Finite Key Analysis of the Extended B92 Protocol

Omar Amer
Department of Computer Science and Engineering
University of Connecticut
06269 Storrs, Connecticut
Email: omar.amer@uconn.edu

Walter O. Krawec
Department of Computer Science and Engineering
University of Connecticut
06269 Storrs, Connecticut
Email: walter.krawec@uconn.edu

***Abstract*—In this paper we derive a key rate expression for the extended version of the B92 quantum key distribution protocol that takes into account, for the first time, the effects of operating with finite resources. With this expression, we conduct an analysis of the protocol in a variety of different noise and key-length settings, and compare to previous bounds on comparable protocols.**

I. Introduction

Quantum Key Distribution is becoming an increasingly practically driven field of research [1] [2]. As advances in this and other fields make commercial implementations of QKD devices more desirable, it is necessary that more work is done to understand the capabilities and limitations of these protocols in practice, as opposed to under ideal circumstances. The B92 protocol [3] has been well researched in the asymptotic setting, where it has been shown to be tolerant to up to 6.5% noise in the channel [4]. An extended variant of B92 was proposed [5], in which, in addition to the two encoding, non-orthogonal states used in B92, Alice and Bob utilize two additional non-encoding, non-orthogonal states to achieve a tighter bound on Eve's information. Analysis of the extended B92 protocol has shown it to be tolerant to up to 11% noise in the asymptotic setting [5]. In this paper we will present what is, to our knowledge, the first analysis of the key rate for the extended B92 protocol in the finite key setting.

We conduct a finite-length, information theoretic security analysis, assuming collective attacks, and rigorously evaluate lower bounds on the key rate and noise tolerance. We evaluate assuming a depolarization channel, though the equations we arrive at hold for arbitrary channels. We do this by following the well established key-rate computations put forth in [9], as well as the methods for utilizing mismatched measurement given in [10]. In this work we will only consider ideal qubits, and as such we will not make considerations for the effect that loss might have on the security of the protocol. On the subject of loss, we note that the original B92 protocol is highly susceptible to the unambiguous state discrimination attack [6] [7] [8], while the extended version, which we analyze here, protects against such attacks [5].

After conducting our security analysis, we will optimize over a number of parameters and discuss optimal trends, as well as compare the key rates achievable through our analysis with the key rates achievable with standard B92 in previous analysis.

A. Notation

Let A be a random variable, we will denote by $H(A)$ the Shannon entropy of A. We will use both $H(p)$ and $h(p)$ to refer to the binary entropy function, and they should both be understood to be equal to $H(p, 1-p)$.

Given a pure state $|\psi\rangle_A \in \mathcal{H}_A$ we will use both $[\psi]_A$ and $P(|\psi\rangle)_A$ to mean $|\psi\rangle\langle\psi|_A$. Given a density operator ρ_{AB} we will write ρ_B to mean the state obtained by taking the partial trace over the A system of ρ_{AB}. By a *classical quantum* or CQ state, we will mean a quantum state that can be described by some $\rho_{AB} = \sum_a p_a[\mathbf{a}] \otimes \rho_B^{(a)}$ for an orthonormal basis $\{|a\rangle\}$.

Given a density operator ρ_A acting on $\mathcal{H}_A$, we will mean by $S(A)_\rho$ the von-Neumann entropy of ρ_A, equivalent to $-tr(\rho_A log \rho_A)$, where here and elsewhere in this paper log is base 2 unless otherwise stated. We will mean by $S(A|B)_\rho$ the von-Neumann entropy of the A register of ρ conditioned on the B register, where $S(A|B)_\rho = S(AB)_\rho - S(B)_\rho$. If the context is clear, for entropy as well as state description, we will often drop the subscript.

