$ |
| 11             | $U_3 = |0\rangle\langle1| - |1\rangle\langle0|$ | $U_3|\psi^-\rangle_{LAT1}|\psi^-\rangle_{LAT2}$ = $\frac{1}{2}(|\phi^+\rangle_{P_j} |\psi^+\rangle_{LAT1} + |\phi^-\rangle_{P_j} |\psi^-\rangle_{LAT2} - |\psi^+\rangle_{P_j} |\psi^-\rangle_{LAT1} - |\psi^-\rangle_{P_j} |\phi^+\rangle_{LAT2})$ |
Step 6   \( \text{LAT}1 \) and \( \text{LAT}2 \) can cooperate with each other (see Table 2) to get the \( TID_i \) sent by \( P_i \) after performing the necessary joint Bell measurements of their respective qubits and the properties of entanglement swapping.

In this way, all the \( P_i \)'s will send their \( TID_i \)'s to the \( LA \) and the \( TID_i \)'s can be opened only if both the \( \text{LAT}1 \) and \( \text{LAT}2 \) cooperate with each other. So, entanglement-based lottery scheme differs from that of BB84-based scheme only in the method adopted to send the ticketing numbers \( (TID_i) \)s from participants to the lottery authority. The advantage of using entanglement is just to provide an additional level of security.

Let us now briefly describe the physical implementation of the proposed scheme. Figure 3 shows the schematic of the resource requirements for participants and the lottery authority to implement the entanglement-based lottery scheme. In contrast to the BB84-based scheme, the resource requirements here are not symmetric with respect to the participants and the lottery authority except the use of QRNGs at both the ends. As mentioned before, in this scheme too authentication of the participants is done via the use of BB84-based digital signature scheme. But for its implementation, only the BB84 state generation set-up is required at the participants end while the BB84 state measurement set-up is required by the lottery authority. Further, the \( TID_i \)'s are sent from participants to the lottery authority via encoding the \( TID_i \)'s into the Bell states. So, the Bell state generation set-up is required by the participants while Bell state measurement set-up is required by lottery authority. Similar to the case of BB84-based scheme, participants and the lottery authority are connected to each other via a quantum channel and classical authenticated channel. As far as current technology is concerned, the proposed scheme can be physically implemented, but certainly the use of fragile resources such as entanglement will come at a very heavy cost. In the next section, we will propose a scheme to minimize the cost by allowing...
all participants to use classical resources, while only lottery authority having access to quantum resources.

3.3 Semi-quantum lottery scheme

In the previous two proposed schemes, all the participants need to have the quantum capabilities. However, in the realistic situations the quantum resources are extremely costly and difficult to maintain. In fact, entanglement is a very fragile resource too. In order to overcome these limitations, Boyer et al. [65] in 2007 proposed a semi-quantum scheme of quantum key distribution, in which only one party has full quantum abilities but the other party is classical. The classical party can either reflect back the qubits or can measure the incoming qubits in the computational basis ($|0\rangle$, $|1\rangle$) only. Since then, various semi-quantum protocols have been proposed in quantum cryptography [66–68] and related areas. As far a current scenario is concerned, infrastructure for classical communication systems is very well developed and is available at a very reasonable cost. But in contrast, the quantum resources such as creation and manipulation of quantum states, quantum entanglement are too costly and difficult to handle. So, the current situation demands the development of schemes in which only few nodes have full quantum capabilities while the rest of the nodes can make of use only classical resources. Such schemes are known as semi-quantum schemes, and those schemes are relevant as they can exploit advantages of the currently available classical infrastructure. Taking the above motivation, we will now present a semi-quantum lottery scheme in which lottery authority will have full quantum capability, but all the participants will have only classical abilities. The proposed semi-quantum lottery scheme is further shown to be equally good in comparison with their quantum counterparts. Let us now describe in detail the semi-quantum scheme for lottery.

