*Article*

# Finite Key Size Analysis of Two-Way Quantum Cryptography

**Jesni Shamsul Shaari** [1] **and Stefano Mancini** [2,3,*]

[1] Faculty of Science, International Islamic University Malaysia (IIUM), Jalan Sultan Ahmad Shah, Bandar Indera Mahkota, 25200 Kuantan, Pahang, Malaysia; E-Mail: jesni@iium.edu.my

[2] School of Science & Technology, University of Camerino, I-62032 Camerino, Italy

[3] INFN-Sezione di Perugia, Via A. Pascoli, I-06123 Perugia, Italy

**\*** Author to whom correspondence should be addressed; E-Mail: stefano.mancini@unicam.it.

**Abstract:** Quantum cryptographic protocols solve the longstanding problem of distributing a shared secret string to two distant users by typically making use of one-way quantum channel. However, alternative protocols exploiting two-way quantum channel have been proposed for the same goal and with potential advantages. Here, we overview a security proof for two-way quantum key distribution protocols, against the most general eavesdropping attack, that utilize an entropic uncertainty relation. Then, by resorting to the "smooth" version of involved entropies, we extend such a proof to the case of finite key size. The results will be compared to those available for one-way protocols showing some advantages.

**Keywords:** quantum cryptography; quantum measurement theory; entropy and other measures of information

## 1. Introduction

Two-way quantum key distribution (QKD) schemes have evolved from a theoretic framework in the context of deterministic schemes to experimental realizations for QKD purposes [1]. The protocol is described by a qubit being sent from one party, say, Bob, to another, Alice, for her encoding before being sent back to him for a measurement to ascertain Alice's encoding. Standing in stark contrast to BB84 like prepare and measure schemes where information encoding is simply in the choice of states and bases of qubits to be sent from the encoding party to the receiver [2], the case for two-way QKDs is really in the choice of unitary transformations by an encoding party that would act on the qubits

traveling to and fro between the legitimate parties. This naturally makes use of the quantum channel twice. Another peculiarity of the above-mentioned two-way protocols would be how its security is to be ensured. The protocols' runs are divided into two modes, namely the encoding mode (EM) where message encoded by Alice is followed by measurements by Bob for decoding purposes and the control mode (CM) where Alice would make projective measurements in randomly selected bases such that when the bases coincide with Bob's then errors can be ascertained. The distribution of the EM and CM would be determined by a factor $c$, with $0 < c < 1$, *i.e.*, the probability of Alice randomly choosing an EM. While messages (bits of raw key) are transmitted via the EM, CM has the critical role of estimating the amount of errors in the channels to ascertain Eve's information gain.

However, despite its early introduction in 2002 [3], and varying versions that followed, it was only about a decade later that a proper proof for one specific two-way protocol was found for unconditional security in [4] and a proof for a purified version was reported in [5]. In [4], the proof was done for the specific case of non-entangled qubits in one of four states coming from two mutually unbiased bases (this protocol has been referred to as LM05 [6] and we shall refer to it as such hereafter). In [5], a purification of two two-way QKD protocol, namely the Super Dense Coding scheme (SDC) and LM05 was done in order to provide a security proof.

Unconditional security proofs provide for an information theoretic security picture of QKD. However, a very important fact that sets constraints within the operational context would be the issue of how such proofs are based on asymptotic analysis that holds true only for infinitely long keys; the concern regarding the security nature of realistic keys, which are finitely long, becomes evident. This has spurred a number of studies including [7–9].

The central feature of this work is a review of the security analysis done based on protocol purifications in [5] and a natural generalization to the the case for finite sized keys. We begin with a quick description of two most relevant two-way QKD protocols followed by their purifications. After a brief on smooth entropies and its application to deriving finite key rates, we provide finite secure key rates in terms of efficiency for both protocols. These will then be compared to an asymmetrical BB84; essentially a BB84 protocol with one basis preferred over another mainly for a more efficient scenario compared to a standard BB84 where choices of bases are equiprobable [8,10].

## 2. Two-Way Protocols

The SDC protocol in some sense is closer to the earlier instances of two-way protocols, namely the Ping-Pong [3] and more specifically its improved version [11] which provides for a higher protocol capacity in terms of the number of classical bits encoded in each EM run. It is however more resource demanding as it requires the use of a quantum memory on Bob's side. Our description of SDC here follows closely that of [5]. Very simply, the SDC protocol sees Bob sending half a Bell pair to Alice (while storing the other half in a quantum memory) for her to encode by virtue of a randomly chosen unitary transformation from the set containing the identity operator and the three Pauli operators, $\{I, \sigma_x, \sigma_y, \sigma_z\}$. She would subsequently submit the qubit back to Bob for measurements. Alternatively, she could measure the received qubit in the $Z$ basis and prepare another in the $X$ basis to be sent to Bob. The former process, done with probability $c \approx 1$, corresponds to her actions in EM, while the latter, done

with probability $1 - c$, corresponds to CM. Despite the use of $4$ unitaries imply a larger alphabet used, particularly elements of $\mathbb{Z}_4$ $0, 1, 2, 3$ mapped to $I, \sigma_x, \sigma_y, \sigma_z$ respectively as opposed to bits for encoding, Alice could in fact assign logical bits (in pairs) $00, 10, 11$ and $01$ to the unitaries. However the mapping $f : \mathbb{Z}_4 \rightarrow \mathbb{Z}_2^2$ to bits should be done only at the end of the protocol to avoid any possibility of Eve capitalizing on the correlation of bits given any pair [12].