Later we will evaluate key rates in a number of channel scenarios, all *symmetric channels*, by which we mean that the channel which connects Alice on Bob (and where Eve's attack takes place), parameterized by quantum noise level Q, can be described by the depolarization channel

$$\mathcal{E}_Q(\rho) \mapsto (1-2Q)\rho + QI. \tag{1}$$

To find a lower bound of the key rate, we make use of the key rate equation, Equation 2, presented in [9], which states that in the finite realm, the key rate, r', of a protocol, under collective attacks, can be calculated as below. We note that as we utilize a different sampling method than was used in [9], we must utilize a larger confidence interval than was used in [9]. Our confidence interval, Equation 4, is derived from Hoeffding's inequality. In [9] it was shown that for a protocol that has run for N rounds, and resulted in $n \leq N$ raw key bits, the key rate r', can be computed to be

$$r' = \frac{l(n)}{n} = S_\xi(A|E) - (leakEC - \Delta)/n, \tag{2}$$

where

$$S_\xi(A|E) = \min_{\sigma_{\bar{A}\bar{E}} \in \Gamma} S(\bar{A}|\bar{E})_\sigma, \tag{3}$$

978-1-7281-6432-8/20/$31.00 ©2020 IEEE

with Γ consisting of all σ which we could expect to induce statistics that differ by no more than $\xi(m_i)$, except with some probability $\epsilon_{PE} > 0$, for any of $\{p_i\}_{i=1}^{k}$ statistics, each gathered over m_i samples, for:

$$\xi(m) = \sqrt{\frac{ln\left(2/\left(1-\sqrt[k]{1-\epsilon_{PE}}\right)\right)}{2m}}, \tag{4}$$

where we take $leakEC$ as the number of bits leaked due to error correction of n raw key bits for a given quantum bit error rate; $\Delta = 2log_2(1/[\epsilon-\overline{\epsilon}-\epsilon_{EC})])+7\sqrt{nlog_2(2/(\overline{\epsilon}-\epsilon'_{EC})}$ are bits lost due to finite key effects; ϵ, ϵ_{EC} are user parameters that denote the security parameter of the key and the failure probability of error correction respectively; and $\overline{\epsilon}, \epsilon_{PE}$, obeying constraints $\epsilon - \epsilon_{EC} > \overline{\epsilon} > \epsilon_{PE} \geq 0$, can be be chosen so as to maximize the key rate.

To evaluate the von-Neumann entropy in Equation 3, we will additionally make use of the following theorem:

Theorem 1. (From [10]): Let ρ_{AE} be a CQ state acting on $\mathcal{H}_A \otimes \mathcal{H}_E$ that can be written as

$$\rho_{AE} = \frac{1}{M}\left([\mathbf{0}]_A \otimes \sum_{i=0}^{1}[\mathbf{g_0^i}]_E + [\mathbf{1}]_A \otimes \sum_{i=0}^{1}[\mathbf{g_1^i}]_E\right). \tag{5}$$

Then

$$S(A|E) \geq \sum_{i=0}^{1}\left(\frac{\langle g_0^i|g_0^i\rangle + \langle g_1^i|g_1^i\rangle}{M}\right)S_i$$

$$S_i = \begin{cases} S_i = h\left(\frac{\langle g_0^i|g_0^i\rangle}{\langle g_0^i|g_0^i\rangle+\langle g_1^i|g_1^i\rangle}\right) - h(\lambda_i) & {\scriptstyle \langle g_0^i|g_0^i\rangle>0, \atop \langle g_1^i|g_1^i\rangle>0} \\ S_i = 0 \text{ else} \end{cases}$$

where

$$\lambda_i = \frac{1}{2} + \frac{\sqrt{\left(\langle g_0^i|g_0^i\rangle + \langle g_1^i|g_1^i\rangle\right)^2 + 4Re^2\langle g_0^i|g_1^i\rangle}}{2\left(\langle g_0^i|g_0^i\rangle + \langle g_1^i|g_1^i\rangle\right)}$$