3.3.1 Registration phase

Step 1 same as that of Sect. 3.1.1
Step 2 same as that of Sect. 3.1.1
Step 3 For the generation of digital signatures, $LAR$ will prepare $n$ qubits in the state $|+\rangle$ and send it to $P_i$ one by one. The participant $P_i$ can either measure the incoming qubit in the computational basis ($|0\rangle$, $|1\rangle$) or let it go as it is to $LAT_1$.
Step 4 $LAT_1$ will randomly choose to measure the qubit in either computational basis ($|0\rangle$, $|1\rangle$) or Hadamard basis ($|+\rangle$, $|−\rangle$) and note the outcome. After performing the measurement, resultant qubit is sent to the participant $P_i$.
Step 5 The participant $P_i$ will perform exactly the same operation as done by him in Step 3 (i.e., either pass the qubit or measure in computational basis) on incoming qubit from $LAT_1$ and send it to $LAT_2$.
Step 6 Similar to $LAT_1$, $LAT_2$ will also randomly choose either computational basis ($|0\rangle$, $|1\rangle$) or Hadamard basis ($|+\rangle$, $|−\rangle$) to measure the qubit and note the outcome.
Step 7 $LAT_1$ and $LAT_2$ will announce the basis used by them to measure each of the $n$ qubits received by them. Further, they will keep only those outcomes in
which they have used the same basis and discard the rest. These outcomes will be used by \( \text{LAT}_1 \) and \( \text{LAT}_2 \) to verify the participant in the ticketing phase.

### 3.3.2 Ticketing phase

**Step 1** Participant \( P_i \) will first send the \( P\text{ID}_i \) to \( \text{LAT}_1 \) and \( \text{LAT}_2 \). After that, \( P_i \) will publicly announce the operation performed by him on all \( n \) qubits, whether he has allowed the qubit to pass to \( \text{LAT}_1 \) and \( \text{LAT}_2 \) or measured in the computational basis before sending them to \( \text{LAT}_1 \) and \( \text{LAT}_2 \).

**Step 2** Both \( \text{LAT}_1 \) and \( \text{LAT}_2 \) will then match the outcomes of their measurement for the cases in which participant \( P_i \) has not measured the qubit before passing it to them. For such cases, the outcome recorded by \( \text{LAT}_1 \) and \( \text{LAT}_2 \) will match with each other. If the number of mismatches is greater than a threshold limit, then the participant is not allowed to take part further. \( P_i \) is allowed to participate only if he is authenticated by \( \text{LAT}_1 \) and \( \text{LAT}_2 \).

**Step 3** \( P_i \) will use the semi-quantum QKD scheme using BB84 protocol given by Boyer et al. [65] or any other semi-quantum QKD protocol to generate two keys namely \( K^L_{\text{LAT}_1} \) and \( K^L_{\text{LAT}_2} \) corresponding to \( \text{LAT}_1 \) and \( \text{LAT}_2 \).

**Step 4** same as that of Sect. 3.1.2

**Step 5** \( P_i \) sends the \( \text{TID}_i \) to both \( \text{LAT}_1 \) and \( \text{LAT}_2 \) using the key \( K_{P_i} = K^L_{\text{LAT}_1} \oplus K^L_{\text{LAT}_2} \) (XOR of the keys \( K^L_{\text{LAT}_1} \) and \( K^L_{\text{LAT}_2} \)) or via use of any other semi-quantum quantum secret sharing protocol. In this way, the \( \text{TID} \) sent by \( P_i \) can be opened only if \( \text{LAT}_1 \) and \( \text{LAT}_2 \) cooperate with each other.

### 3.3.3 Rewards phase

Same as that of Sect. 3.1.3

So, we can see that the lottery scheme can be implemented using the lesser resources in comparison to that of full quantum lottery schemes. It is to be mentioned here that the above lottery scheme is also a BB84 state-based scheme, but this allows the users to have only classical resources with only lottery authority having full quantum capabilities. Figure 4 describes the schematic of the resource requirements for participants and lottery authority to implement the protocol. We can clearly see that, except for the QRNG (required for performing certain steps), participants just need to have access to quantum channel coming out from the lottery authority. After receiving the qubits from the lottery authority, the participants just need a set-up for measurement of the incoming qubits in the computational basis (\(|0\rangle, |1\rangle\)). Also, they can allow the qubits to be returned back to lottery authority as it is without any modification. Further, to reduce the costs the participants may use PRNGs which passes the NIST tests, but at the cost of security. Looking at the lottery authority, they require quantum resources such as QRNG, BB84 states generation as well as measurement set-up. With the current advancements of technology, the proposed protocol can be implemented with the currently available hardware.
So far we have proposed three protocols for lottery, which can be realized using different amount (and type) of quantum resources. Further, we have shown that the proposed theoretical schemes can be implemented using the currently available hardware. However, the security of the protocols is not discussed in detail until now. Consequently, it will be apt to perform security analysis of the proposed lottery schemes in the next section.

