Quantum Information Processing (2020) 19:349
https://doi.org/10.1007/s11128-020-02861-9

A game-theoretic security framework for quantum cryptography: Performance analysis and application

Songyang Han[1] · Walter O. Krawec[1] · Fei Miao[1]

Received: 27 February 2020 / Accepted: 3 September 2020 / Published online: 22 September 2020
© Springer Science+Business Media, LLC, part of Springer Nature 2020

Abstract
In this paper, we analyze quantum key distribution (QKD) protocols through a game-theoretic framework. In particular, we assume parties and adversaries are "rational." Unlike other game theoretic models, we show how important key-rate and noise tolerance computations may be performed through our system allowing for interesting comparisons to the "standard adversarial model" of QKD. We show that, depending on the relative cost of operating devices, increased noise tolerance and improved secure communication rates are possible if one assumes adversaries are rational as opposed to being malicious.

Keywords Quantum Cryptography · Game Theory · Quantum Key Distribution · Security

1 Introduction

Quantum key distribution (QKD) allows for the establishment of a secret key, secure against all-powerful adversaries. Beginning in the 1980's with the development of the much celebrated BB84 protocol [1], QKD research has since flourished both in theory and in practice, with numerous experimental and even commercial systems. For a general survey of QKD technology, both the theory and the practice, the reader is referred to [2].

In general, these systems are all analyzed in a *standard adversarial model* where any adversary is considered to be simply malicious. However, considering the cost of operating an attack against a QKD protocol using current technology, it is likely that any adversary would need to invest significant time and resources to launch an attack against such a system. Furthermore, due to the effects of privacy amplification, any such attack can only slow down or halt the communication—only with negligible

✉ Walter O. Krawec
walter.krawec@gmail.com

[1] Department of Computer Science and Engineering, University of Connecticut, Storrs, CT 06269, USA

probability would an adversary actually succeed in learning the final secret key [2,3]. In this sense, it is interesting to ask the question, what would be the motivation for an adversary? To answer this question, and study the effects of so-called rational adversaries, one must consider a game theoretic model of security, often used in classical cryptography [4] to understand the behavior and dynamics of systems under attack by adversaries who have a rational motivation as opposed to simply attacking for the sake of attacking.

In this paper we investigate such a game-theoretic model, extending preliminary work we did in a recent conference paper [5]. While we are not the first to apply game theory to QKD security (we review prior approaches in the next section), the model we propose in this work is the most flexible and general purpose, allowing for critical noise tolerance and efficient computations to be performed. These computations are highly important, first, to understand how the protocol would behave in "real-world" scenarios assuming rational adversaries. Second, they are also critical in comparing the performance of different protocols, and, *very importantly from our perspective* to allow for a comparison between the game-theoretic model, and the standard adversarial model. Such a comparison was impossible before our work and so it wasn't clear what, if any, benefit could be attained by considering rational adversaries. We show in this work that the game-theoretic approach can actually lead to more efficient communication systems in some scenarios or support higher noise tolerances. Thus, by assuming rational adversaries, increased secure communication rates may be possible.

We note that there have been other attempts at creating alternative security models for quantum cryptography, weakening the power of the adversary below the status of "all-powerful." Two prominent examples are the quantum bounded storage model [6] and the noisy storage model [7], both of which make assumptions on the memory capabilities of an attacker. While ultimately a weaker form of security, such assumptions allow for increased cryptographic functionalities which are impossible in the standard adversarial model, along with potentially increased performance of QKD protocols [8]. We are proposing an alternative, game-theoretic model of security in this paper which allows one to rigorously analyze adversaries who are "rationally motivated" as opposed to simply being malicious. That is, we are able to analyze the behavior of quantum protocols when they are faced by adversaries who have, for instance, cost limitations on their attack capabilities. Rational models of cryptography have been investigated for classical cryptographic and communication systems (see the Related Work section below) leading to interesting insights in secure communication [9].

In this paper, we show that by considering rational adversaries for QKD systems, one may possibly attain improved performance and noise tolerance of systems beyond the capabilities of the standard adversarial model. One potential motivation for our security model could be in the near future where attacking a QKD system would be expensive, requiring components similar in cost to that of the users (e.g., photon detectors and sources) while providing only the ability to gain minimal information. If QKD systems are to be adopted, first, by large corporations and government agencies, such a rational model may make sense and, as demonstrated in our work, can cause increased communication rates. Alternatively, one may consider the rational approach, with its ability to effectively factor in cost of devices, to be used to motivate other

alternative models of security, such as the previously mentioned bounded and noisy storage models (though we leave that as interesting future work). Finally, by analyzing alternative models of security, one can often discover novel theoretical insights into systems and perhaps develop new applications of quantum cryptography beyond QKD. Our work here lays the groundwork for such rigorous future investigations.

We make several contributions in this work. Extending our preliminary work in our conference paper [5], we propose a general-purpose framework allowing for a game-theoretic analysis of QKD protocols. Our method is the first such framework to allow for critical security computations, as mentioned, and we demonstrate this on several protocols and attack scenarios. Furthermore, unlike our conference paper, the method proposed in this work requires fewer assumptions made on the part of the honest users, which makes it more useful. We show how our method can be applied to practical, real-world devices (which, to our knowledge, has never been considered in any previous game-theoretic approaches). Finally, we make several interesting observations about the efficiency and noise tolerances of QKD protocols operating against rational adversaries. In particular, we show that, under natural assumptions, if an adversary is rational, as opposed to simply malicious, users may increase QKD key generation rates beyond what is possible in the standard adversarial model.

Note that, in this work, we only consider the theoretical asymptotic limit of the QKD systems under investigation. Such work is useful to show the theoretical behavior and potential of systems. We leave as future work, a rigorous analysis of these protocols under finite-key settings. Here, one must take into account also the cost of sampling along with finite key effects. Such challenges are very interesting, and certainly important to undertake, though out of scope for this work. Our model, however, can be extended to the finite key realm, one must, however, consider other costs, such as the amount of sampling to use in order to attain accurate channel characteristics (which would be "costly" for A and B) along with suboptimal error correction (which would be a gain for the adversary).

1.1 Related work

For some time, game theory has been successfully applied to study *classical* cryptography [10–12] (also see [4] for a general survey) and in Cyber Physical System security [9,13–17]. One important contribution of game-theoretic approaches for network communication security is the economics of information security. As networks play an increasingly important role in modern society, new types of security and privacy challenges arise and involve direct participation of network agents. These agents are individual devices or software, acting on their own behalf as independent decision makers, they can be selfish, malicious, or anything in between. Security decisions based on game-theoretic approaches help to allocate limited resources, balance perceived risks, and take into account the underlying incentive mechanisms of behaviors of the other agents in the network.

Attempts to apply game theory to quantum cryptography have begun only recently. In [18], a novel quantum secret sharing scheme was analyzed through game-theoretic means. This same protocol was then used as a subroutine in [19] to solve a quantum

version of the "millionaire's problem," using also a *rational third party*. A quantum bit commitment scheme was proposed in [20] and, assuming rational parties, was proven secure in a game theoretic sense, thus showing an interesting advantage to this model, as perfect security in the standard adversarial model of bit commitment is impossible even with quantum communication [21].

A rational quantum state sharing protocol was proposed in [22] with a goal of sending a quantum state to a designated receiver through the help of additional, rational, parties. Secure direct communication protocols, whose goal is to send a message directly from A to B, was proposed in [23] and analyzed using game-theoretic methods. However, their protocol did not consider a third-party attacker; instead, only A and B were considered and they could either choose to "run the protocol", "stay silent", or "cheat."

The prior work described above all involved cryptographic protocols different from quantum key distribution (QKD). Some recent work, however, has been made in attempting to apply game theory to QKD. A cooperative game was developed in [24] to establish a quantum network which consisted of QKD links capable of relaying information between nodes. However, in that work, QKD was only used as a tool—the primary use of game-theory was in analyzing the nodes so as to construct an optimal network topology for a vehicular network (i.e., game theory was used to analyze the classical problem and QKD was only used as a tool to establish information theoretic secure keys between nodes).

In [25], game theory was used to directly analyze the BB84 QKD protocol. In their model, a three-party game was constructed, with the three parties being A, B, and the adversary E. The strategy space of each participant was to choose a basis (either Z or X) from which to send and receive quantum states in. Thus, the game consisted of A choosing a basis to encode information in (her key-bit information); E choosing a basis to "attack" (using a measure-resend strategy); and B finally choosing a basis to measure in, attempting to learn A's key-bit information. This was the first attempt, to our knowledge, to analyze QKD through game-theoretic means; however, it did not have a goal of actually establishing a key between A and B; instead, the goal was for A and B to detect the adversary E while E's goal was to avoid detection. Our model will incorporate goals related directly to the efficiency of key distillation after quantum communication and privacy amplification are run.