II. The Protocol and Key-Rate Computation

The protocol we analyze is actually a simplified version of the Extended B92 protocol that operates as follows. Alice and Bob utilize the bases $Z = \{|0\rangle, |1\rangle\}$ and $A = \{|\alpha\rangle, |\overline{\alpha}\rangle\}$ where $|\alpha\rangle = \alpha|0\rangle + \beta|1\rangle$ and $|\overline{\alpha}\rangle = \beta|0\rangle - \alpha|1\rangle$, $0 < \alpha < 1$ is a publicly known parameter of the protocol, and $\beta = \sqrt{(1-\alpha^2)}$. On an iteration of the protocol, with probability P_{enc}, also a parameter, this round is a *key round*, and Alice randomly prepares and transmits either the state $|0\rangle$ or $|\alpha\rangle$ to Bob. Otherwise, with probability $(1-P_{enc})$ she sends state $|1\rangle$. Bob chooses to measure his received state in the Z or A basis with equal probability. At the end of a round, Alice notifies Bob if the round was a key round, and, if Bob measured either $|\overline{\alpha}\rangle$ or $|1\rangle$, Bob notifies Alice that the round was conclusive, otherwise that it was inconclusive. On a conclusive key round, Alice's key bit is 0 if she sent $|0\rangle$ and 1 if she sent $|\alpha\rangle$, and Bob's key bit is 0 if he measured $|\overline{\alpha}\rangle$, and 1 if he measured $|1\rangle$. If a round is not conclusive, or not a key round, the results are used for channel tomography.

Following N rounds of this protocol, Alice and Bob will share a correlated but noisy raw key string of length $n < N$, as well as $m < N - n$ samples that we will show can be used to estimate various channel statistics, obtained from rounds that did not contribute to the key. At this point Alice and Bob follow standard post processing procedures, conducting error correction and privacy amplification to distill an $l(n)$ bit secret key [1] [2].

In this section we model the state of the system at the end of a key round so that we may find a lower bound on $S(A|E)$, in order to compute the key rate. Towards this end, we also discuss how to estimate the parameters of Eve's attack with statistics that are observed during the course of the protocol, as well as how to calculate the confidence interval that must be minimized over for each of those statistics in the finite case.

A. Bounding the Conditional Entropy

To bound the quantity $S(A|E)$ we must first compute a density operator for the system at the end of a key round. Because we are considering collective attacks, Eve's attack can be modeled by unitary operator U, acting on a qubit and her ancillary space, initialized as $|\chi_E\rangle$, as follows:

$$U|0,\chi_E\rangle \mapsto |0,e_0\rangle + |1,e_1\rangle,$$
$$U|1,\chi_E\rangle \mapsto |0,e_2\rangle + |1,e_3\rangle.$$

For ease of notation we will make explcit the action $U|\alpha,\chi_E\rangle \mapsto |\alpha,f_0\rangle + |\overline{\alpha},f_1\rangle$ where

$$|f_0\rangle = \alpha^2|e_0\rangle + \alpha\beta|e_2\rangle + \alpha\beta|e_1\rangle + \beta^2|e_3\rangle, \tag{6}$$
$$|f_1\rangle = \alpha\beta|e_0\rangle + \beta^2|e_2\rangle - \alpha^2|e_1\rangle - \alpha\beta|e_3\rangle. \tag{7}$$

As we are interested in the entropy of Alice's key, we condition on this round of the protocol being a key round. As such, Alice begins the protocol by preparing the transit space $\mathcal{H}_T$ as either $|0\rangle$ or $|\alpha\rangle$ and storing her key bit in the register $\mathcal{H}_A$. Eve attacks with U acting on $\mathcal{H}_T \otimes \mathcal{H}_E$, resulting in the joint state:

$$\rho_{ATE} = \frac{1}{2}[\mathbf{0}]_A \otimes P(|0,e_0\rangle + |1,e_1\rangle)_{TE}$$
$$+ \frac{1}{2}[\mathbf{1}]_A \otimes P(|\alpha,f_0\rangle + |\overline{\alpha},f_1\rangle)_{TE}.$$