4 Security analysis

The proposed schemes conform to the requirements of a good lottery scheme as described in Sect. 2. Also, in all the proposed schemes, we can see that the tickets are generated by the participants and the lottery authority only collects the generated TIDs which are then further used for deciding the rewards. In this section, we will first look at the security aspects of the BB84 and entanglement-based schemes (henceforth referred to as Type I scheme) and then look at the security of semi-quantum schemes (henceforth referred to as Type II scheme). It is important to note that in this work we have tried to look at the security analysis in a qualitative manner rather than specifying the quantitative bounds on the level of security with respect to the different parameters as the idea of the work is to introduce the use of quantum and semi-quantum schemes for enhancing the security of lottery schemes. A detailed and thorough mathematical analysis of the security bounds will be provided in future works.

For the Type I scheme, we can see that the registration phase and rewards phase is the same for both BB84 and entanglement-based scheme with differences arising only in the ticketing phase. Let us first look at the security aspects of the registration phase. In this phase, the participants \( (P_i) \) get themselves registered with the lottery authority \( (LA) \) and each participant \( P_i \) receives a \( PID_i \) for maintaining his/her privacy.
Then, every $P_i$ generates a digital signature with $LA$ by the use of unconditionally secure BB84-based digital signature scheme. These digital signatures are used for the authentication of the eligible participants and only eligible participants are allowed to generate the tickets and take part further in the process. Authentication is perhaps one of the most important aspects of any communication system as an eavesdropper can become a legitimate participant in the absence of a secure authentication scheme. So, the Type I lottery scheme has tried to make use of quantum states in order to enhance the security of the authentication process by generating unconditionally secure digital signatures for every participant. We will not go into the details of the security proofs of generated digital signatures as the unconditional security of the BB84-based digital signature scheme against any potential Eve has already been proven by Wallden et al. [47] in which they have shown that the probability of forging as well as repudiation decreases exponentially with increase in the length of the digital signature. In this way, only legitimate registered users can take part in the ticketing process where $TID_i$s are generated. So, the eligibility condition is satisfied. It is here to be mentioned that, it may sometimes be possible for an Eve to get the $PID_i$ of the participant $P_i$. If Eve is able to get the $PID_i$ after the participant has generated the digital signature, then that $PID_i$ will be of no use as the digital signature cannot be created again and Eve has no information about the digital signature created by the legitimate party. In case, Eve gets hold of the $PID_i$ before the legitimate party has created the digital signature, then Eve can impersonate the legitimate party and can take part in the whole process as the legitimate party may have done. But, Eve will not be able to control the outcome of the lottery as per his wishes because for that he has to get hold of $PID_i$’s of all the participants. In an ideal scenario, even the $PID$s need to be sent by $LA$ to all the participants using unconditionally secure quantum cryptographic protocols. But that will lead to an increase in the cost, so we have decided that $PID$s can be sent by using classical secure public key cryptosystems. From the above discussion, we can see that even after getting hold of some $PID_i$s Eve will not be able to control the outcome of rewards as for that one has to break the unconditionally secure digital signature of the participants. Now if we look at the condition of equi-probability, then we can see that the winning ticket ($T^W$) is announced by taking the bitwise XOR of all the valid $TID_i$s. So every $TID_i$ has an equal probability to win. Further, no one including the lottery authority will be able to predict the winning ticket beforehand until and unless one gets hold of all the $TID_i$s. So, all the participants have an equal chance of getting the winning ticket. In fact, the equi-probability condition is always satisfied irrespective of the number of participants.