A new model was recently proposed in [26] and is, perhaps, the closest to our work. There, the authors analyzed two QKD protocols, namely the LM05 protocol [27] and the so-called Ping-Pong protocol [28]. Both of these protocols require a two-way quantum channel (sending qubits from A, to B, then back to A). A two-player game was proposed (where one player is the joint A and B party while the second player is the rational adversary E). The strategy space for the AB player was to run the protocol or to run a variant of the given protocol. Parties did not have a choice to "abort" or to choose between the Ping-Pong protocol or the LM05 protocol (instead, two different games were analyzed for the separate protocols). The goal of the adversary was to maximize her information on the distilled raw-key while also avoiding detection. The goal of the AB player was to maximize their mutual information. However, key-rate computations and communication efficiency were not considered in [26]. Also,

avoiding detection is a difficult concept to put into practice as there is always natural noise in the quantum channel [2,3].

In a recent conference paper, we proposed a different approach [5]. As in [26], we consider a two-party game, merging A and B into a single rational entity; we also consider mutual information and adversarial information gain to be goals of the two parties. However, for our framework, we introduced the idea of *decoy iterations* (not to be confused with *decoy states* in standard QKD research [29]) to attempt to find protocols that were "cheap enough" for A and B to be motivated to run them, but "expensive enough" to discourage E from attacking too much. Unlike [26], our framework did not consider probabilities of detection but our method did, importantly, allow for secure key-rate computations. This allowed us to show a direct advantage to rational models of security over standard adversarial models in that, for certain noise scenarios, we showed greatly increased secure communication efficiency (such results were not considered in prior game-theoretic frameworks for QKD). It also allowed us to prove interesting noise tolerance results for rational adversaries. Finally, we also analyzed cases where parties had choices of multiple protocols or to simply "abort", which is an important option in standard QKD research.

However, our previous method only considered certain game-theoretic solutions and required a short-term secret channel between users to allow them to select a strategy. In this paper, we extend our initial conference paper to remove this necessity of the secret channel and also consider a stronger game-theoretic solution. We also extend our analysis to a broader range of channels and design considerations.

1.2 Game-theoretic concepts

We now introduce the game-theoretic concepts necessary to understand our work. Given a tuple $q = (q_1, \ldots, q_n)$ we write q_{-i} to mean the $n-1$ tuple consisting of all q_j for $j \neq i$; i.e., $q_{-i} = (q_1, \ldots, q_{i-1}, q_{i+1}, \ldots, q_n)$.

Definition 1 (*Normal Form Game*) An n-player normal form game G is a tuple (N, S, u), where:

- $N = \{1, \ldots, n\}$ is a set including all the players.
- $S = \{S_1, \ldots, S_n\}$ where S_i is a nonempty set, called player i's strategy space.
- $u = \{u_1, \ldots, u_n\}$; $u_i \colon S_1 \times \cdots \times S_n \to \mathbb{R}$ is a utility function for player i.

Definition 2 [*Best Response* (*BR*)] For agent i, a best response to $s_{-i} = (s_1, \ldots, s_{i-1}, s_{i+1}, \ldots, s_n)$ is a mixed strategy s_i^*, where $s_i^* \in BR(s_{-i})$ iff $\forall s_i \in S_i, u_i(s_i^*, s_{-i}) \geq u_i(s_i, s_{-i})$.

Definition 3 [*Nash Equilibrium* (*NE*)] $s^* \in S$ is a Nash equilibrium of G iff $\forall i, s_i \in BR(s_{-i})$.

No player can gain more utility by changing its strategy unilaterally in a Nash equilibrium, given that the other players' strategies are fixed. Therefore, no rational player wants to deviate from Nash equilibrium.

A normal form game is usually represented by a game matrix. As the example in Table 1, there are two players: A and B. Each of them has two strategies to select.

Table 1 Game matrix example

A	B	
	S_3	S_4
S_1	(x_1, y_1)	(x_2, y_2)
S_2	(x_3, y_3)	(x_4, y_4)

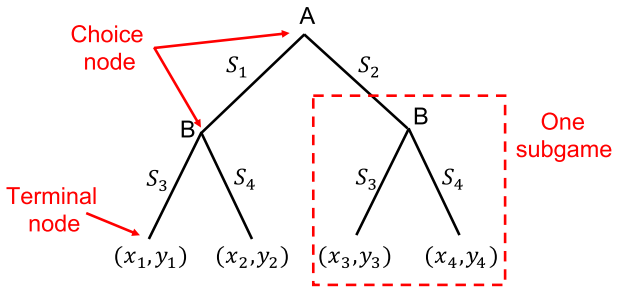

Fig. 1 Game tree example

Once they have selected a strategy, e.g., player A selects S_1 and player B selects S_3, then we can find their corresponding utilities from this game matrix. In the example, A's utility is x_1 and B's utility is y_1. In normal form games, players know the tuple (N, S, u) and take actions simultaneously.

When players take actions by turns, this game is usually represented by a game tree, like the example in Fig. 1, and the corresponding game is called an extensive form game. In Fig. 1, player A selects strategies first. After observing A's strategy (S_1 or S_2), player B will select her strategy accordingly. The extensive form game is formally defined as follows:

Definition 4 (*Extensive form Game*) An n-player (perfect information) extensive form game G is a tuple $(N, S, H, Z, \chi, \rho, \sigma, u)$, where:

- $N = \{1, \ldots, n\}$ is a set including all the players.
- $S = \{S_1, \ldots, S_n\}$ where S_i is a nonempty set, called player i's strategy space.
- H is a set including all the choice nodes.
- $\chi: H \to 2^S$ assigns each choice node several strategies.
- $\rho: H \to N$ assigns each choice node a player.
- Z is a set including all the terminal nodes.
- $\sigma: H \times S \to H \cup Z$ is a successor function that gives a successor for each choice node.
- $u = \{u_1, \ldots, u_n\}$; $u_i: Z \to \mathbb{R}$ is a utility function for player i on the terminal nodes.

An extensive form game usually contains a part that can be considered as a smaller game within itself. This smaller game embedded in the original game is called a subgame.

Definition 5 (*Subgame Perfect Equilibrium*) $s^* \in S$ is a subgame perfect equilibrium of G if and only if for any subgame G', the subset of s in G' is a Nash equilibrium of G'. The subgame of G rooted at $h \in H$ is the subset of G to the descendants of H.

A subgame perfect equilibrium is a Nash equilibrium in the extensive form game and it is able to induce a Nash equilibrium in every subgame. In subgame perfect equilibrium, each player selects a strategy that can finally induce the maximum utility for itself in every subgame. As in Fig. 1, both player A and B know the game tuple $(N, S, H, Z, \chi, \rho, \sigma, u)$. The difference with Table 1 is that player B knows player A's selection when she is making a decision.

2 Description of model

As in our conference paper [5], we consider a two-party normal form game where A and B act as one player (denoted AB) and E acts as a second player. The goal of party AB is to establish a shared secret key as efficiently as possible. E's goal, however, is to decrease A and B's efficiency while remaining "within budget." Since denial-of-service attacks are a cheap way to decrease an honest participant's efficiency to zero, and since such attacks are equally devastating to any point-to-point communication system (including, but not limited to, QKD), we do not consider these attacks in our work. Instead, we will limit Eve to attack strategies that induce no more than a certain upper-tolerated noise level. This also keeps in line with the standard model of QKD security and will allow us to study the maximal noise tolerance permitted within our game-theoretic model, comparing to the standard adversarial model.

Besides these goals for each player (AB to increase communication efficiency; E to decrease it), utilizing communication resources invokes a cost penalty. Thus, for AB, while they wish to establish a shared secret key, if doing so is too expensive (which will depend on many factors including the noise Eve's attack induces), they will choose to simply "abort." Likewise, for E, if attacking the quantum channel is too expensive, she will prefer not to attack or to perform a weaker attack.

The motivation behind our model is to provide a rigorous framework to argue about rational adversaries in order to determine how protocols behave in this security model. As mentioned in the Related Work section, game-theoretic models have been used in classical security settings with many interesting results, including the ability to better allocate resources in a network. Due to the advanced resources needed to optimally attack a QKD protocol in the standard adversarial model, it makes sense to consider adversaries who are limited in "budget." The game-theoretic framework described here allows one to rigorously analyze QKD protocols in such a setting.