Bob now chooses to make a measurement of $\mathcal{H}_T$ in either the Z or A basis, each with equal probability. Again conditioning on this round being a key round, he observes either $|1\rangle$ or $|\overline{\alpha}\rangle$, corresponding to his key register $\mathcal{H}_B$ being set as 1 or 0 respectively. Tracing out the spaces $\mathcal{H}_T$ and $\mathcal{H}_B$ after we condition on a conclusive measurement, we are left with:

$$\rho_{AE} = \frac{1}{M}[\mathbf{0}]_A \otimes (P(|e_1\rangle) + P(\beta|e_0\rangle - \alpha|e_1\rangle))_E$$
$$+ \frac{1}{M}[\mathbf{1}]_A \otimes (P(|f_1\rangle) + P(\beta|f_0\rangle - \alpha|f_1\rangle))_E,$$

where M is a normalization term we will define shortly. In accordance with Theorem 1, we can then represent this state in the form given in Equation 5, with:

$$M = \sum_{i=0}^{1} \langle g_0^i | g_0^i \rangle + \langle g_1^i | g_1^i \rangle \,, \tag{8}$$

$$|g_0^0\rangle = |e_1\rangle \,, \tag{9}$$

$$|g_0^1\rangle = \beta |e_0\rangle - \alpha |e_1\rangle \,, \tag{10}$$

$$|g_1^0\rangle = |f_1\rangle \,, \tag{11}$$

$$|g_1^1\rangle = \beta |f_0\rangle - \alpha |f_1\rangle = \alpha |e_1\rangle + \beta |e_3\rangle \,. \tag{12}$$

B. Parameter Estimation

With an operator determined it remains to estimate the various inner products of Eve's states as functions of the observable statistics we gather. It is trivial to find the following identities based on Eve's attack operator:

$$\langle e_0|e_0\rangle = P_{00}, \qquad \langle e_1|e_1\rangle = P_{01},$$
$$\langle e_2|e_2\rangle = P_{10}, \qquad \langle e_3|e_3\rangle = P_{11}.$$

Where P_{ij} denotes the probability of Bob measuring $|j\rangle$ after Eve's attack, conditioned on Alice sending the state $|i\rangle$.

Next we consider the information that can be gained by gathering mismatched statistics [10] [11] [12], gathered from rounds in which Alice and Bob chose to prepare and measure states in mismatched bases. For example, by computing the probability $P_{0\alpha}$ we are able to compute the quantity $Re\,\langle e_0|e_1\rangle$. Indeed, tracing the evolution of the qubit in that case, we find:

$$\begin{aligned}
|0\rangle &\mapsto |0, e_0\rangle + |1, e_1\rangle \\
&= |\alpha\rangle \otimes (\alpha |e_0\rangle + \beta |e_1\rangle) + \\
&\quad |\overline{\alpha}\rangle \otimes (\beta |e_0\rangle + \alpha |e_1\rangle) \\
\implies P_{0\alpha} &= \alpha^2 \langle e_0|e_0\rangle + \beta^2 \langle e_1|e_1\rangle \\
&\quad + 2\alpha\beta Re \,\langle e_0|e_1\rangle \\
\implies Re\,\langle e_0|e_1\rangle &= \frac{P_{0\alpha} - \alpha^2 \langle e_0|e_0\rangle - \beta^2 \langle e_1|e_1\rangle}{2\alpha\beta}. \qquad (13)
\end{aligned}$$

Similarly we can also find:

$$Re\,\langle e_2|e_3\rangle = \frac{P_{1\alpha} - \alpha^2 \langle e_2|e_2\rangle - \beta^2 \langle e_3|e_3\rangle}{2\alpha\beta}, \tag{14}$$

$$Re\,\langle e_0|e_2\rangle = \frac{P_{\alpha 0} - \alpha^2 \langle e_0|e_0\rangle - \beta^2 \langle e_2|e_2\rangle}{2\alpha\beta}, \tag{15}$$

$$Re\,\langle e_1|e_3\rangle = \frac{P_{\alpha 1} - \alpha^2 \langle e_1|e_1\rangle - \beta^2 \langle e_3|e_3\rangle}{2\alpha\beta}. \tag{16}$$

Through much the same method, utilizing the states given in Equations 6 and 15, we are able to find the following identity using $P_{\alpha\overline{\alpha}}$.