Now, let us look at the security of transmission of the $TID_i$s from the $P_i$ to $LA$. In the proposed lottery scheme using BB84 states, the $TID_i$s are sent by the participants to the lottery authority using the unconditionally secure experimentally feasible BB84 protocol. Here, it is important to mention that the BB84 protocol [14] was in fact the first quantum cryptography protocol proposed to provide unconditional security for the transmission of data. The unconditional security of BB84 protocol was mathematically proven [69] by Shor and Preskil. The field of secure transmission using BB84 protocol and its different variants have grown such that there now are commercially available products, too [32, 33]. In fact, QKD using BB84 protocol has been demonstrated over a distance of 1200 KM via use of satellite [70]. In the proposed scheme, the $TID_i$s
are first generated by the participants and then sent to the lottery authority via the use of keys generated by use of BB84 protocol, so it is practically impossible for any adversary to manipulate, change or get hold of the $TID_i$s. Further, the $TID_i$s are sent by $P_i$ to $LAT_1$ and $LAT_2$ using the key $K_{P_i}^{LAT_1} \oplus K_{P_i}^{LAT_2}$, which is made up of XOR of individual key generated between $P_i$ and $LAT_1$ and $P_i$ and $LAT_1$. So, the $TID_i$s sent by the participant $P_i$ can be opened only if $LAT_1$ and $LAT_2$ cooperate with each other. In this way, all the members of $LA$ have to cooperate with each other in order to get hold of all the $TID_i$s. For the case of Type I entanglement-based lottery scheme, the $TID_i$s are sent by $P_i$ to $LA$ via the use of protocol akin to Quantum Secret Sharing (QSS) protocol. Here, $P_i$ shares 256 pair of entangled Bell states with $LAT_1$ and $LAT_2$. The presence of Eve is detected via the use of half of the entangled Bell states by randomly measuring the states either in the computational basis ($|0\rangle$, $|1\rangle$) or Hadamard basis ($|+\rangle$, $|-\rangle$) and then publicly announcing the basis used for measurement of his qubits. The presence of Eve will be reflected in the breaking of correlations between the measurements when the same basis is used. Once the channel is certified to be free from the presence of Eve (errors are lesser than some threshold value), then only the $P_i$ will encode the $TID_i$ by application of appropriate unitary operators on the rest of Bell states. The $TID_i$ is sent to $LA$ by use of entanglement swapping (as shown in Table 2) and the $TID_i$ can be opened only if $LAT_1$ and $LAT_2$ cooperate with each other. The security of $TID_i$ is hence based on the nonlocal properties of Bell states. So, we can see that in the Type I scheme, the $TID_i$s are sent from the $P_i$ to $LA$ in a secure manner by making sure that the channel is secure. For BB84-based scheme, the security is based on uncertainty principle and no-cloning theorem, while the security of entanglement-based scheme depends on nonlocal properties of Bell states.

Now, let us look at the binding property for Type I schemes. The binding property of $TID_i$s is implemented using the classical hash function. It is here important to mention that the impossibility of unconditionally secure quantum bit commitment protocol has already been proved [71, 72], so we have proposed to implement the binding property of lottery tickets by use of computationally secure hash functions only. Here, every participant $P_i$ publicly announces the hash value of their $TID_i$ before being sent to the lottery authority. This is done to prevent the participant to claim a different $TID_i$ once the rewards have been announced. Under the semi-honest assumption of lottery authority, any mismatch in the hash of $TID$’s will be attributed to cheating on part of participant. So, the Type I lottery schemes are unconditionally secure while sending of the $TID_i$s but the binding property of the $TID_i$s via hash function makes it only computationally secure as an adversary can perform the dictionary attack. In this attack, an adversary can compute the hash of all the $TID_i$s before hand and then via the mapping of the $TID_i$ with their hash value the adversary can get hold of all the transmitted $TID_i$. But since one is using 256 bit $TID_i$ so it is computationally not feasible for the current set of computers to do a mapping of all possible $TID_i$s with their hash value. Further, other different attacks are also possible on hash functions [48–53], which makes the binding nature of $TID_i$ by the participant only computationally secure. In fact, unconditional security of any quantum bit commitment scheme is shown to be impossible [71, 72]. Now the Type I scheme is verifiable as after the announcement of the winning ticket, every participant can announce their $TID_i$ which can be used to
verify the outcome of the lottery. Further, any malicious participant cannot change his ticket after the announcement of the winning ticket as every participant has announced the hash value of their $TID_i$ before being sent to the lottery authority. So, to conclude, the proposed Type I lottery schemes satisfy all the requirements to be considered as good schemes.