We envision the following scenario: To begin, parties A and B advertise a maximal tolerated noise level Q (i.e., this Q is a publicly known constant). We enforce that the noise in the quantum channel (either natural noise or adversarial noise) be no greater than this value. Based on this Q, and the cost of A and B's devices, they may choose to run a QKD protocol or to simply "do nothing" (which costs them nothing, but, of course, they also gain nothing from this action). Unlike the standard adversarial model, we assume that if there is no adversary, then there is still natural noise in the channel (thus, error correction will still be required, giving E information "for free"). Thus Eve, on the other hand, knowing Q is allowed to ignore the quantum channel (in which case, it will still be noisy, but this noise does not relate to Eve's information gain) or she may choose to attack the quantum channel, essentially replacing it with a

perfect channel, and probing each qubit sent according to some attack strategy. Since E is actually *rational*, AB may make things costly for Eve to attack thus motivating her to not even bother (unlike the standard adversarial model where she will always attack). Thus, if we assume the game-theoretic model of security, we can actually make a plausible distinction between natural noise and adversarial noise. If A and B can force Eve not to attack, then E will not have any quantum information on the raw-key (only information leaked by the error-correcting code). This will allow for potentially greater efficiency as less raw key material must be wasted later. Note that, as in the standard model, error correction and privacy amplification are still run, though we will be able to argue that, if E is rational, she will have less information on the raw key, thus privacy amplification needs to shrink the key by less.

What gives A and B the ability to make a QKD protocol "costly" for E is the addition of *decoy iterations* (note that these are different from decoy states used in [29] for weak coherent sources). Decoy iterations, which are added randomly into the qubit stream from A to B, will be completely indistinguishable from real iterations. This can be achieved in a variety of ways. For our work analyzing BB84 and B92, decoy iterations operate exactly the same as standard, "real" iterations, namely with A sending a randomly prepared qubit using the same probability distribution as in the real case. Only later, when the round is complete, is it divulged whether the iteration was a decoy or real iteration. Since both iterations run identically and this information is leaked only afterward, the decoy and real iterations are indistinguishable to an adversary when the qubit is actually traveling (similar to how those iterations used for quantum tomography, needed to ascertain the noise in the channel, are also indistinguishable as they are chosen later).

Though the decoy iteration runs identically to a real iteration, it does not contribute to the key or in any subsequent sampling to determine the channel noise—thus it costs Eve to attack such iterations (leading to no gain); of course it is also costly for Alice and Bob (again, for no gain). Depending on the relative costs between AB's protocol and E's attack strategy, and also depending on the upper-bound noise limit Q, AB may set the probability of decoy iterations to a suitably high value, motivating E to not attack while still keeping AB motivated to run the protocol. If Eve is not attacking, privacy amplification does not have to shrink the raw key by as much. Of course, decoy iterations will affect efficiency as they do not contribute to the final key. Thus, there is an interesting balance and the main question will be: for what noise levels Q will there exist a setting for the number of decoy iterations, whereby AB prefer to run the protocol and E prefers not to attack.

More formally, let Σ_{AB} be the set of strategies allowed to party AB. These are protocols $\Pi^{(\alpha)}$ (e.g., BB84 [1]) parameterized by a decoy value $\alpha \in [0, 1]$ which may be set arbitrarily by Alice or Bob, but once set is constant and public knowledge. This value α represents the probability that any particular iteration is a "real" iteration; that is, $1 - \alpha$ is the probability that an iteration is used as a decoy iteration. At a minimum, we have protocol $I_{AB} \in \Sigma_{AB}$, where we use I_{AB} to mean the "do nothing" protocol, A and B choose to immediately abort, receive no secret key, but also expend no resources. For Eve, we use Σ_E to denote her allowed strategies. We denote $I_E \in \Sigma_E$, where I_E is the "do not attack" strategy for Eve (she may still listen to the classical authenticated channel, though).

Knowing Q, party AB will make a choice of strategy in Σ_{AB}. In reality, since A and B are separate entities, party A will make a choice of strategy and send this choice to B using the public authenticated channel, who will always agree to follow (since, in our game-theoretic model, both parties act as one when choosing a strategy). Eve, of course, learns the strategy choice that AB is playing and she will then choose a strategy of her own based on this information. Note that this is an improvement from our conference version [5] where we assumed the strategy was sent in secret. In our model now, we do not require this secrecy and, instead, assume E is allowed to choose her strategy after observing which protocol A and B will use.

Once both AB and E choose their strategies, they will execute their respective protocol/attack for N iterations (where N is arbitrarily long in our analyses). Of course, standard error correction and privacy amplification procedures are then run distilling a secret key of size $M \leq N$. The overall cost of the protocol is denoted as c_{AB}. The utility assigned to this outcome for AB will be:

$$u_{AB}(M, c_{AB}) = w_{AB}^{+} M - w_{AB}^{-} c_{AB}, \tag{1}$$

where w_{AB}^{+} and w_{AB}^{-} are positive weights. We will simply set these to one in our subsequent analysis.

For Eve, who wishes to decrease the efficiency of A and B's communication, we will assume she gains in utility whenever $N - M$ is large (i.e., whenever M is small). Of course, her attack will also invoke a cost to her, denoted c_E. Due to privacy amplification, the more information E has on the secret key, either gained through her attack, or by listening to the error correction information, the smaller the users' key will be. Thus, we actually define utility in terms of E's information gain on the *raw key* (before error correction and privacy amplification). The more information she has here, the smaller A and B's key will be. Thus, if we let K be E's information on the raw-key, then E's utility will be:

$$u_E(M, c_E) = w_E^{+} K - w_E^{-} c_E, \tag{2}$$

where, again, we will assume both weight values are one. Note that it may seem odd to define utility in terms of information gained on the raw-key when it is really the *secret* key that E wants. However, after privacy amplification, E will have negligible information on the secret key and so we cannot define utility in terms of this (she will never gain anything). Instead, we assume she wants to limit A and B's communication efficiency by making their secret key as small as possible, while keeping within a given noise tolerance upper bound (as discussed our model does not handle denial-of-service attacks). This is equivalent to her being motivated to gain information on the raw key as this will directly correlate to a smaller key.

We use $U_{AB}(\Pi^{(\alpha)}, \mathcal{A})$ and $U_E(\Pi^{(\alpha)}, \mathcal{A})$ to denote AB's (respectively E's) expected utility when protocol $\Pi^{(\alpha)}$ is used by AB and attack $\mathcal{A}$ is used by E for $\Pi^{(\alpha)} \in \Sigma_{AB}$ and $\mathcal{A} \in \Sigma_E$.

In our conference paper, we analyzed the conditions under which strict Nash Equilibrium could exist. Namely, we considered noise scenarios whereby there could exist a value of α, such that $(\Pi^{(\alpha)}, I_E)$ is a strict Nash Equilibrium. Here, it was assumed

that $\Pi^{(\alpha)}$ was a standard protocol (such as BB84 [1] or B92 [30]) augmented with the before mentioned decoy iterations. I_E, of course, was the "do nothing" attack for E (though she still gained information by listening to the error-correction information; recall that, absent Eve, we assume there is still natural noise).

In this paper, however, we improve the solution concept and, instead, analyze the game as an Extensive form Game whereby A will broadcast, in the clear, using the authenticated channel, the strategy choice (our conference paper required this to be sent in secret). In our extension here, therefore, E actually can adapt her strategy based on knowledge of AB's choice. This is a more realistic model with fewer requirements on the users. We will analyze under what noise conditions Q does there exist a value α such that $(\Pi^{(\alpha)}, I_E)$ is a subgame perfect equilibrium. Furthermore, what will be the resulting efficiency of the system (which depends on Q and also α since decoy iterations are useless for key distillation). Under such a solution concept, assuming a rational adversary, it holds, then, that:

1. After A divulges the choice of $\Pi^{(\alpha)}$ (which includes both the protocol and the choice of α, E will be motivated only to perform the "do nothing" attack. This implies the noise in the channel will be due to natural noise (as E did not replace the channel with a perfect one and then probe the qubits with an attack of her choice).
2. Assuming E is rational, if such an α exists, it can be assumed that E did not attack. Thus, only information is leaked due to error correction and one can assume that $I(A : E)$, the mutual information held between A and E *before* error correction, is zero. Thus, less raw-key material must be lost due to privacy amplification. Depending on the choice of α (which, as we will see, depends on several factors including Q and the cost), this may lead to more efficient secure communication rates.
3. A and B are actually motivated to run the given protocol $\Pi^{(\alpha)}$.

We analyze BB84 [1] and B92 [30] protocols in our model assuming intercept resend attacks looking for the noise conditions under which an α exists satisfying our game theoretic solution. Following this, we consider practical devices and imperfect sources.