$$\begin{aligned}
&2\alpha^2\beta^2 Re\,(\langle e_0|e_3\rangle + \langle e_1|e_2\rangle) = \\
&\alpha^2\beta^2\,(\langle e_0|e_0\rangle + \langle e_3|e_3\rangle) + \\
&\beta^4 \langle e_2|e_2\rangle + \alpha^4 \langle e_1|e_1\rangle + \\
&2\alpha^3\beta Re\,(\langle e_1|e_3\rangle - \langle e_0|e_1\rangle) + \\
&2\alpha\beta^3 Re\,(\langle e_0|e_2\rangle - \langle e_2|e_3\rangle) - P_{\alpha\overline{\alpha}}. \qquad (17)
\end{aligned}$$

With the last of our identities described, we can now apply Theorem 1 to find a lower bound on the entropy of Eve's system to be:

$$S(A|E) \geq \sum_{i=0}^{1} \left(\frac{E_0[i] + E_1[i]}{M} \right) S_i \tag{18}$$

$$S_i = \begin{cases} S_i = h\left(\frac{E_0[i]}{E_0[i]+E_1[i]}\right) - h(\lambda_i) & \substack{\text{if } E_0[i]>0 \\ \text{and } E_1[i]>0} \\ S_i = 0 \text{ else} \end{cases}$$

where $A[i]$ denotes indexing into any of the ordered sets A given below, and

$$\begin{aligned}
\lambda_i &= \frac{1}{2} + \frac{\sqrt{(E_0[i] + E_1[i])^2 + 4Re^2\Lambda[i]}}{2\,(E_0[i] + E_1[i])}, \\
E_0 &= \{\langle g_0^0|g_0^0\rangle \,, \langle g_0^1|g_0^1\rangle\} = \{P_{01}, 1 - P_{0\alpha}\}, \qquad (19) \\
E_1 &= \{\langle g_1^0|g_1^0\rangle \,, \langle g_1^1|g_1^1\rangle\} = \{P_{\alpha,\overline{\alpha}}, 1 - P_{\alpha 0}\}, \qquad (20) \\
\Lambda &= \{\langle g_0^0|g_1^0\rangle \,, \langle g_0^1|g_1^1\rangle\}, \\
\Lambda[0] &= \alpha\beta Re\,(\langle e_0|e_1\rangle + \langle e_1|e_3\rangle) - \alpha^2 \langle e_1|e_1\rangle \\
&\quad + \beta^2 Re\,\langle e_1|e_2\rangle \,, \qquad (21) \\
\Lambda[1] &= \alpha\beta Re\,(\langle e_0|e_1\rangle + \langle e_1|e_3\rangle) - \alpha^2 \langle e_1|e_1\rangle \\
&\quad + \beta^2 Re\,\langle e_0|e_3\rangle \,. \qquad (22)
\end{aligned}$$

We note that all of the inner products above, with the exception of $\langle e_1|e_2\rangle$ in Equation 21, can be estimated by the statistics gathered in this protocol, either having been made explicit in earlier discussion or, in the case of Equations 19 and 20, can be computed to be as we claim by further tracing of the evolution of the state. We can now compute the bound given in Equation 18 by minimizing over the sole free variable, which itself can be bounded by Cauchy-Schwartz as $\langle e_1|e_2\rangle \in \left[-\sqrt{\langle e_1|e_1\rangle \langle e_2|e_2\rangle}, \sqrt{\langle e_1|e_1\rangle \langle e_2|e_2\rangle}\right]$, with $\langle e_0|e_3\rangle$ obtained by Equation 17.

C. Finite Key Effects

To calculate the key rate in the finite case, we must account for uncertainty in our observed statistics, and consider all possible attacks Eve may have used that induce statistics within the relevant confidence interval, as given by Equation 4. Let each statistic P_{ij} have been sampled over C_{ij} samples, then, following the work done in [9], we find that to calculate a worst case bound on Eve's information we must further minimize the entropy expression given in Equation 18, now replacing all observed P_{ij} used in parameter estimation with

$$\hat{P_{ij}} \in (P_{ij} - \xi(C_{ij}), P_{ij} + \xi(C_{ij})),$$

save for $\hat{P_{00}}$, $\hat{P_{11}}$, and $\hat{P_{\alpha 1}}$ which we take to be equal to $1 - \hat{P_{01}}$, $1 - \hat{P_{10}}$, and $1 - \hat{P_{\alpha 0}}$ respectively. This minimization results in a new worst case bound on Eve's uncertainty, correct with probability $1 - \epsilon_{PE}$, which we denote $S_\xi(A|E)$.