Bob, on the other hand would, with a probability $c$ make a Bell measurement and with probability $1-c$ measure his stored and received qubit in the $Z$ and $X$ basis respectively. A protocol run which sees Bell measurements by Bob coinciding with Alice's unitary transformations would allow Bob to distinguish between Alice's unitaries perfectly (given that the Pauli matrices would shift between orthogonal Bell states). Assigning logical symbols $0, 1, 2$ and $3$ to the Bell states $|\psi^+\rangle, |\psi^-\rangle, |\phi^+\rangle$ and $|\phi^-\rangle$ respectively, these instances referred to as EM provide for sharing of a raw key between Alice and Bob. Again, it is possible for Bob to use bits instead when Alice submits the mapping information to Bob at the end of the protocol runs. The instances when Alice's and Bob's measurements in the $Z$ and $X$ bases coincides would allow for a meaningful CM. Hence a successful EM happens only with probability $c^2$ and CM happens with probability $(1 - c)^2$. A schematic diagram for SDC is illustrated in Figure 1 below.
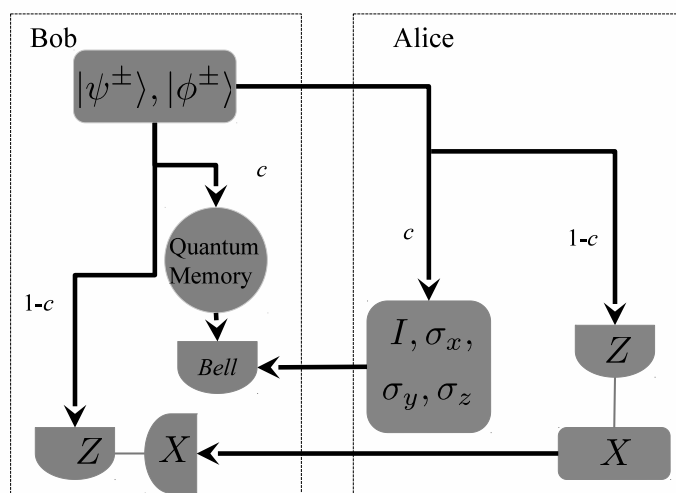


**Figure 1.** Schematic diagram for SDC. Arrows represent the distribution of qubits in the channels between Alice and Bob. The arrows in Bob's and Alice's stations both see branchings with probability $c$ or $1 - c$ for EM or CM respectively.

The case for a two-way QKD without using entanglement, namely the LM05, sees a qubit prepared by Bob in a particular bases randomly chosen from either the $X$ or $Z$ with probabilities $p_X$ and $p_Z$ respectively to be sent to Alice for her encoding. In the original LM05 protocol, apart from $p_X = p_Z$, only two unitary transformations were considered, namely the passive $I$ and $i\sigma_y$. In [5], a generalization was made to include another two unitary transformation, namely the $\sigma_x$ and $\sigma_z$, and the possibility of having different probabilities $p_X$ and $p_Z$. In this protocol, upon executing her unitary transformation, Alice would resubmit the qubit to Bob who would measure in the same basis he prepared in. Defining the eigenstates of $\sigma_z$ and $\sigma_x$ as $|z\pm\rangle$ and $|x\pm\rangle$ respectively, bit values $0$ may be assigned to the states $|z+\rangle$ or $|x+\rangle$ and $1$ to the states $|z-\rangle$ or $|x-\rangle$. Bob then adds (modulo 2) the bit value corresponding to

his prepared state (prior sending to Alice) to the bit value corresponding to his measurement result of the state (after Alice's encoding). We will mention shortly what Alice needs to do in order to share bit-wise information with Bob. This run of the protocol corresponds to an EM.

With the probability $1 - c$, Alice would make measurements of the qubit she receives instead in either the $Z$ or $X$ bases for CM purposes. A schematic diagram for LM05 is shown in Figure 2 below.
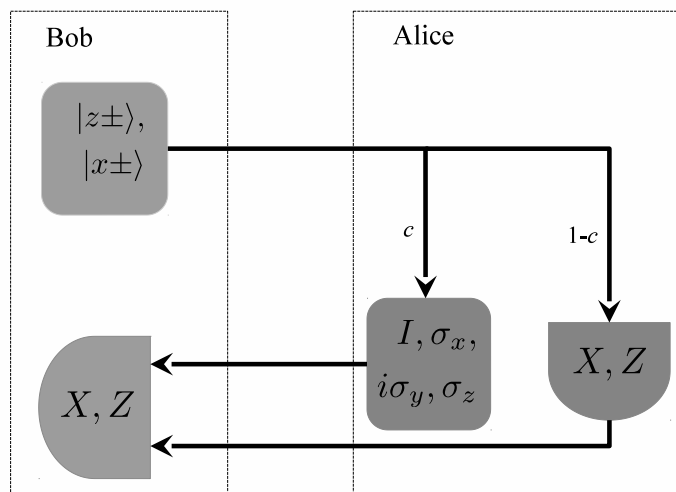


**Figure 2.** Schematic diagram for LM05. Arrows represent the distribution of qubits in the channels between Alice and Bob. Note that the arrow in Alice's station branches off with probability $c$ or $1 - c$ for EM or CM respectively.