3 Perfect qubit scenario

We first consider the case where A, B, and E are restricted to perfect qubit channels. This is also the scenario considered in our conference paper [5] (though, there, as mentioned, we used a different game solution mechanism), and also the scenario considered in all other game-theoretic analyses of QKD we are aware of, as discussed in the Related Work section. In a later section of this paper, we will consider practical devices including imperfect sources (e.g., sources that emit multiple photons with nonzero probability) and lossy channels.

For this analysis, we let Σ_{AB}, the strategy set allowed for AB to be $\Sigma_{AB} = \{I_{AB}, \Pi^{(\alpha)}_{BB84}, \Pi^{(\alpha)}_{B92}\}$, where I_{AB} is the "do nothing strategy," $\Pi^{(\alpha)}_{BB84}$ is the BB84 protocol [1] augmented with decoy iterations, and $\Pi^{(\alpha)}_{B92}$ is the B92 protocol [30], again

Table 2 Parameters used to compute the cost of a protocol or attack

Parameter	Description
C_S	E's initial cost to setup her attack equipment. This can include splicing into the quantum channel and replacing a noisy channel with a perfect one from which her attack may "hide" in the original natural noise. We include this parameter for completeness, though we actually consider this to be "free" in our analysis later.
C_{auth}	The cost for A and B to use the authenticated classical channel. This will be a one-time cost.
C_M	This represents the cost to operate a single measurement device capable of detecting one quantum state (e.g., a single SPAD device). We use a function γ_x to denote the multiplicative cost increase of requiring a measurement apparatus capable of detecting x different states. Thus, for example, to measure in two bases (four states), the cost would be $\gamma_4 C_M$. For example, $\gamma_x = 1$ for all x and $\gamma_x = x$.
C_P	This represents the cost to operate the hardware necessary to prepare a qubit state. We use $\gamma_x C_P$ to denote the cost of operating the hardware necessary to prepare x possible states.
C_R	The cost to produce a single uniform random bit. If a δ-biased bit is required, we will assume this costs $h(\delta)C_R$.

augmented with decoy iterations. Recall that the probability of any iteration being used as a decoy is $1 - \alpha$. As these are perhaps the two most commonly implemented protocols in practice, it makes sense to consider both of these. Furthermore, since the hardware requirements are also similar, it also gives an interesting comparison in the rational model.

3.1 Notations

To determine the cost of these protocols, we must parameterize the cost of certain basic operations. This parameterization will also be used to compute the cost of E's attack. We use the same cost variables as in our conference paper [5] which are described in Table 2.

Using these values, we may compute the cost of running $BB84$ for N iterations as:

$$C_{AB}(\Pi_{BB84}^{(\alpha)}) = N[(3 + h(\alpha))C_R + \gamma_4(C_P + C_M)] + C_{\text{auth}}. \tag{3}$$

The $(3 + h(\alpha))C_R$ term accounts for the total number of random bits needed on a single iteration (here, A must choose a key-bit; A and B must both choose a basis, and finally, A must decide whether this is a decoy iteration or not, with probability α). Note that we are considering the unbiased version of BB84 here, thus basis choices are uniform; analyzing the asymmetric case, where basis choices are biased [31], may be interesting future work. Finally, the $\gamma_4(C_P + C_M)$ term accounts for the fact that A must be able to prepare four different states while B must be able to measure in

two bases, with an outcome of four different states. As we combine A and B as one player, their total cost is the cost associated with each of their devices, thus we must add both terms here.

For B92, the cost is found to be:

$$C_{AB}(\Pi_{B92}^{(\alpha)}) = N[(2 + h(\alpha))C_R + \gamma_4 C_M + \gamma_2 C_P] + C_{\text{auth}}. \tag{4}$$

The function clearly takes into account that B92 is a "cheaper" protocol to implement. First, there are fewer random choices (as A need not choose a basis independently—her key choice determines the basis). Also, there are fewer states that A must prepare (2 as opposed to 4).

We must now consider E's attack space. As in our conference paper [5], we will consider Intercept/Resend (IR) attacks. These IR attacks consist of Eve intercepting all qubits and measuring in a particular basis; based on this basis measurement result, she will forward a newly prepared qubit in the state she observed. To ensure that the noise level remains below the given maximum threshold Q, we will additionally introduce a parameter p, which will be the probability that she performs this attack (with probability $1 - p$, she will simply forward the qubit to B without disturbing it—as E is the source of noise when she chooses to attack, the qubit will reach B in the same state that A sent it). We will simply assume that E chooses p so as to maximize the probability of her attacking (thus maximizing her information gain), while keeping the noise induced by her attack at exactly Q (recall, when E chooses to attack, she replaces the noisy channel with a perfect one and then her attack is the only source of noise; however, if she chooses not to attack, the source of noise is natural). Other scenarios and choices of p we leave as future work. It is not difficult to define the cost of such an attack, regardless of basis choice, as the following:

$$C_E = N(h(p)C_R + p\gamma_2(C_M + C_P)) + C_S. \tag{5}$$

(Note that we do not invoke a cost to E if she chooses not to attack based on her parameter p.)

Let $\{|v_0\rangle, |v_1\rangle\}$ be any orthonormal basis that E may use for her IR attack. We restrict our attention to three particular, common, choices: the $Z = \{|0\rangle, |1\rangle\}$ basis, the $X = \{|+\rangle, |-\rangle\}$ basis, and the Breidbart basis B (spanned by states $|v_0\rangle = \cos\frac{\pi}{8}|0\rangle + \sin\frac{\pi}{8}|1\rangle$ and $|v_1\rangle = \sin\frac{\pi}{8}|0\rangle - \cos\frac{\pi}{8}|1\rangle$). E's attack strategies, therefore, are denoted as $\Sigma_E = \{I_E, Z, X, B\}$, where I_E is the "do not attack" strategy.

To finalize the utility computation for both AB and E, we must determine the mutual information between A and E, denoted $I(A : E)$, for each of her possible attacks. This is needed for E's utility, and also needed to determine the final key size for AB's utility. Indeed, using results from [32], we know the key-rate may be computed as $I(A : B) - I(A : E)$. In our conference paper [5], we worked out the value of $I(A : E)$ for any basis choice, and in particular for the three bases of interest. If we denote by $I(\Pi^{(\alpha)}, \mathcal{A})$ to be the value of $I(A : E)$ given that the protocol chosen was $\Pi^{(\alpha)}$ and the attack chosen was $\mathcal{A}$, these computations yield:

$$I(\Pi_{BB84}^{(\alpha)}, Z) \approx .378Q \quad I(\Pi_{BB84}^{(\alpha)}, X) \approx .378Q \quad I(\Pi_{BB84}^{(\alpha)}, B) \approx 1.596Q$$

$$I(\Pi_{B92}^{(\alpha)}, Z) \approx .918Q \qquad I(\Pi_{B92}^{(\alpha)}, X) \approx .918Q \qquad I(\Pi_{B92}^{(\alpha)}, B) \approx 0 \quad (6)$$

(for details on these information computations, the reader is referred to our conference paper [5]). Finally, using this notation, we have the utility of party AB, U_{AB}, and the attacker E, U_E, under different strategies as the following:

$$\begin{aligned} U_{AB}(\Pi^{(\alpha)}, \mathcal{A}) &= \eta\alpha N(I(A:B) - I(\Pi^{(\alpha)}, \mathcal{A})) - C_{AB}(\Pi^{(\alpha)}) \\ U_E(\Pi^{(\alpha)}, \mathcal{A}) &= \eta\alpha N(I(\Pi^{(\alpha)}, \mathcal{A}) + h(\bar{Q})) - C_E \\ U_E(\Pi^{(\alpha)}, I_E) &= \eta\alpha N(h(\bar{Q})) - C_E \end{aligned} \quad (7)$$

where $\bar{Q}$ is the bit error rate for the given protocol and η is the probability that a non-decoy iteration contributes to the raw key (i.e., the probability that A and B choose compatible bases and, in B92's case, that there was no indeterminate measurement). For BB84, $\eta = 1/2$, while for B92, $\eta \leq 1/4$. Note that, above for E's utility, we used not only $I(\cdot)$ (from Eq. 6), but also the fact that she gains information leaked through error correction proportional to $h(\bar{Q})$. Here, $\bar{Q} = Q$ for BB84 and $\bar{Q} = \frac{2Q}{1+2Q}$ for B92.

Computing $I(A:B)$ requires only the noise in the raw key (before error correction and privacy amplification); for BB84, this quantity is easily seen to be simply $1-h(Q)$. For B92, this quantity is found to be $1-h(\bar{Q})$ where $\bar{Q} = 2Q/(1+2Q)$. Combining everything, we can compute the needed utility functions.

3.2 When $(\Pi_{BB84}^{(\alpha)}, I_E)$ is a subgame perfect equilibrium

We now prove a theorem showing for what noise level Q an α exists whereby $(\Pi_{BB84}^{(\alpha)}, I_E)$ is the only subgame perfect equilibrium.