Let us now look at the security aspects of semi-quantum lottery scheme. The semi-quantum lottery scheme (Type II) differs from the Type I schemes in terms of resources as in the Type II scheme only lottery authority needs quantum resources while the participants can be classical only. Due to this, the registration phase in which digital signatures for participants are generated is different from that of Type I scheme. As can be seen from the scheme discussed in the previous section, the participant’s signature is encoded in the form of whether the participant has measured the incoming qubit in the computational basis or let it be passed without any modification. Lottery authority can authenticate the participant when he reveals his choices and $LAT_1$ and $LAT_2$ announce the measurement results. For all the qubits in which participant has passed the qubits, the measurement outcomes of $LAT_1$ and $LAT_2$ will be identical provided they use the same basis for measurement. The uncertainty principle and no-cloning theorem guarantee that any Eve is not able to forge the participant’s signature and the probability to forge the participant’s digital signature decreases exponentially with increase in the length of the digital signature. In this way, only authenticated participants will be allowed to proceed in the ticketing phase. Further, in the ticketing phase the $TIDs$ are sent by participants to lottery authority via the use of semi-quantum QKD protocols. Currently, there are several semi-quantum QKD protocols [65–68] which have already been proved to be unconditionally secure and have been experimentally tested. So, the $TIDs$ generated by the eligible participants can be unconditionally shared to lottery authority where the $TIDs$ can be opened only if all the members of lottery authority cooperate with each other. Similar to the Type I schemes, here also the binding property of lottery tickets is via the use of hash functions. Further, the winning ticket can be verified if all the participants cooperate with each other. So, the semi-quantum lottery scheme also satisfies the requirements of a good lottery scheme.

5 Conclusion

The Nature is quantum mechanical and the quantum mechanical world is probabilistic in nature. In short, quantum mechanics is a probabilistic theory and in our daily life we often come across situations that can be best realized within the framework of a probabilistic theory (not essentially quantum mechanics). Lottery is one such phenomenon which can be appropriately realized only in the framework of a probabilistic theory. It’s possible to design schemes of lottery in any non-classical probabilistic theory. However, without going into the details of the generalized probability theory (GPT) [71, 72] and the specific toy theories which can support secure lottery schemes, here we have restricted ourselves to quantum mechanics and have provided three specific schemes for lottery. These schemes require different type of quantum resources. To be precise, in contrast to the entanglement-based scheme proposed above, the other two schemes, i.e., BB84 state-based scheme and semi-quantum schemes can be realized.
using separable states or more appropriately using single photon states. In fact, these two single-photon-based (or equivalently BB84 state based) schemes do not require entanglement and non-locality, and thus such schemes can also be realized in a non-classical toy theory [73] which has only the feature of uncertainty relations between incompatible observables. This is similar to the availability of a wide variety of practical QKD systems [32, 33] and quantum random number generators [36, 38] with different levels of security aspects. The unconditional security can be derived from the use of only ‘incompatibility and uncertainty’ feature of quantum mechanics, but the device independence security can be derived only through the use of features such as ‘entanglement’ and ‘non-locality’.

In this work, we have highlighted the importance of lottery in many important works of life and have noted that despite its existence from the days of early civilization there is no fair and secure scheme for lottery. In fact, current implementations of the schemes for lottery are not fully secure. Further, we identified the requirements for a scheme to be considered as a good scheme for lottery. The gap is addressed here by designing a set of secure schemes for lottery and establishing their security. We analysed the resource requirements of the three proposed scheme, and have shown that these schemes, can be implemented using the available devices. We hope that this study will help in providing physical insights towards the development of commercial quantum lottery solutions.

Acknowledgements Authors thank Kishore Thapliyal and Abhishek Parakh for their feedback and interest in this work. Further, the authors acknowledge that this study is supported by the project “Partnership 2020: Leveraging US-India Cooperation in Higher Education to Harness Economic Opportunities and Innovation” which is enabling a collaboration between University of Nebraska at Omaha, and JIIT, Noida.

Data availability Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

Declaration

Conflict of interest The authors state that they have not known competing financial interests or personal connections that may seem to have influenced the work described in this study.