With this, we can now calculate the finite key-length rate, r' with Equation 2, with the constraints discussed with Equation

2, though, for our purposes, we are more concerned with evaluating the effective key rate,

$$r = \frac{r'n}{N}, \tag{23}$$

rather than the key rate itself, where n is the number of raw key bits.

III. Evaluation and Comparison

With a key rate equation finalized, we now consider the key rates that are realizable at various noise and signal size scenarios. We consider a symmetric channel, as defined in Equation 1 parameterized on quantum noise level Q, though we note the equations we have derived thus far hold for arbitrary channels. We calculate the expected number of samples C_{ij} that contribute to statistic P_{ij}, for a given α and P_{enc} over N rounds as:

$$\begin{aligned} C_{01} = C_{\alpha\overline{\alpha}} &= \frac{P_{enc}Q}{4}N, \\ C_{10} &= \frac{(1-P_{enc})Q}{2}N, \\ C_{0\alpha} = C_{\alpha 0} &= \frac{P_{enc}(Q+(1-2Q)\alpha^2)}{4}N, \\ C_{1\alpha} &= \frac{(1-P_{enc})(Q+(1-2Q)(1-\alpha^2))}{2}N, \\ C_k &= \frac{P_{enc}(Q+(1-2Q)(1-\alpha^2))}{2}N, \end{aligned}$$

where we use C_k to denote the number of samples that contribute to the raw key. We also note that in practice these values would be observed, and we utilize these expressions only to calculate what they might be expected to be for the purposes of our evaluation.

We will conduct our analysis with $leakEC = 1.2h(QBER)$ to account for practical inefficiencies in error correction protocols, where QBER is the error rate of the raw key string, for which we will use a worst case upper bound of:

$$QBER \leq \frac{P_{01} + \xi(C_{01}) + P_{\alpha\overline{\alpha}} + \xi(C_{\alpha\overline{\alpha}})}{p_{acc}}, \tag{24}$$

where

$$\begin{aligned} p_{acc} = P_{01} &+ \xi(C_{01}) + P_{\alpha\overline{\alpha}} + \xi(C_{\alpha\overline{\alpha}}) \\ &+ 2 - (P_{0\alpha} + \xi(C_{0\alpha}) + P_{\alpha 1} + \xi(C_{\alpha 1})). \end{aligned}$$

Further, in our analysis, we fix the user parameters $\epsilon = 1 \times 10^{-9}$ and $\epsilon_{EC} = 1 \times 10^{-10}$. Additionally, we fix the optimizable parameters $\bar{\epsilon} = 8 \times 10^{-10}$ and $\epsilon_{PE} = 7 \times 10^{-10}$. Finally, we numerically optimized over α and P_{enc} in each case to find an optimal effective key rate in various noise level and signal number. In Figure 1 we show the optimal effective key rate at various noise levels, increasing with N, appearing to numerically approach the asymptotic bound (not shown) at each noise level. In Figure 2, we show the effective key rate for various N as noise increases, where we can see an increasing

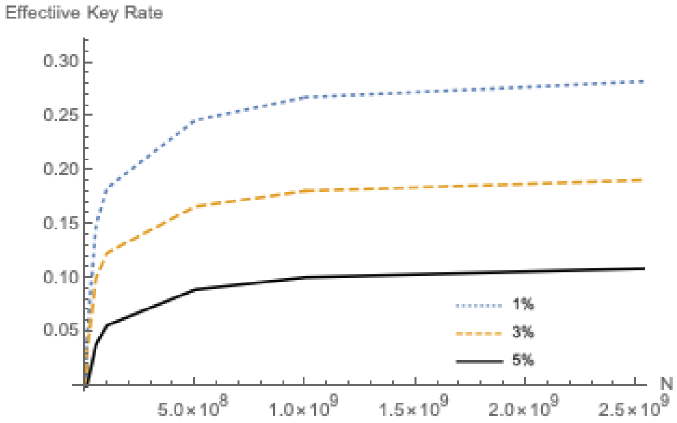

Fig. 1. This figure depicts the effective key rate, optimized over α and P_{enc} for quantum noise levels $Q \in \{.01, .03, .05\}$ and evaluated at $N = 1 \times 10^n$ and $N = 5 \times 10^n$ for $n \in \{6, 7, 8, 9\}$.