Theorem 1 *Assume classical resources are free, namely $C_S = C_{\text{auth}} = 0$ (note, setting $C_S = 0$ is a strong assumption in favor of the adversary). Also assume randomness is free for the adversary (again, a strong assumption in favor of the adversary). If there exists $\alpha \in (0, 1)$ satisfying:*

$$\frac{C_R + (\gamma_4 - \gamma_2)C_P}{\frac{1}{4} + \frac{1}{4}h\left(\frac{2Q}{1+2Q}\right) - \frac{1}{2}h(Q)} < \alpha < 5.013\gamma_2(C_M + C_P), \quad (8)$$

then $(\Pi_{BB84}^{(\alpha)}, I_E)$ is the only subgame perfect equilibrium.

Proof The game tree of this extensive form game is shown in Fig. 2, where the utility values are summarized in Table 3. We first show that, if AB choose $\Pi_{BB84}^{(\alpha)}$, then I_E is the preferred strategy for E, given a suitable choice of α. When the cost of applying an attack is not neglectable, Eve will consider a choice with the least cost as a rational player. In other words, I_E should bring the highest utility value for Eve. For this to be

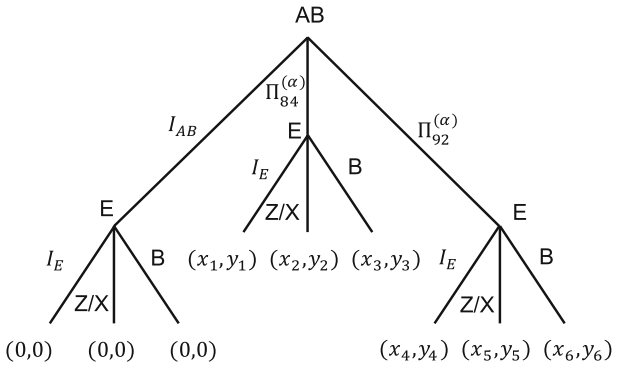

Fig. 2 Game tree of the extensive form game for the perfect qubit scenario

Table 3 Utility values x_i (for AB) and y_i (for E) based on Equations 6 and 7

E	AB $\Pi_{BB84}^{(\alpha)}$
I_E	$U_{AB} = x_1 = \frac{\alpha}{2}(1 - h(Q)) - [(3 + h(\alpha))C_R + \gamma_4 C_M + \gamma_4 C_P]$
	$U_E = y_1 = \frac{\alpha}{2}h(Q)$
Z/X	$U_{AB} = x_2 = \frac{\alpha}{2}(1 - h(Q) - 0.378Q) - [(3 + h(\alpha))C_R + \gamma_4 C_M + \gamma_4 C_P]$
	$U_E = y_2 = \frac{\alpha}{2}(h(Q) + 0.378Q) - [h(2Q)C_R + 2Q\gamma_2(C_M + C_P)]$
B	$U_{AB} = x_3 = \frac{\alpha}{2}(1 - h(Q) - 1.596Q) - [(3 + h(\alpha))C_R + \gamma_4 C_M + \gamma_4 C_P]$
	$U_E = y_3 = \frac{\alpha}{2}(h(Q) + 1.596Q) - [h(4Q)C_R + 4Q\gamma_2(C_M + C_P)]$
E	AB $\Pi_{B92}^{(\alpha)}$
I_E	$U_{AB} = x_4 = \frac{\alpha}{4}\left(1 - h\left(\frac{2Q}{1+2Q}\right)\right) - [(2 + h(\alpha))C_R + \gamma_4 C_M + \gamma_2 C_P]$
	$U_E = y_4 = \frac{\alpha}{4}h\left(\frac{2Q}{1+2Q}\right)$
Z/X	$U_{AB} = x_5 = \frac{\alpha}{4}\left(1 - h\left(\frac{2Q}{1+2Q}\right) - 0.918Q\right) - [(2 + h(\alpha))C_R + \gamma_4 C_M + \gamma_2 C_P]$
	$U_E = y_5 = \frac{\alpha}{4}\left(h\left(\frac{2Q}{1+2Q}\right) + 0.918Q\right) - [h(2Q)C_R + 2Q\gamma_2(C_M + C_P)]$
B	$U_{AB} = x_6 = \frac{\alpha}{4}\left(1 - h\left(\frac{2Q}{1+2Q}\right)\right) - [(2 + h(\alpha))C_R + \gamma_4 C_M + \gamma_2 C_P]$
	$U_E = y_6 = \frac{\alpha}{4}h\left(\frac{2Q}{1+2Q}\right) - [h(4Q)C_R + 4Q\gamma_2(C_M + C_P)]$

true, we require $y_1 > y_2$ and $y_1 > y_3$. This requires:

$$\begin{aligned} y_1 > y_2 &\iff \frac{\alpha}{2}h(Q) > \frac{\alpha}{2}(h(Q) + .378Q) - 2Q\gamma_2(C_M + C_P) \\ &\iff \alpha < 10.582\gamma_2(C_M + C_P). \end{aligned}$$

Similar algebra shows that $y_1 > y_3 \iff \alpha < 5.013\gamma_2(C_M + C_P)$. Thus, for both to be satisfied, we must require that:

$$\alpha < 5.013\gamma_2(C_M + C_P). \tag{9}$$

Next, we require, for any best response of E to $\Pi^{(\alpha)}_{B92}$, AB get a higher reward for playing $\Pi^{(\alpha)}_{BB84}$ for suitable α (assuming, also, that α is such that E prefers I_E in the BB84 case). First we determine E's best response to $\Pi^{(\alpha)}_{B92}$; in particular, we determine the maximum of y_4, y_5, and y_6. It can be shown that:

$$\begin{aligned} y_5 &= y_4 + .2295\alpha Q - 2Q\gamma_2(C_M + C_P) \\ y_6 &= y_4 - 4Q\gamma_2(C_M + C_P). \end{aligned}$$

Thus, $y_6 < y_4$. Let $\Delta = y_5 - y_4 = .2295\alpha Q - 2Q\gamma_2(C_M + C_P)$. However, Eq. 9 implies that $\Delta < 0$. Indeed:

$$\begin{aligned} &\alpha < 5.013\gamma_2(C_M + C_P) < 8.714\gamma_2(C_M + C_P) \\ &\implies .2295\alpha Q < 2Q\gamma_2(C_M + C_P) \\ &\implies \Delta < 0. \end{aligned}$$

Thus, we have y_4 is the largest of these three values implying that the best response for E, in the event AB choose to play $\Pi^{(\alpha)}_{B92}$, is I_E. With this consideration, we require $x_1 > x_4$ implying that, with this knowledge in mind, AB prefer to play $\Pi^{(\alpha)}_{BB84}$. This requirement yields:

$$\begin{aligned} &\frac{\alpha}{2}(1 - h(Q)) - ([3 + h(\alpha)]C_R + \gamma_4[C_M + C_P]) \\ &\quad > \frac{\alpha}{4}\left(1 - h\left[\frac{2Q}{1+2Q}\right]\right) - ([2 + h(\alpha)]C_R + \gamma_4 C_M + \gamma_2 C_P) \\ &\iff \alpha\left(\frac{1}{4} + \frac{1}{4}h\left[\frac{2Q}{1+2Q}\right] - \frac{1}{2}h(Q)\right) > C_R + (\gamma_4 - \gamma_2)C_P. \end{aligned}$$

A graph of $\frac{1}{4} + \frac{1}{4}h\left[\frac{2Q}{1+2Q}\right] - \frac{1}{2}h(Q)$ is shown in Fig. 3 and for all Q it holds that this expression is positive. Thus, we conclude that, for x_1 to be larger than x_4 (i.e., $\Pi^{(\alpha)}_{BB84}$ to be preferred over $\Pi^{(\alpha)}_{B92}$), we must have:

$$\alpha > \frac{C_R + (\gamma_4 - \gamma_2)C_P}{\frac{1}{4} + \frac{1}{4}h\left(\frac{2Q}{1+2Q}\right) - \frac{1}{2}h(Q)}. \tag{10}$$

Also, AB will not select I_{AB} because $x_1 > 0$. Therefore, if an α exists satisfying both Eqs. 9 and 10, $(\Pi^{(\alpha)}_{BB84}, I_E)$ is the only subgame perfect equilibrium completing the proof. □