References

1. Blanche, E.E.: Lotteries yesterday, today, and tomorrow. Ann. Am. Acad. Polit. Soc. Sci. 269(1), 71–76 (1950)
2. Rubner, A.: The Economics of Gambling. Macmillan, London (1966)
3. Ball, P.S.: Gambling in Elizabethan England: perspectives on England’s ‘Lotterie Generall’ of 1567–69. Ph.D. thesis, University of Tasmania (2018)
4. Boyce, J.R.: Allocation of goods by lottery. Econ. Inquiry 32(3), 457–476 (1994)
5. Shaddy, F., Shah, A.K.: When to use markets, lines, and lotteries: how beliefs about preferences shape beliefs about allocation. J. Mark. 86(3), 140–156 (2021)
6. Stone, P.: Why lotteries are just. J. Polit. Philos. 15(3), 276–295 (2007)
7. Saunders, B.: The equality of lotteries. Philosophy 83(3), 359–372 (2008)
8. Eckhoff, T.: Lotteries in allocative situations. Soc. Sci. Inf. 28(1), 5–22 (1989)
9. Waldspurger, C.A.: Lottery and stride scheduling: flexible proportional-share resource management. Ph.D. thesis, Massachusetts Institute of Technology (1995)
10. Frankle, J., Carbin, M.: The lottery ticket hypothesis: finding sparse, trainable neural networks. In: International Conference on Learning Representations (2019)
11. Liu, M., Choy, V., Clarke, P., Barnett, A., Blakely, T., Pomeroy, L.: The acceptability of using a lottery to allocate research funding: a survey of applicants. Res. Integr. Peer Rev. 5, 3 (2020)
12. Fang, F.C., Casadevall, A.: Grant funding: playing the odds. Science 352(6282), 158–158 (2016)
13. Adam, D.: Science funders gamble on grant lotteries. Nature 575(7785), 574–575 (2019)
14. Charles, H.B., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: International Conference on Computer System and Signal Processing, Vol. 1984, pp. 175–179. IEEE (1984)
15. Shenoy-Hejamadi, A., Pathak, A., Radhakrishna, S.: Quantum cryptography: key distribution and beyond. Quanta 6(1), 1–47 (2017)
16. Gisin, N., Ribordy, G., Titel, W., Zbinden, H.: Quantum cryptography. Rev. Mod. Phys. 74(1), 145–195 (2002)
17. Feihu, X., Ma, X., Zhang, Q., Lo, H.-K., Pan, J.-W.: Secure quantum key distribution with realistic devices. Rev. Mod. Phys. 92(2), 025002 (2020)
18. Brassard, G., Crépeau, C., Jozsa, R., Langlois, D.: A quantum bit commitment scheme provably unbreakable by both parties. In: Proceedings of 1993 IEEE 34th Annual Foundations of Computer Science, pp 362–371. IEEE (1993)
19. Hoi-Kwong, L., Chau, H.F.: Is quantum bit commitment really possible? Phys. Rev. Lett. 78(17), 3410–3413 (1997)
20. Mayers, D.: Unconditionally secure quantum bit commitment is impossible. Phys. Rev. Lett. 78(17), 3414–3417 (1997)
21. Naseri, M.: Secure quantum sealed-bid auction. Opt. Commun. 282(9), 1939–1943 (2009)
22. Hogg, T., Harsha, P., Chen, K.-Y.: Quantum auctions. Int. J. Quantum Inf. 5(05), 751–780 (2007)
23. Hillery, M., Ziman, M., Bužek, V., Bieliková, M.: Towards quantum-based privacy and voting. Phys. Lett. A 349(1–4), 75–81 (2006)
24. Vaccaro, J.A., Spring, J., Cheffles, A.: Quantum protocols for anonymous voting and surveying. Phys. Rev. A 75(1), 012333 (2007)
25. Thapliyal, K., Sharma, R.D., Pathak, A.: Protocols for quantum binary voting. Int. J. Quantum Inf. 15(01), 1750007 (2017)
26. Mishra, S., Thapliyal, K., Parakh, A., Pathak, A.: Quantum anonymous veto: a set of new protocols. EJP Quantum Technol. 9(1), 14 (2022)
27. Colbeck, R.: Quantum and relativistic protocols for secure multi-party computation. Ph.D. thesis, University of Cambridge. arXiv:0911.3814 (2009)