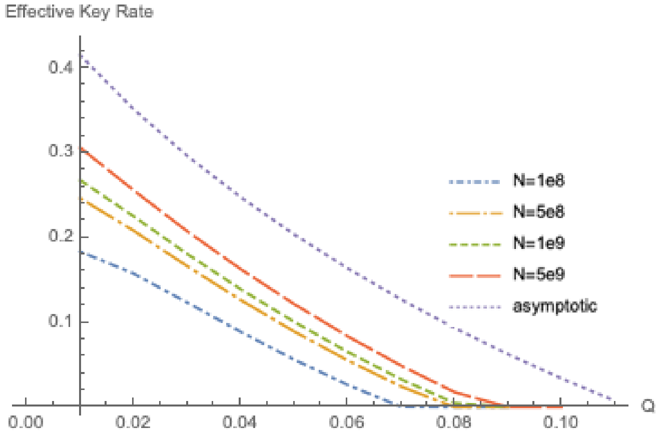

Fig. 2. This figure depicts the effective key rate, optimized over α and P_{enc} for various N, as well as the asymptotic case (the top line), as noise in the channel increases.

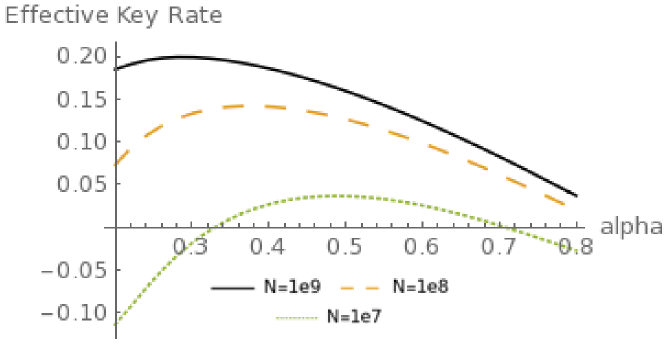

Fig. 3. This chart shows effective key rate as α varies for a fixed $P_{enc} = .8$ at noise level $Q = .02$ for various N. We found that while in the asymptotic case, the optimal α approaches 0 as shown in [5], while in the finite case there is an advantage in optimizing over α (and indeed over P_{enc}) in each şcenario

effective key rate and noise tolerance as N increases, again approaching the asymptotic bound.

In our analysis, we observed that the values of α and P_{enc} that led to the optimal key rate (Equation 2) did not necessarily result in the optimal effective key rate. Additionally we observed that, as N increased, the optimal α decreased while the optimal P_{enc} increased, approaching the asymptotic optimal values of 0 and 1 respectively [5]. Further, we found that for a given P_{enc}, the key rate varied with α as shown by the curves in Figure 3, reaching no more than one positive maximum.

A. Comparisons

As this is the first analysis of extended B92 in the finite setting, we instead compare our results to the performance of standard B92 and BB84 in finite settings. Our analysis shows that the extended variant of B92, which utilizes additional quantum states to better bound $S(A|E)$, results in higher noise tolerance and effective key rates in the finite setting than can be obtained with standard B92. A recent analysis [13] showed that with 10^8 signals, standard B92 achieves a positive key rate up to at least 6.4% noise while our analysis shows that extended B92 has a noise tolerance of at least 7%. Conversely, while the work done in [9] shows that at 5% noise BB84 can achieve positive key rates with as few as 10^5 signals, we do not achieve positive rates at that noise until 10^8 signals.

IV. Closing Remarks

In this work we have, with a rigorous, information theoretic finite key-length analysis, bounded the key rate of the extended B92 protocol under collective attacks on arbitrary channels. We have evaluated that bound under various scenarios for a symmetric channel, and shown that the key rate can be improved by optimizing over P_{enc} and α, noting that the optimal choices for those parameters obey interesting trends.