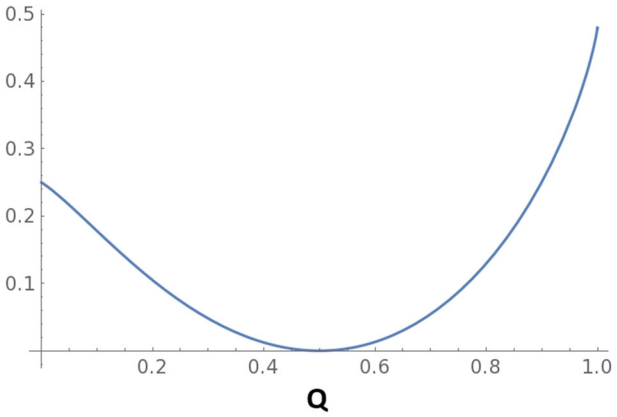

Fig. 3 A graph of $\frac{1}{4} + \frac{1}{4}h\left[\frac{2Q}{1+2Q}\right] - \frac{1}{2}h(Q)$ used in Theorem 1

3.3 Evaluation

Let us look closer at Theorem 1 in order to understand its actual meaning. In particular, we wish to determine for what values of Q, $(\Pi^{(\alpha)}_{BB84}, I_E)$ is actually a subgame perfect equilibrium. Namely, how much noise can be tolerated in our model. Clearly, looking at Eq. 8, we require:

$$\frac{C_R + (\gamma_4 - \gamma_2)C_P}{\frac{1}{4} + \frac{1}{4}h\left(\frac{2Q}{1+2Q}\right) - \frac{1}{2}h(Q)} < 1,$$

as, otherwise no $\alpha \in (0, 1)$ could possibly exist. This gives us some constraint on the cost of preparing a qubit. To evaluate, let us assume randomness is also free for AB and, so, set $C_R = 0$. Note that, in this case, if $\gamma_4 = \gamma_2$, this expression is always satisfied. If $\gamma_4 > \gamma_2$, then we must have:

$$C_P < \frac{1}{\gamma_4 - \gamma_2}\left(\frac{1}{4} + \frac{1}{4}h\left(\frac{2Q}{1+2Q}\right) - \frac{1}{2}h(Q)\right). \tag{11}$$

A graph of the right-hand-side of Eq. 11 is shown in Fig. 4. So long as the cost of preparing a photon is less than this function, it is *possible* that an α exists making $(\Pi^{(\alpha)}_{BB84}, I_E)$ a subgame perfect equilibrium.

However, that alone, is insufficient. Next, to satisfy the main equation in Theorem 1, we also need (again, assuming $C_R = 0$):

$$\frac{(\gamma_4 - \gamma_2)C_P}{\frac{1}{4} + \frac{1}{4}h\left(\frac{2Q}{1+2Q}\right) - \frac{1}{2}h(Q)} < 5.013\gamma_2(C_M + C_P) \tag{12}$$

Let's write $C_M = x \cdot C_P$ for some $x > 0$ (generally, x should be larger than 1 as measurements are often more complicated to perform than state preparation). In that

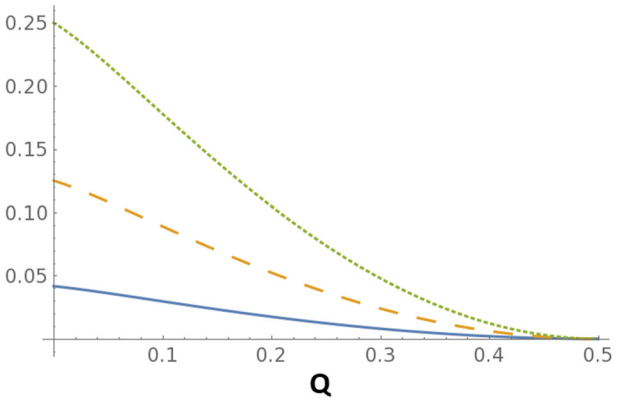

Fig. 4 The cost C_P must be below this line for there to exist an appropriate choice of α. (Note, as mentioned in the text, this is not sufficient.) Showing here for $\gamma_4 - \gamma_2 = 6$ (Solid), 2 (Dashed), and 1 (Dotted). Notice that, the more "expensive" the difference, the cheaper the cost of preparing a state must be for parties to be motivated to run the protocol

case, the above inequality simplifies to:

$$\begin{aligned}
&\frac{(\gamma_4-\gamma_2)C_P}{\frac{1}{4}+\frac{1}{4}h\left(\frac{2Q}{1+2Q}\right)-\frac{1}{2}h(Q)} < 5.013\gamma_2 C_P(x+1)\\
&\quad\iff \gamma_4-\gamma_2 < 5.013\gamma_2(x+1)\left(\frac{1}{4}+\frac{1}{4}h\left(\frac{2Q}{1+2Q}\right)-\frac{1}{2}h(Q)\right)\\
&\quad\iff 0 < 5.013\gamma_2(1+x)\cdot\left(\frac{1}{4}+\frac{1}{4}h\left(\frac{2Q}{1+2Q}\right)-\frac{1}{2}h(Q)\right)-\gamma_4+\gamma_2. \quad (13)
\end{aligned}$$

Notice that this inequality depends only on the noise Q and the *relative* cost of preparing versus measuring states along with the relative cost of preparing or measuring 4 versus 2 states. A graph of the right-hand side of Eq. 13 is shown in Fig. 5. The right-hand side of this equation must be positive in order for an α to exist satisfying the desired game-theoretic property—namely AB will run the protocol while E will not be motivated to attack (though there still will be natural noise in the channel and, so, E will gain information from error correction).

For a given noise level Q, assuming A and B's devices are such that Eq. 11 are satisfied and Eq. 13 is satisfied, one may find an α such that $(\Pi^{(\alpha)}_{BB84}, I_E)$ is a subgame perfect equilibrium. The key-rate is easily computed as $\alpha\frac{1}{2}(1-h(Q))$ which, depending on the cost of the devices (affecting the choice of α) may lead to more efficient communication rates than in the standard adversarial model (where the key-rate there would be $\frac{1}{2}(1-2h(Q))$ [33]).

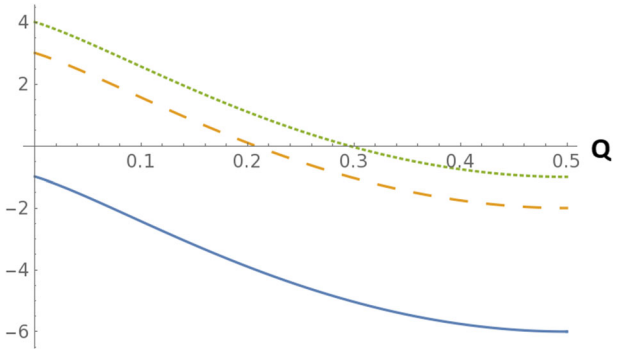

Fig. 5 Showing a graph of Eq. 13 (the right-hand-side) for $x = 1$, $\gamma_2 = 2$ and $\gamma_4 = 8$ (Solid line), $\gamma_4 = 4$ (Dashed line), and $\gamma_4 = 3$ (Dotted line). As long as the noise in the channel Q (x-axis) is such that the curve above is positive, an α may exist satisfying the desired game-theoretic property (one also needs Eq. 11 as shown in Fig. 4 to be satisfied), namely AB will be motivated to run $\Pi^{(\alpha)}_{BB84}$ and Eve will not be motivated to launch a quantum intercept-resend attack. This gives an upper-bound on maximal noise tolerance in the game-theoretic model. Note that, for decreasing γ_4 in this case, the maximal noise tolerance increases

4 Analysis with practical sources

We next consider practical sources and fiber channels. For this, we will only consider AB's strategy space to consist of $\Pi^{(\alpha)}_{BB84}$ or I_{AB}. E's strategy space will consist of I_E or $\mathcal{A}$, where $\mathcal{A}$ is an optimal attack against the system (perhaps requiring a quantum memory system). To determine utility functions, we require the key-rate of the protocol assuming practical sources along with the information gained by an adversary performing an optimal attack. For this, we will use results in [34] which computed these values for BB84.

4.1 Notations

To model the channel noise (which may be natural noise in the event E uses I_E or adversarial noise if she replaces the noisy, and lossy, channel with a perfect one and uses $\mathcal{A}$ which simulates the natural noise and loss in the original channel), we will assume A's source is a weak coherent source, emitting n photons with probability p_n where:

$$p_n = \frac{\mu^n}{n!} e^{-\mu}, \tag{14}$$

and where μ is the intensity of the laser, chosen by A. We assume a fiber channel of length ℓ in which case, the probability of transmittance is:

$$\eta = 10^{-\alpha \ell / 10}, \tag{15}$$

where we will use $\alpha = .15\,\mathrm{dB/km}$.

Again, using notation from [34], let Y_n be the probability that B observes a conclusive result (i.e., not a vacuum signal or double click) given that A sent n photons.