28. Danilov, V.I., Lambert-Mogiliansky, A., Vergopoulos, V.: Dynamic consistency of expected utility under non-classical (quantum) uncertainty. Theory Decis. 84(4), 645–670 (2018)
29. Sun, X., Kulicki, P., Sopek, M.: Lottery and auction on quantum blockchain. Entropy 22(12), 1377 (2020)
30. Menezes, A.J., Van Oorschot, P.C., Vanstone, S.A.: Handbook of Applied Cryptography. CRC Press, Boca Raton (2018)
31. Ekert, A.K.: Quantum cryptography based on Bell’s theorem. Phys. Rev. Lett. 67(6), 661–663 (1991)
32. Feihu, X., Ma, X., Zhang, Q., Lo, H.-K., Pan, J.-W.: Secure quantum key distribution with realistic devices. Rev. Mod. Phys. 92(2), 025002 (2020)
33. Pirandola, S., Andersson, U.L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., Englund, D., Gehring, T., Lupo, C., Ottaviani, C., et al.: Advances in quantum cryptography. Adv. Opt. Photonics 12(4), 1012–1236 (2020)
34. Bera, M.N., Acín, A., Kuš, M., et al.: Randomness in quantum mechanics: philosophy, physics and technology. Rep. Prog. Phys. 80(12), 124001 (2017)
35. How to Turn a Quantum Computer Into the Ultimate Randomness Generator | Quanta Magazine, Jun 2019. [Online]. Accessed 28 Feb 2022
36. Mannalath, V., Mishra, S., Pathak, A.: A comprehensive review of quantum random number generators: concepts, classification and the origin of randomness. arXiv:2203.00261 (2022)
37. Jacak, M.M., Jóźwiak, P., Niemczuk, J., Jacak, J.E.: Quantum generators of random numbers. Sci. Rep. 11(1), 16108 (2021)
38. Herrero-Collantes, M., García-Escartin, J.C.: Quantum random number generators. Rev. Mod. Phys. 89(1), 015004 (2017)
39. Ma, X., Yuan, X., Cao, Z., et al.: Quantum random number generation. NPJ Quantum Inf. 2(16021), 1–9 (2016)
40. ID Quantique. Quantis qrng (quantum random number generator)—id quantique. https://www.idquantique.com/random-number-generation/products. Accessed 25 Feb 2022
41. Toshiba. https://www.toshiba.eu/pages/eu/Cambridge-Research-Laboratory/quantum-random-number-generators. Accessed 25 Feb 2022
42. PicoQuant. Quantum random number generator | picoquant. https://www.picoquant.com/scientific/product-studies/pqrng-150-product-study. Accessed 25 Feb 2022
43. MPD. Micro photon devices—quantum random number. http://www.micro-photon-devices.com/Docs/Datasheet/QRNG.pdf. Accessed 25 Feb 2022
44. Nielsen, M.A., Chuang, I.L.: Quantum Computing and Quantum Information. Cambridge University Press, Cambridge (2000)
45. Pathak, A.: Elements of Quantum Computation and Quantum Communication. CRC Press, Boca Raton (2013)
46. Pathak, A., Banerjee, A.: Optical Quantum Information and Quantum Communication. SPIE, Bellingham (2016)
47. Wallden, P., Dunjko, V., Kent, A., Andersson, E.: Quantum digital signatures with quantum-key-distribution components. Phys. Rev. A 91(4), 042304 (2015)
48. Wang, X., Yin, Y.L., Yu, H.: Finding collisions in the full sha-1. In: Annual International Cryptology Conference, pp. 17–36. Springer (2005)
49. Lenstra, A., Wang, X., de Weger, B.: Colliding x. 509 certificates. Cryptology ePrint Archive (2005)
50. Wang, X., Feng, D., Lai, X., Yu, H.: Collisions for hash functions md4, md5, haval-128 and ripemd. Cryptology ePrint Archive (2004)
51. Yu, H., Wang, G., Zhang, G., Wang, X.: The second-preimage attack on md4. In: International Conference on Cryptology and Network Security, pp. 1–12. Springer (2005)
52. Wang, X., Yu, H.: How to break md5 and other hash functions. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 19–35. Springer (2005)
53. Wang, X., Lai, X., Feng, D., Chen, H., Yu, X.: Cryptanalysis of the hash functions md4 and ripemd. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques, pp. 1–18. Springer (2005)