Apart from the use of non entangled qubits by Bob, another obvious difference with the SDC is in the possible options in the post processing feature of the protocols. In SDC, post processing only includes Alice's and Bob's discussion to ascertain which signals were to be used for EM and CM purposes apart from error estimations, error corrections and privacy amplifications. In the LM05 on the other hand, Alice and Bob have the option to commit to either direct reconciliation (DR) or reverse reconciliation (RR) which would determine the type of information to be disclosed over an authenticated public channel. In the case of RR, Bob should disclose the bases he prepared and measured qubits in. Using the same assignment of logical bit pairs to unitary transformations as in SDC, Alice would keep only the first bit of the pair when Bob uses $Z$ and the second when Bob uses $X$. On the other hand, if a RR is considered, then Alice would reveal from which of the two sets, $S_0 = \{I, i\sigma_y\}$ and $S_1 = \{\sigma_x, \sigma_z\}$ was the transformation she had used and only the first bit of the bit pair for each transformation is used. This revelation is necessary given Bob's measurement in the $X$ basis would give him an erroneous bit when Alice uses $S_1$. In these cases, Bob would need to flip his bit.

## 2.1. Purifications of Two-Way Protocols

The approach to the security proof presented in [5] is based on the notion of purification of protocols where the protocols can be described by the measurements made by Alice and Bob on a system provided to them by Eve [13]. Writing the measurements of Alice and Bob as Probability Operator Value Measure

(POVM) maps $M_A^{\text{EM}}$ and $M_B^{\text{EM}}$ respectively in EM (or $M_A^{\text{CM}}$ and $M_B^{\text{CM}}$ in CM), the state after the measurements is given by

$$M_A^i \otimes M_B^i(\rho_{ABE}) \tag{1}$$

with $i = $ EM or CM. In the purified version of both the SDC and the LM05 as reported in [5], $\rho_{ABE}$ is a state in the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$ (Alice's, Bob's and Eve's respectively) and $\mathcal{H}_A$ and $\mathcal{H}_B$ are Hilbert spaces for two qubit systems each. Alice's measurement $M_A^{\text{EM}}$, in EM which acts on a two qubit system must be in such a way that it is equivalent to her encoding operation in the protocols. If we recall how in both protocols, Alice receives a state from Bob and resends after a unitary encoding on the state, $M_A^{\text{EM}}$ can be understood as a (POVM) acting on the received state with half of some entangled state so as the other half of the entangled state (after the measurement $M_A^{\text{EM}}$) is the same as the output from Alice's encoding to be sent to Bob [14]. Thus we can imagine $\rho_{ABE}$ as that pure state which distributes a pair of qubits to Alice and Bob each. Alice's measurement on the two received qubits, $\text{tr}_{BE}(\rho_{ABE})$ would ensure that Bob's measurement, $M_B^{\text{EM}}$ on his received pair, $\text{tr}_{AE}(\rho_{ABE})$ is equivalent to Alice making a unitary transformation on Bob's prepared qubit for his subsequent decoding measurement. With regards to Bob's measurements, $M_B^{\text{EM}}$, it is instructive to note that in SDC, $M_B^{\text{EM}}$ is really the Bell measurement for decoding purposes while in LM05, Bob's measurement on the first half of $\text{tr}_{AE}(\rho_{ABE})$ effectively prepares the qubit state sent to Alice (in the forward path) while his other measurement is on the other half of $\text{tr}_{AE}(\rho_{ABE})$. The measurements $M_A^{\text{CM}}$ and $M_B^{\text{CM}}$ would then correspond to relevant local measurements of each qubit in the qubit pairs in CM (detailed in the ensuing section). Given these, the main ingredient in the security proof for the purified protocols is based on bounding Eve's information gain given Bob-Alice's using an uncertainty relation which measures the overlap of Bob's (Alice's) measurements, *i.e.*, $M_B^{\text{EM}}, M_B^{\text{CM}}$ ($M_A^{\text{EM}}, M_A^{\text{CM}}$) in a reverse (direct) reconciliation scenario.