In this case, we define R_n to be the *sifting rate* in the case of n photons and this is simply $R_n = p_n Y_n$. The total sifting rate, given intensity setting μ, is defined to be $R_\mu = \sum_n R_n$. The average error in the distilled raw key will be denoted $Q_\mu = \sum_n Q_n R_n / R_\mu$, where Q_n is the error rate conditioned on A sending n photons. From this, it was shown that the key-rate r in the standard adversarial model is:

$$r = R_1(1 - h(Q_1)) - R_\mu h(Q_\mu). \tag{16}$$

Obviously, if E chooses not to attack, then the only loss in efficiency will be due to information leaked through error correction. In this case, we have:

$$r_{\text{no-attack}} = \alpha R_\mu (1 - h(Q_\mu)). \tag{17}$$

where $1 - \alpha$ is, as usual, the probability of a decoy iteration (which do not contribute to the secret key). Note that, if E chooses to not attack, we assume she is also not performing any photon number splitting (PNS) attack which makes sense as this would be expensive to operate; whereas if she does choose to attack, she performs a PNS attack on any multi-state photon pulse (gaining full information since, in this section, we assume she has access to a perfect quantum memory) while probing, optimally, all single-photon emissions (thus learning something about the key information).

Clearly Q_μ and R_μ are observable quantities while individual Q_n and R_n are not. However, they can be bounded as shown in [34]:

$$R_\mu - \frac{1}{2}\sum_{n\geq 2} p_n \leq R_1 \leq \frac{1}{2} p_1. \tag{18}$$

Naturally, it is in E's best interest to set R_1 as low as possible since E attains full information whenever A sends out 2 or more photons due to the photon number splitting (PNS) attack. Thus, we assume the worst case that:

$$R_1 = R_\mu - \frac{1}{2}\sum_{n\geq 2} p_n = R_\mu - \frac{1}{2}(1 - p_0 - p_1).$$

Finally, we may also estimate [34]:

$$Q_1 = \min\left(\frac{Q_\mu R_\mu}{R_1}, \frac{1}{2}\right).$$

Note that we are not considering the decoy-state protocol [29] which may lead to better results in our game-theoretic model. (One must have both decoy states and decoy iterations and we leave this analysis as future work.)

If E decides to attack using this optimal strategy she gains full information on any multi-photon pulse. She also gains information proportional to $h(Q_1)$ on single

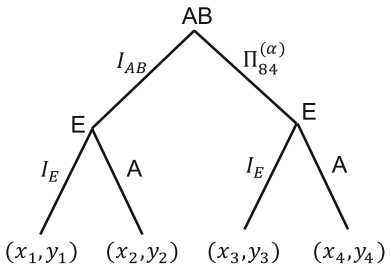

Fig. 6 Game tree considering optimal attack under practical channel

photon emissions. Therefore, her total information gain is no more than:

$$R_1 h(Q_1) + \sum_{n \neq 1} R_n + R_\mu h(Q_\mu) = R_1 h(Q_1) + (R_\mu - R_1) + R_\mu h(Q_\mu). \quad (19)$$

Note that the $R_\mu(Q_\mu)$ term is the information leaked from error correction. Of course, if she does not attack, then she gains only $R_\mu h(Q_\mu)$ due to information leaked during error correction. Given this scenario, we are in a position to prove our second theorem of this work, showing sufficient conditions on the noise Q, and the distance ℓ which allows for there to exist an α whereby $(\Pi_{BB84}^{(\alpha)}, I_E)$ is a subgame perfect equilibrium.

4.2 When $(\Pi_{BB84}^{(\alpha)}, I_E)$ is a subgame perfect equilibrium

Theorem 2 *Let $\Sigma_{AB} = \{I_{AB}, \Pi_{BB84}^{(\alpha)}\}$ and $\Sigma_E = \{I_E, \mathcal{A}\}$ where $\Pi_{BB84}^{(\alpha)}$ is implemented using practical sources and measurement devices and where $\mathcal{A}$ is an optimal attack as discussed. Then $(\Pi_{BB84}^{(\alpha)}, I_E)$ is the only subgame perfect equilibrium if there exists an $\alpha \in (0, 1)$ such that:*

$$\frac{C_{AB}}{R_\mu(1 - h(Q_\mu))} < \alpha < \frac{C_E}{R_1 h(Q_1) + (R_\mu - R_1)}. \quad (20)$$

Proof In this scenario, we have an extensive form game as shown in Fig. 6. The values of the utilities are:

$$\begin{aligned}
x_1 &= x_2 = y_1 = 0 \\
y_2 &= -C_E \\
x_3 &= \alpha R_\mu(1 - h(Q_\mu)) - C_{AB} \\
y_3 &= \alpha R_\mu(Q_\mu) \\
x_4 &= \alpha R_1(1 - h(Q_1)) - \alpha R_\mu h(Q_\mu) - C_{AB} \\
y_4 &= \alpha(R_1 h(Q_1) + (R_\mu - R_1) + R_\mu h(Q_\mu)) - C_E
\end{aligned}$$

We want $(\Pi_{BB84}^{(\alpha)}, I_E)$ to be a subgame perfect equilibrium. Therefore, the best response of $\Pi_{BB84}^{(\alpha)}$ should be I_E, which requires $y_3 > y_4$. This condition leads to the

following inequality:

$$\alpha R_\mu(Q_\mu) > \alpha(R_1 h(Q_1) + (R_\mu - R_1) + R_\mu h(Q_\mu)) - C_E$$
$$\Rightarrow \alpha < \frac{C_E}{R_1 h(Q_1) + (R_\mu - R_1)}. \tag{21}$$

In this case, E is motivated to choose I_E rationally as more advanced resources will be required if she chooses to attack.

Note that, when AB choose I_{AB}, E will choose I_E as a response since $y_1 = 0 > y_2$ (so long as $C_E > 0$ which we assume in our game-theoretic model). When AB makes selection between I_{AB} and $\Pi^{(\alpha)}_{BB84}$, she simply compares x_1 with x_3 and select the one with a higher utility. When $(\Pi^{(\alpha)}_{BB84}, I_E)$ is the equilibrium, it requires $x_3 > x_1$ which results in:

$$\alpha R_\mu(1 - h(Q_\mu)) - C_{AB} > 0 \tag{22}$$
$$\Rightarrow \alpha > \frac{C_{AB}}{R_\mu(1 - h(Q_\mu))}. \tag{23}$$

Under these conditions, AB will never select $\Pi^{(\alpha)}_{BB84}$, so $(\Pi^{(\alpha)}_{BB84}, I_E)$ is the only sub-game perfect equilibrium. This completes the proof. □

4.3 Evaluation

To evaluate, we use values for the practical channel as derived in [34]. Namely, this assumes a weak coherent source and a standard fiber channel. Let p_d be the dark count of B's detectors and η_{eff} be their efficiency. We use η to be the total transmittance of the system, namely:

$$\eta = 10^{-.15\ell/10}\eta_{\text{eff}}, \tag{24}$$

where ℓ is the length of the fiber channel connecting the two users (in km). From this, the values we use for observed statistics are (see [34]):

$$R_\mu = \frac{1}{2}\left(1 - (1 - p_d)^2 e^{-\mu\eta}\right)$$
$$R_\mu Q_\mu = \frac{1}{4}\left(1 + (1 - p_d)e^{-\mu F\eta} - (1 - p_d)e^{-\mu V\eta} - (1 - p_d)^2 e^{-\mu\eta}\right)$$

Estimates on the values R_1 and Q_1 are discussed above (derived from [34]).

To ensure that $(\Pi^{(\alpha)}_{BB84}, I_E)$ is a solution according to Theorem 2, we need (from Eq. 20):

$$C_{AB} < R_\mu(1 - h(Q_\mu)), \tag{25}$$

thus placing a restriction on the cost of A and B's devices.