54. Guo, G.-P., Guo, G.-C.: Quantum secret sharing without entanglement. Phys. Lett. A 310(4), 247–251 (2003)
55. Hsu, L.-Y., Li, C.-M.: Quantum secret sharing using product states. Phys. Rev. A 71(2), 022321 (2005)
56. Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Barker, E.: A statistical test suite for random and pseudo-random number generators for cryptographic applications. Technical report, Booz-allen and hamilton inc mclean va (2001)
57. Lo, H.-K., Curty, M., Qi, B.: Measurement-device-independent quantum key distribution. Phys. Rev. Lett. 108(13), 130503 (2012)
58. Yin, H.-L., Chen, T.-Y., Zong-Wen, Yu., Liu, H., You, L.-X., Zhou, Y.-H., Chen, S.-J., Mao, Y., Huang, M.-Q., Zhang, W.-J., et al.: Measurement-device-independent quantum key distribution over a 404 km optical fiber. Phys. Rev. Lett. 117(19), 190501 (2016)
59. Hillery, M., Bužek, V., Berthiaume, A.: Quantum secret sharing. Phys. Rev. A 59(3), 1829 (1999)
60. Zhang, Z., Li, Y., Man, Z.: Multiparty quantum secret sharing. Phys. Rev. A 71(4), 044301 (2005)
61. Xiao, L., Long, G.L., Deng, F.-G., Pan, J.-W.: Efficient multiparty quantum-secret-sharing schemes. Phys. Rev. A 69(5), 052307 (2004)
62. Zhang, Z., Man, Z.: Multiparty quantum secret sharing of classical messages based on entanglement swapping. Phys. Rev. A 72(2), 022303 (2005)
63. Zukowski, M., Zeilinger, A., Horne, M.A., Ekert, A.K.: “Event-ready-detectors” Bell experiment via entanglement swapping. Phys. Rev. Lett. 71(26), 4287–4290 (1993)
64. Ji, Z., Fan, P., Zhang, H.: Entanglement swapping for bell states and Greenberger–Horne–Zeilinger states in qubit systems. Phys. A Stat. Mech. Appl. 585, 126400 (2022)
65. Boyer, M., Kenisberg, D., Mor, T.: Quantum key distribution with classical Bob. Phys. Rev. Lett. 99(14), 140501 (2007)
66. Zou, X., Qiu, D., Li, L., Lihua, W., Li, L.: Semiquantum-key distribution using less than four quantum states. Phys. Rev. A 79(5), 052312 (2009)
67. Kun-Fei, Yu., Yang, C.-W., Liao, C.-H., Hwang, T.: Authenticated semi-quantum key distribution protocol using bell states. Quantum Inf. Process. 13(6), 1457–1465 (2014)
68. Shukla, C., Thapliyal, K., Pathak, A.: Semi-quantum communication: protocols for key agreement, controlled secure direct communication and dialogue. Quantum Inf. Process. 16(12), 1–19 (2017)
69. Shor, P.W., Preskill, J.: Simple proof of security of the BB84 quantum key distribution protocol. Phys. Rev. Lett. 85, 441–444 (2000)
70. Liao, S.-K., Cai, W.-Q., Liu, W.-Y., Zhang, L., Li, Y., Ren, J.-G., Yin, J., Shen, Q., Cao, Y., Li, Z.-P., et al.: Satellite-to-ground quantum key distribution. Nature 549(7670), 43–47 (2017)
71. Janotta, P., Hinrichsen, H.: Generalized probability theories: what determines the structure of quantum theory? J. Phys. A Math. Theor. 47(32), 323001 (2014)
72. Barrett, J.: Information processing in generalized probabilistic theories. Phys. Rev. A 75(3), 032304 (2007)
73. Aravinda, S., Pathak, A., Srikanth, R.: Hierarchical axioms for quantum mechanics. Eur. Phys. J. D 73(9), 207 (2019)

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

Springer Nature or its licensor (e.g. a society or other partner) holds exclusive rights to this article under a publishing agreement with the author(s) or other rightsholder(s); author self-archiving of the accepted manuscript version of this article is solely governed by the terms of such publishing agreement and applicable law.