### 2.2. Measurements and Entropic Uncertainty Relations

Entropic uncertainty relations are used in some security proofs of particular QKD protocols given its power to describe bounds of uncertainty parties may share of a certain quantum system, say $B$. In its simplest description, it is simply Heisenberg's uncertainty principle in an entropic form first proven by [15]. It was later generalized [16–18] to include correlation of the system to be measured with disjoint (possibly quantum) systems $A$ and $E$ given by

$$H(X|E) + H(Z|A) \geq -\log_2 \mathcal{C}, \tag{2}$$

where $X$ and $Z$ are results from POVMs $\mathbb{X}$ and $\mathbb{Z}$ respectively on $B$. Writing the POVM elements of $\mathbb{X}$ and $\mathbb{Z}$ as $\{E_x^{\mathbb{X}}\}$ and $\{E_z^{\mathbb{Z}}\}$ respectively, the term $\mathcal{C}$ is given by

$$\mathcal{C} = \max_{x,z} \left\| \sqrt{E_x^{\mathbb{X}}} \sqrt{E_z^{\mathbb{Z}}} \right\|_\infty^2. \tag{3}$$

Equation (2) together with the Devatak-Winter security bound [19] is employed in [5] to provide a security proof for the purified SDC and LM05 protocols. In order to make use of such an entropic relation, [5] necessarily describes the term $\mathcal{C}$ as the (effective) overlap between Bob's measurements in a RR picture. Given the assumptions in [5], Bob's measurements in the purified SDC protocol are either

the Bell measurements or a measurement that can be described as $\sigma_z \otimes \sigma_x$ where the overlap between the POVM elements as defined in Equation (3) is $1/4$. This maximal overlap is achieved when considering the overlap between the POVM elements in EM and that of in CM. If we let the measurements by Alice and Bob to result in the strings $S_A^{\mathrm{EM}}$ and $S_B^{\mathrm{EM}}$ respectively from EM and $S_A^{\mathrm{CM}}$ and $S_B^{\mathrm{CM}}$ respectively from CM, and Eve's system as $E$ we can bound Eve's information based on Equation (2) as

$$H(S_B^{\mathrm{EM}}|E) + H(S_B^{\mathrm{CM}}|S_A^{\mathrm{CM}}) \geq 2. \tag{4}$$

The key rate of the SDC, $R_{SDC}$, is given by the Devetak-Winter rate [19]

$$R_{SDC} \geq H(S_B^{\mathrm{EM}}|E) - H(S_B^{\mathrm{EM}}|S_A^{\mathrm{EM}}). \tag{5}$$

With $H(S_B^{\mathrm{CM}}|S_A^{\mathrm{CM}})$ upper bounded by $h_4(\overline{q}_{\mathrm{CM}})$, $H(S_B^{\mathrm{EM}}|S_A^{\mathrm{EM}})$ by $h_4(\overline{q}_{\mathrm{EM}})$ where $h_4$ is the 4-ary Shannon entropy and $\overline{q}_{\mathrm{CM}}$ and $\overline{q}_{\mathrm{EM}}$ are errors in Alice's and Bob's strings in CM and EM respectively, applying the bound of Equation (4) we arrive at

$$R_{SDC} \geq 2 - h_4(\overline{q}_{\mathrm{CM}}) - h_4(\overline{q}_{\mathrm{EM}}). \tag{6}$$

It is instructive to note that the errors $\overline{q}_{\mathrm{CM}}$ and $\overline{q}_{\mathrm{EM}}$ affects a two-bit message transmission resulting from a use of two noisy channels and thus comes as a triple; namely error exclusively in either one channel, say $q_1^a$ and $q_2^a$ as well as errors in both channels, $q_3^a$ for $a = \mathrm{CM}, \mathrm{EM}$. Hence,

$$h_4(\overline{q}_a) = -\sum_{i}^{3} q_i^a \log_2 q_i^a - (1 - \sum_{i}^{3} q_i^a) \log_2 \left(1 - \sum_{i}^{3} q_i^a\right). \tag{7}$$

It is certainly possible to consider the entropic bounds dictated by the overlap of Alice's measurements instead of Bob's as shown above. The key rate would remain the same nonetheless.

A similar line of argument can be applied to the LM05 protocol; though the measurements made for decoding purposes by Bob would be $\mathcal{Z} = \sigma_z \otimes \sigma_z$ or $\mathcal{X} = \sigma_x \otimes \sigma_x$ followed by an XOR of the measurements' results to reveal the encoding done by Alice in the EM. Another set of measurements, which would be useful for the CM would be $\mathcal{Z}_C = \sigma_z \otimes I$ or $\mathcal{X}_C = \sigma_x \otimes I$ where the maximal overlap between the POVM elements for measurements made in EM and that in CM is $1/2$. Using the relevant entropic bounds (similar to SDC though the overlap is now $1/2$ instead of $1/4$), the key rate for LM05, $R_{LM05}$ can be easily shown to be

$$R_{LM05} \geq 1 - h_2(q_{\mathrm{CM}}) - h_2(q_{\mathrm{EM}}), \tag{8}$$

where $h_2$ is the binary Shannon entropy and $q_{\mathrm{CM}}$ and $q_{\mathrm{EM}}$ are the errors in the CM and EM respectively.

The above key rates are derived from inequalities based on terms that are meaningful only within the infinitely long key limits and is thus unsatisfactory from an operational and practical perspective. In the following subsection, we shall review briefly the notion of smooth entropies and relevant entropic bounds that we shall use to derive a finite key rate for SDC and LM05.