Future areas of interest in this area include refactoring this analysis to utilize a single POVM for gathering statistics, so as to obtain a tighter confidence interval in Equation 4 as was done in [9]. Further, it may be possible to achieve higher key rates with a tighter bound on QBER than was given in Equation 24. An analysis of achievable key rates and optimal choices under arbitrary channels may also lead to interesting results, as would an investigation of where optimal values for $\bar{\epsilon}$ and ϵ_{EC} lie, which we held fixed in our optimization. Likewise, in the future it may be worthwile to extend this analysis to the include additional test states, rather than the simplified set we use in this work.

Expanding our analysis to include additional practical factors would also be worthwile. In this work we consider idealized photons, in the future it may be interesting to extend our analysis to more practical channel models, perhaps using techniques such as those discussed in [14]. Further such expansions could be made to account for additional imperfections in the channel, source, and detectors used.

References

[1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, pp. 1301–1350, Sep 2009. [Online]. Available: http://link.aps.org/doi/10.1103/RevModPhys.81.1301

[2] S. Pirandola, U. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani *et al.*, "Advances in quantum cryptography," *arXiv preprint arXiv:1906.01645*, 2019.

[3] C. H. Bennett, "Quantum cryptography using any two nonorthogonal states," *Phys. Rev. Lett.*, vol. 68, pp. 3121–3124, May 1992. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.68.3121

[4] R. Matsumoto, "Improved asymptotic key rate of the b92 protocol," *2013 IEEE International Symposium on Information Theory*, Jul 2013. [Online]. Available: http://dx.doi.org/10.1109/ISIT.2013.6620246

[5] M. Lucamarini, G. Di Giuseppe, and K. Tamaki, "Robust unconditionally secure quantum key distribution with two nonorthogonal and uninformative states," *Phys. Rev. A*, vol. 80, p. 032327, Sep 2009. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.80.032327

[6] M. Dušek, M. Jahma, and N. Lütkenhaus, "Unambiguous state discrimination in quantum cryptography with weak coherent states," *Physical Review A*, vol. 62, no. 2, p. 022306, 2000.

[7] K. Tamaki, M. Koashi, and N. Imoto, "Security of the bennett 1992 quantum-key distribution protocol against individual attack over a realistic channel," *Physical Review A*, vol. 67, no. 3, Mar 2003. [Online]. Available: http://dx.doi.org/10.1103/PhysRevA.67.032310

[8] H. Ko, B.-S. Choi, J.-S. Choe, and C. J. Youn, "Advanced unambiguous state discrimination attack and countermeasure strategy in a practical b92 qkd system," *Quantum Information Processing*, vol. 17, no. 1, p. 17, 2018.

[9] V. Scarani and R. Renner, "Quantum cryptography with finite resources: Unconditional security bound for discrete-variable protocols with one-way postprocessing," *Physical review letters*, vol. 100, no. 20, p. 200501, 2008.

[10] W. O. Krawec, "Quantum key distribution with mismatched measurements over arbitrary channels," *Quantum Information and Computation*, vol. 17, no. 3 and 4, pp. 209–241, 2017.

[11] S. M. Barnett, B. Huttner, and S. J. Phoenix, "Eavesdropping strategies and rejected-data protocols in quantum cryptography," *Journal of Modern Optics*, vol. 40, no. 12, pp. 2501–2513, 1993.

[12] S. Watanabe, R. Matsumoto, and T. Uyematsu, "Tomography increases key rates of quantum-key-distribution protocols," *Phys. Rev. A*, vol. 78, p. 042316, Oct 2008. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.78.042316

[13] H. Sasaki, R. Matsumoto, and T. Uyematsu, "Key rate of the b92 quantum key distribution protocol with finite qubits," in *2015 IEEE International Symposium on Information Theory (ISIT)*. IEEE, 2015, pp. 696–699.

[14] A. Kozubov, A. Gaidash, and G. Miroshnichenko, "Finite-key security for quantum key distribution systems utilizing weak coherent states," *arXiv preprint arXiv:1903.04371*, 2019.