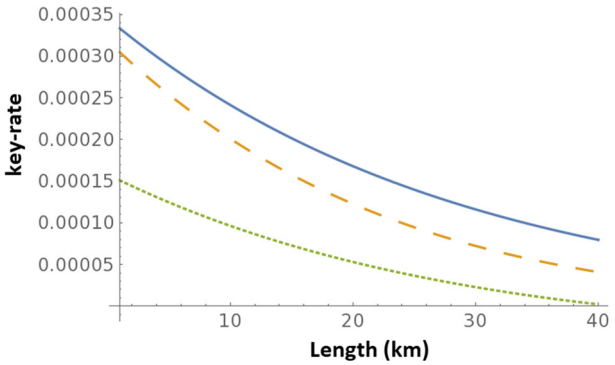

Fig. 7 Showing the key-rate of the BB84 protocol under practical device settings and comparing to the standard adversarial model. As discussed in the text, length and noise tolerances are identical in both models; however, as demonstrated here, even taking into account the additional decoy iterations, greater efficiency is possible, depending on the cost of the devices. Solid line: Game theoretic model with $\gamma \approx 1$; Dashed line: Game-theoretic model with $\gamma = 1/2$; Dotted line (lowest) standard adversarial model. Here we have $p_d = 10^{-5}$, $Q = .05$, $\eta_{\text{eff}} = .1$, and $\mu = .01$. Note that, for these device settings, 41 km is the maximal distance allowed for both the standard and game-theoretic model

Next, let's assume that $C_{AB} = C_E$ (a very strong assumption *in favor of the adversary* as to perform an optimal probe may require perfect quantum memory—a much more expensive device than A and B's preparation and measurement devices). In that case, to satisfy Eq. 20, it is easy to see that we require $R_1(1-h(Q_1))-R_\mu h(Q_\mu) > 0$; thus, the noise and length tolerances are identical to the standard attack model (as dictated by Eq. 16). However, greater efficiency may be possible.

Indeed, to compute the key-rate of the protocol in our game theoretic model, we require α (see Eq. 17). From Eq. 25, let $C_E = C_{AB} = \gamma R_\mu(1 - h(Q_\mu))$ for some $0 < \gamma < 1$. Then if we set:

$$\alpha = \min\left(\frac{\gamma R_\mu(1 - h(Q_\mu))}{R_1 h(Q_1) + R_\mu - R_1} - \epsilon, 1 - \epsilon\right), \tag{26}$$

for suitably small ϵ, the requirements of Theorem 2 are satisfied. The resulting key-rate evaluation is shown in Fig. 7. This shows that, even though noise and distance limitations are identical in both models, increased efficiency is possible depending on the cost.

5 Closing remarks

In this paper, we showed how a rational model of quantum cryptography may be applied to QKD. Our model allows for important key-rate and noise tolerance computations for a variety of protocols. In particular, we show that high noise tolerances are possible (exceeding the standard model if one assumes rational adversaries and depending on the relative cost of devices) and greater efficiency is possible, even when using practical devices. There are several interesting open problems, including an anal-

ysis of alternative protocols and attack scenarios. We also did not consider finite-key effects and only looked at asymptotic scenarios; analyzing these in our game-theoretic framework would also be interesting.

References

1. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, vol. 175. New York (1984)
2. Scarani, V., Bechmann-Pasquinucci, H., Cerf, N.J., Dušek, M., Lütkenhaus, N., Peev, M.: The security of practical quantum key distribution. Rev. Mod. Phys. **81**, 1301–1350 (2009)
3. Pirandola, S., Andersen, U.L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., Englund, D., Gehring, T., Lupo, C., Ottaviani, C., et al.: Advances in quantum cryptography (2019). arXiv preprint arXiv:1906.01645
4. Katz, J.: Bridging game theory and cryptography: Recent results and future directions. In: Theory of Cryptography Conference, pp. 251–272. Springer, Berlin (2008)
5. Krawec, W.O., Miao, F.: Game theoretic security framework for quantum key distribution. In: International Conference on Decision and Game Theory for Security, pp. 38–58. Springer, Berlin (2018)
6. Damgård, I.B., Fehr, S., Salvail, L., Schaffner, C.: Cryptography in the bounded-quantum-storage model. SIAM J. Comput. **37**(6), 1865–1890 (2008)
7. Wehner, S., Schaffner, C., Terhal, B.M.: Cryptography from noisy storage. Phys. Rev. Lett. **100**(22), 220502 (2008)
8. Damgård, I.B., Fehr, S., Renner, R., Salvail, L., Schaffner, C.: A tight high-order entropic quantum uncertainty relation with applications. In: Annual International Cryptology Conference, pp. 360–378. Springer, Berlin (2007)
9. Manshaei, M., Zhu, Q., Alpcan, T., Basar, T., Hubaux, J.: Game theory meets network security and privacy. ACM Comput. Surv. **45**(3), 25:1–25:39 (2013)
10. Halpern, J., Teague, V.: Rational secret sharing and multiparty computation. In: Proceedings of the Thirty-Sixth Annual ACM Symposium on Theory of Computing, pp. 623–632. ACM, New York (2004)
11. Asharov, G., Lindell, Y.: Utility dependence in correct and fair rational secret sharing. In: Advances in Cryptology-CRYPTO 2009, pp. 559–576. Springer, Berlin (2009)
12. Kol, G., Naor, M.: Cryptography and Game Theory: Designing Protocols for Exchanging Information. In: Theory of Cryptography Conference, pp. 320–339. Springer, Berlin (2008)
13. Miao, F., Zhu, Q., Pajic, M., Pappas, G.J.: A hybrid stochastic game for secure control of cyber-physical systems. Automatica **93**, 55–63 (2018)
14. Pajic, M., Tabuada, P., Lee, I., Pappas, G.J.: Attack-resilient state estimation in the presence of noise. In: 2015 54th IEEE Conference on Decision and Control (CDC), pp. 5827–5832 (2015)
15. Miao, F., Zhu, Q., Pajic, M., Pappas, G.J.: Coding schemes for securing cyber-physical systems against stealthy data injection attacks. IEEE Trans. Control Netw. Syst. **4**(1), 106–117 (2016)
16. Zhu, Q., Basar, T.: Game-theoretic methods for robustness, security, and resilience of cyberphysical control systems: games-in-games principle for optimal cross-layer resilient control systems. Control Syst. IEEE **35**(1), 46–65 (2015)
17. Zhu, M., Martinez, S.: Stackelberg-game analysis of correlated attacks in cyber-physical systems. Am. Control Conf. (ACC) **2011**, 4063–4068 (2011)
18. Maitra, A., De Joyee, S., Paul, G., Pal, A.K.: Proposal for quantum rational secret sharing. Phys. Rev. A **92**(2), 022305 (2015)
19. Maitra, A., Paul, G., Pal, A.K.: Millionaires problem with rational players: a unified approach in classical and quantum paradigms (2015). arXiv preprint
20. Zhou, L., Sun, X., Su, C., Liu, Z., Choo, K.-K.R.: Game theoretic security of quantum bit commitment. Inf. Sci. **479**, 503–514 (2018)
21. Mayers, D.: Unconditionally secure quantum bit commitment is impossible. Phys. Rev. Lett. **78**, 3414–3417 (1997)
22. Dou, Z., Xu, G., Chen, X.-B., Liu, X., Yang, Y.-X.: A secure rational quantum state sharing protocol. Sci. China Inf. Sci. **61**(2), 022501 (2018)

23. Qin, H., Tang, W.K.S., Tso, R.: Establishing rational networking using the DL04 quantum secure direct communication protocol. Quantum Inf. Process. **17**(6), 152 (2018)
24. Das, B., Roy, U., et al.: Cooperative quantum key distribution for cooperative service-message passing in vehicular ad hoc networks. Int. J. Comput. Appl. **975**(8887), 37–42 (2014)
25. Houshmand, M., Houshmand, M., Mashhadi, H.R.: Game theory based view to the quantum key distribution bb84 protocol. In: Intelligent Information Technology and Security Informatics (IITSI), 2010 Third International Symposium on, pp. 332–336. IEEE (2010)
26. Kaur, H., Kumar, A.: Game-theoretic perspective of ping-pong protocol. Phys. A Stat. Mech. Appl. **490**, 1415–1422 (2018)
27. Lucamarini, M., Mancini, S.: Secure deterministic communication without entanglement. Phys. Rev. Lett. **94**(14), 140501 (2005)
28. Boström, K., Felbinger, T.: Deterministic secure direct communication using entanglement. Phys. Rev. Lett. **89**(18), 187902 (2002)
29. Lo, H.-K., Ma, X., Chen, K.: Decoy state quantum key distribution. Phys. Rev. Lett. **94**(23), 230504 (2005)
30. Bennett, C.H.: Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett. **68**, 3121–3124 (1992)
31. Lo, H.-K., Chau, H.-F., Ardehali, M.: Efficient quantum key distribution scheme and a proof of its unconditional security. J. Cryptol. **18**(2), 133–165 (2005)
32. Devetak, I., Winter, A.: Distillation of secret key and entanglement from quantum states. Proc. R. Soc. A Math. Phys. Eng. Sci. **461**(2053), 207–235 (2005)
33. Shor, P.W., Preskill, J.: Simple proof of security of the BB84 quantum key distribution protocol. Phys. Rev. Lett. **85**, 441–444 (2000)
34. Kraus, B., Branciard, C., Renner, R.: Security of quantum-key-distribution protocols using two-way classical communication or weak coherent pulses. Phys. Rev. A **75**(1), 012316 (2007)

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