### 2.3. Smooth Entropies and Finite Keys

The smooth entropy is defined based on the conditional entropy. More rigorously, following the definition given in [20] for a bipartite state $\rho_{BE}$ on $B$ and $E$, the entropy of $B$ given $E$ is defined as

$$H_{min}(B|E) = \max_{\sigma_E} \sup \{\lambda \in \mathbb{R} : 2^{-\lambda} I_B \otimes \sigma_E \geq \rho_{BE}\} \tag{9}$$

where the maximum is taken overall states $\sigma_E$ in $E$ and $I_B$ is the identity on $B$. The $\epsilon$-smooth min-entropy for $\epsilon \geq 0$ is then defined as

$$H_{min}^\epsilon(B|E) = \max_\rho H_{min}(B|E). \tag{10}$$

with maximization over all bipartite states $\rho$ on $B$ and $E$ with a purified distance [21] to $\rho_{BE}$ not exceeding $\epsilon$. The smooth max-entropy is defined as the dual of the smooth min-entropy with regards to any purification of $\rho_{BE}$.

For the tripartite state $\rho_{ABE}$ and POVMs $\mathbb{X}$ and $\mathbb{Z}$ respectively on $B$ (resulting in bit strings $X$ and $Z$), from [20], the smooth min-entropy of $X$ conditioned on $E$, $H_{min}^\epsilon(X|E)$, gives the number of bits contained in $X$ that are $\epsilon$-close [22] to a uniform distribution and independent of $E$. The smooth max-entropy of $Z$ conditioned on $A$, $H_{max}^\epsilon(Z|A)$, gives the number of bits needed to reconstruct $Z$ from $A$ up to a probability of failure $\epsilon$ and the generalized uncertainty relation involving smooth entropies is given as [20]

$$H_{min}^\epsilon(X|E) + H_{max}^\epsilon(Z|A) \geq -\log_2 \mathcal{C}. \tag{11}$$

In identifying the measurements and results in both the SDC and LM05 with Equation (11), similar to the above, $H_{min}^\epsilon(X|E)$ will be identified with Eve's correlation with Bob's string (in EM) while $H_{max}^\epsilon(Z|A)$ is to be identified with Alice's and Bob's in CM. There are two points worth mentioning with regards to the measurements made in CM. The first is in particular reference to LM05's measurements $\mathcal{Z}_C$ and $\mathcal{X}_C$ where a passive operation is noted on the second qubit (received in the backward path). This does not necessarily require Bob to *not* measure the qubit in the backward path; rather he could just ignore the measurement made and consider only the result of his first measurement [23]. In other words, in the cases Alice note a particular round of the protocol is a CM, Bob would ignore the result of his measurement on the second qubit. If it was the EM, then both the measurement results would be XOR-ed for decoding purposes.

The second point is that as the $\sigma_z \otimes \sigma_x$ in SDC and $\mathcal{Z}_C$ and $\mathcal{X}_C$ in LM05 happens only in CM, one can see the protocol as analogous to the asymmetrical prepare and measure protocol of BB84 where the measurements in EM is seen as measurements in the preferred basis in the asymmetrical BB84. In the case for the latter, in [9], where measurements are made in the $X$ and $Z$, a *gedankenexperiment* was considered where all measurements were done in the $Z$ basis to establish an uncertainty relation. Following [9], in the case for the LM05, we can use the bits derived in the CM to provide for an estimation of the errors in the application of the uncertainty relation using a similar *gedankenexperiment* where all rounds are CM; and since Bob can choose to measure for EM, security follows from the notion that the better Alice could estimate Bob's bits in CM, the worse would Eve's estimation of Bob's bits in EM.

## 3. Efficiency and Secure Key Rates

In what follows, we shall assume implementations of the two-way protocols using depolarizing channels. The depolarizing channel, $\mathcal{D}$ is described by the parameter $q$, such that $0 \leq q \leq 1$, which affects a quantum state, $\rho$ independent of the basis as such

$$\rho \mapsto \mathcal{D}(\rho) = (1 - q)\rho + qI/2. \tag{12}$$

For two-way protocols, the use of depolarizing channels can be categorized as either independent or correlated channels. Such a correlation can be understood in terms of the errors estimated in the forward and backward paths in CM against errors in EM. Given bit wise errors $e_1$ and $e_2$ in the forward and backward paths respectively, we say the channels are independent provided the errors in EM is given by $e_m = e_1(1 - e_2) + e_2(1 - e_1)$. Otherwise they are correlated [24]. While the case for independent channels are unique by definition, the cases for correlated channels can be infinitely many. However, we shall only consider, as in [5] correlated channels where $e_1 = e_2 = e_m$.

To ascertain a finite key rate for the two-way protocols given such implementation, we need to determine the distribution of finite number of bits between the EM and the CM. Choices of the value of $c$ for both protocols would determine this and ultimately how much of a key rate one can have. Hence, in order to determine the optimal value for $c$, assuming one has a value of $k$ for bits in CM and $n$ in EM (more precisely the cases where Alice's encoding measurements coincide with Bob's decoding measurements), the total number qubits, $M(n, k)$ sent [25] before $n$ bits are derived from EM and $k$ for CM estimation can be made is given by probability value $c = (\sqrt{1 + k/n})^{-1}$. This is immediately derived from modelling the protocol based on [9].

Subsequently, the already mentioned *gedankenexperiment* will provide for an uncertainty relation of Equation (11) and the smooth-max entropy term for an $n$-bit string, $Z$ given $C$, $H^{\epsilon}_{max}(Z|C)$ would be upper bounded by $nh_2(Q + \mu(n, k))$ where

$$\mu(n, k) = \sqrt{\frac{n + k}{nk} \frac{k + 1}{k} \ln \frac{2}{\epsilon_S}}, \tag{13}$$

with the strings $Z$ and $C$ derived from CM differing at $Q$ bits. The parameter $\epsilon_S > 0$ is a security parameter as defined in [9].

Strings shared between Alice and Bob in the EM, which one party's may be characterized as having errors $e$ relative to the other need be subjected to an error correction procedure. This can conventionally be understood as the amount of pre shared secret bits invested in the communications for error correction purposes [26].

The Leftover Hashing Lemma [27] then provides for the length of the secret key as

$$L = \lfloor H^{\epsilon}_{min}(X|E) + 2\log 2\epsilon \rfloor, \tag{14}$$

which is $2\epsilon$ close to a bit string which is uniform and independent of Eve's knowledge.

The efficiency of the protocol, $\mathcal{E}$ can be defined based on the amount of resources in terms of number of qubits required,

$$\mathcal{E} = L/M(n, k). \tag{15}$$

It should be noted that for SDC, a factor of 2 should be further multiplied to the denominator reflecting the use of entangled pairs. As in [9], we do not include any classical bits necessary in the protocol unlike [28].

### 3.1. Finite Key Analysis for SDC

We let a total of $2M(n,k)$ pairs of qubits travel to and fro between Bob and Alice with the latter committing to encoding with probability $c$. Thus one gets $n$ amount of quaternary digits from the EM. Following earlier notation, the $n$ quaternary strings of Alice and Bob are $S_A^{\mathrm{EM}}$ and $S_B^{\mathrm{EM}}$ respectively while the $k$ quaternary strings derived from the CM are $S_A^{\mathrm{CM}}$ and $S_B^{\mathrm{CM}}$ respectively. Considering a *gedankenexperiment* where all runs are CM lets us bound Eve's information on the $n$ quaternary string using Equation (11) as

$$H_{min}^{\epsilon}(S_B^{\mathrm{EM}}|E) + H_{max}^{\epsilon}(S_B^{\mathrm{CM}}|S_A^{\mathrm{CM}}) \geq 2n. \tag{16}$$

The term $H_{min}^{\epsilon}(S_B^{\mathrm{EM}}|E)$ is the smooth min-entropy of $S_B^{\mathrm{EM}}$ conditioned on $E$. It reflects Eve's correlation with Bob's string in the EM giving the number of bits contained in $S_B^{\mathrm{EM}}$ that are $\epsilon$-close to a uniform distribution and independent of $E$. In ascertaining the term $H_{max}^{\epsilon}(S_B^{\mathrm{CM}}|S_A^{\mathrm{CM}})$ reflecting the correlation between Bob's and Alice's strings, the case for two way channels with depolarization $q$ each allows us to consider bit error rate in qubit measurements as $q/2$ for each channel instead of a channel transmitting quaternary digits instead. Thus in this case,

$$h_4(\overline{q}) = 2h_2(q/2), \tag{17}$$

for $\overline{q} = ((1-q/2)q/2, (q/2)(1-q/2), q^2/4)$. The number of bits required to reconstruct $S_B^{\mathrm{CM}}$ from $S_A^{\mathrm{CM}}$ (as two $n$ bit length strings) up to a probability of failure $\epsilon$,

$$H_{max}^{\epsilon}(S_B^{\mathrm{CM}}|S_A^{\mathrm{CM}}) \leq 2nh_2\left(\frac{q}{2} + \mu(n,k)\right), \tag{18}$$

where $q/2$ is the error rate for each independent depolarizing channel in the CM. If we write the smooth max-entropy of Alice's string conditioned on Bob's in EM as $H_{max}^{\epsilon}(S_B^{\mathrm{EM}}|S_A^{\mathrm{EM}}) \leq nh_4(\mathcal{Q}_E)$ with $\mathcal{Q}_E$ as errors in the EM, then Equations (14), (16) and (18) gives the key length after error correction and privacy amplification as

$$L_{SDC} \leq n\left[2 - 2h_2\left(\frac{q}{2} + \mu(n,k)\right) - h_4(\mathcal{Q}_E)\right] - \log\frac{2}{\epsilon_S^2}, \tag{19}$$

where from [9], we have the term $nh_4(\mathcal{Q}_E)$ as the amount of information leaked to Eve due to error correction [30] of the string $S_A^{\mathrm{EM}}$ and $\log(\epsilon_S^2)$ results from the quantum Leftover Hashing Lemma [27].

### 3.2. Finite Key Analysis for LM05

In this work, we will consider the LM05 protocol with Bob's choice for qubit preparation and measurement in the $Z$ bases is preferred ($p_Z > p_X$) and Alice either encodes with anyone of her transformations with probability $c/4$ or make measurements in the $X$ bases only with probability $1-c$. Furthermore, the deliberations ensue would be focused on the RR scenario. Alice's and Bob's choice of

measuring $2M(n,k)$ qubit pairs in the basis $X$ with probability $1-c$ results in $n_e = n + \sqrt{nk}$ number of bits derived from EM and $k$ for CM. Hence $\sqrt{nk}$ pairs would be wasted due to bases mismatch when Alice measures in $X$ while Bob chooses $Z$ (notice that $2\sqrt{nk}$ qubits are wasted in [9] for similar reasons).

Let us write the string Bob has in the EM and CM as $s_B^{EM}$ and $s_B^{CM}$ respectively as well as Alice's as $s_A^{EM}$ and $s_A^{CM}$ respectively. As described above, let us consider a *gedankenexperiment* where all qubits are measured using $X$ basis (for CM), we can therefore write an uncertainty relation from Equation (11) to bound Eve's information as

$$H_{min}^{\epsilon}(s_B^{EM}|E) + H_{max}^{\epsilon}(s_B^{CM}|s_A^{CM}) \geq n_e. \tag{20}$$

Similar to earlier discussions, the first term in the left hand side of the above equation is the smooth min-entropy reflecting the number of bits contained in Bob's string, $s_B^{EM}$ that are $\epsilon$-close to a uniform distribution and independent of Eve. The second term $H_{max}^{\epsilon}(s_B^{CM}|s_A^{CM})$ reflects the correlation between Bob's and Alice's strings and gives the number of bits needed to reconstruct $s_B^{CM}$ from $s_A^{CM}$ up to a probability of failure $\epsilon$,

$$H_{max}^{\epsilon}(s_B^{CM}|s_A^{CM}) \leq n_e h_2\left(\frac{q}{2} + \mu(n_e, k)\right). \tag{21}$$

With $Q_f$ as the error rate in EM, noting $H_{max}^{\epsilon}(s_B^{EM}|s_A^{EM}) \leq n_e h_2(Q_f)$ and following Equations (14), (20) and (21), the key length after error correction and privacy amplification is given by

$$L_{LM05} \leq n_e - n_e h_2\left(\frac{q}{2} + \mu(n_e, k)\right) - n_e h_2(Q_f) - \log \frac{2}{\epsilon_S^2}. \tag{22}$$

## 4. Numerical Results and Comparisons

In making use of the key rate formulae of Equations (19) and (22) above, we need to first assume a value for the security parameter $\epsilon_S$, for which we set as $10^{-10}$. Then, for a given value for errors in the CM (errors in EM is then immediately defined), setting the number for $M(n,k)$, we determine the value $k$ which achieves the maximal value for secure key length. As $M(n,k)$ approaches infinite for $n \to \infty$, following [9] we could let $k < \mathcal{K}\sqrt{n}$ for some fixed $\mathcal{K}$, so that

$$\lim_{n \to \infty} \mu(n,k) = 0, \tag{23}$$

and consider secure keys within the infinite key regime. In the infinite key regime, the efficiency for the protocols SDC becomes

$$\lim_{n \to \infty} L_{SDC}/2M(n,k) = 1 - h_2\left(\frac{q}{2}\right) - \frac{h_4(\mathcal{Q}_E)}{2}, \tag{24}$$

and for LM05 we have

$$\lim_{n \to \infty} L_{LM05}/M(n,k) = 1 - h_2\left(\frac{q}{2}\right) - h_2(Q_f). \tag{25}$$

It is worth noting that the 'additional' term $\sqrt{nk}$ for amount of bits that can be derived from EM in LM05 becomes negligible in the infinite key regime and $\lim_{n\to\infty} \sqrt{nk}/M(n,k) = 0$. Furthermore, for this condition, it would be only the final term (related to error correction) that would determine how one protocol outperforms another.

### 4.1. Independent Channels

In Figures 1 and 2, we present the results for implementations of the SDC and LM05 for independent channels compared to the asymmetrical BB84 in terms of protocol efficiency against errors. In this case, the error rates for SDC and LM05 in EM are given by $2q/2(1 - q/2)$ and $(2q - q^2)/4$ respectively [5].

We can observe that there are particular regions where LM05 outperforms both SDC and BB84. Generally, this can be understood when considering the competing terms of the extra $\sqrt{nk}$ contributing to LM05's raw key versus the amount of bits to be discarded due to error correction. For LM05, this is given by $h_2[2q/2(1 - q/2)]$, SDC's $h_4[(2q - q^2)/4]/2$ while for BB84, it is simply $h_2(q/2)$ where

$$h_2[2q/2(1 - q/2)] \geq h_4[(2q - q^2)/4]/2 \geq h_2(q/2), \tag{26}$$

with equality only at $q = 0$ or $q = 1$. The term $\sqrt{nk}$ is most dominant for relatively small values of $n$, hence LM05's best performance of the three in Figure 3 where $M(n, k) = 10^4$. In the same figure we see instances when the errors are big enough and outweighs the contribution from $\sqrt{nk}$, LM05 performs poorly compared to BB84. The error correction term for SDC is only very slightly better than that of LM05 in the infinite key regime, explaining why it still does not exceed LM05's $\sqrt{nk}$ advantage in the finite key scenario here. Thus LM05 exceeds BB84 up to an error rate of about $2.7\%$. However, in Figure 4 where the number of qubits used, $M(n, k) = 10^7$, LM05 exceeds BB84 only up to about $1\%$ and SDC's up to $3.8\%$. The plot of the protocols' efficiency against $M(n, k)$ for the error of $0.01$ in Figure 5 exhibits the convergence of the efficiencies as the number of qubits used increases up to $10^7$. These results clearly emphasizes LM05's determinism over the asymmetric BB84's. It is worth recalling the fact that while LM05 claims deterministic status in terms of the absence for bases mismatch in EM, BB84 only approximates this (in the infinite key regime). Figure 6 exhibits the case for the three protocols in the infinite key regime.
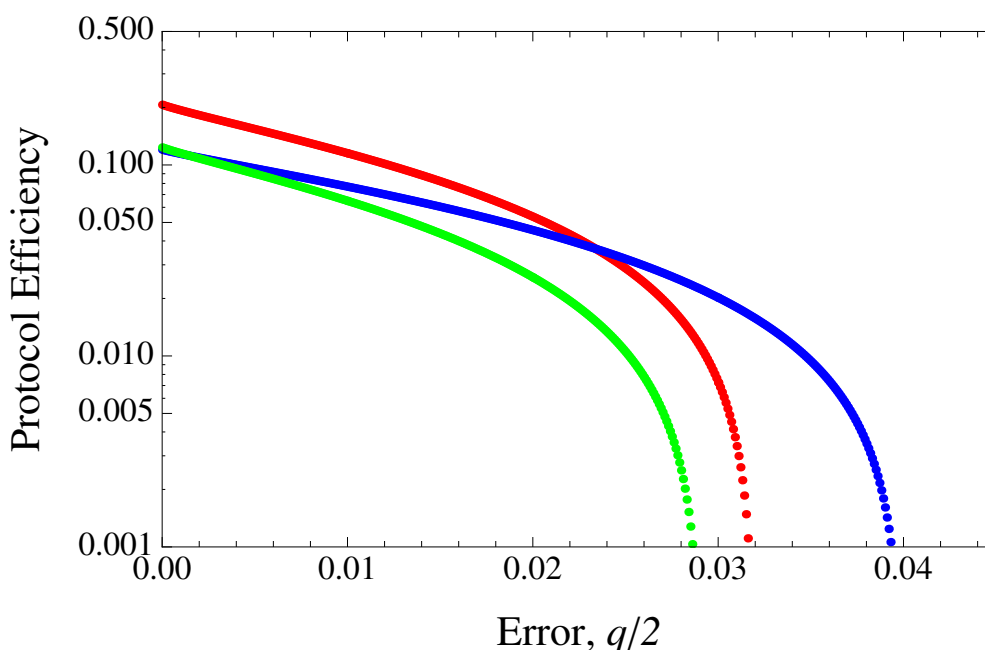


**Figure 3.** Efficiency for Asymmetrical BB84 (blue), LM05 (red) and SDC (green) against error rate $q/2$ given independent channels for total qubit used as $M = 10^4$.
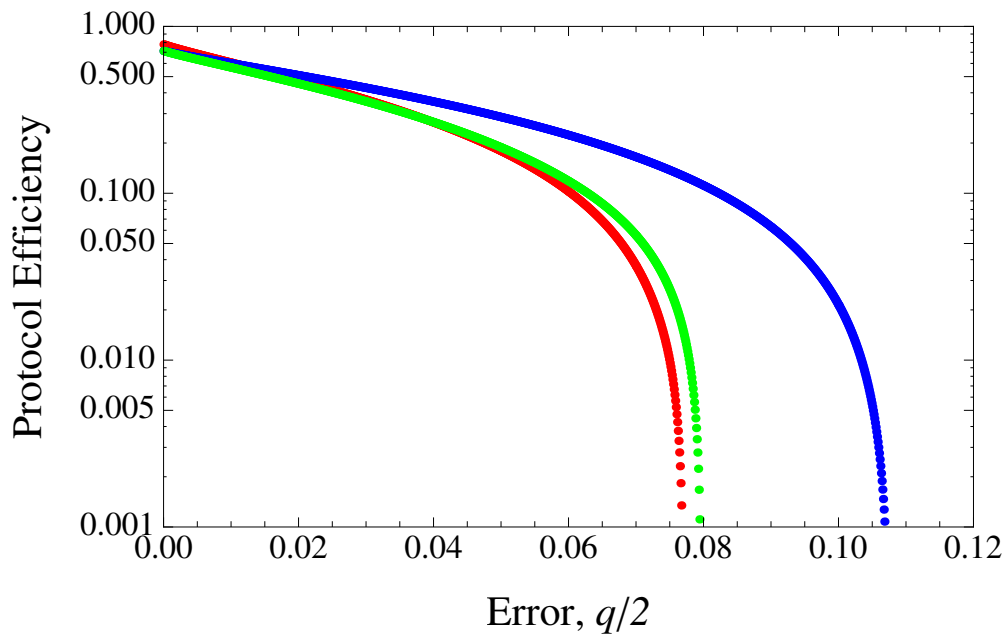
**Figure 4.** Efficiency for Asymmetrical BB84 (blue), LM05 (red) and SDC (green) against error rate $q/2$ given independent channels for total qubit used as $M = 10^7$.
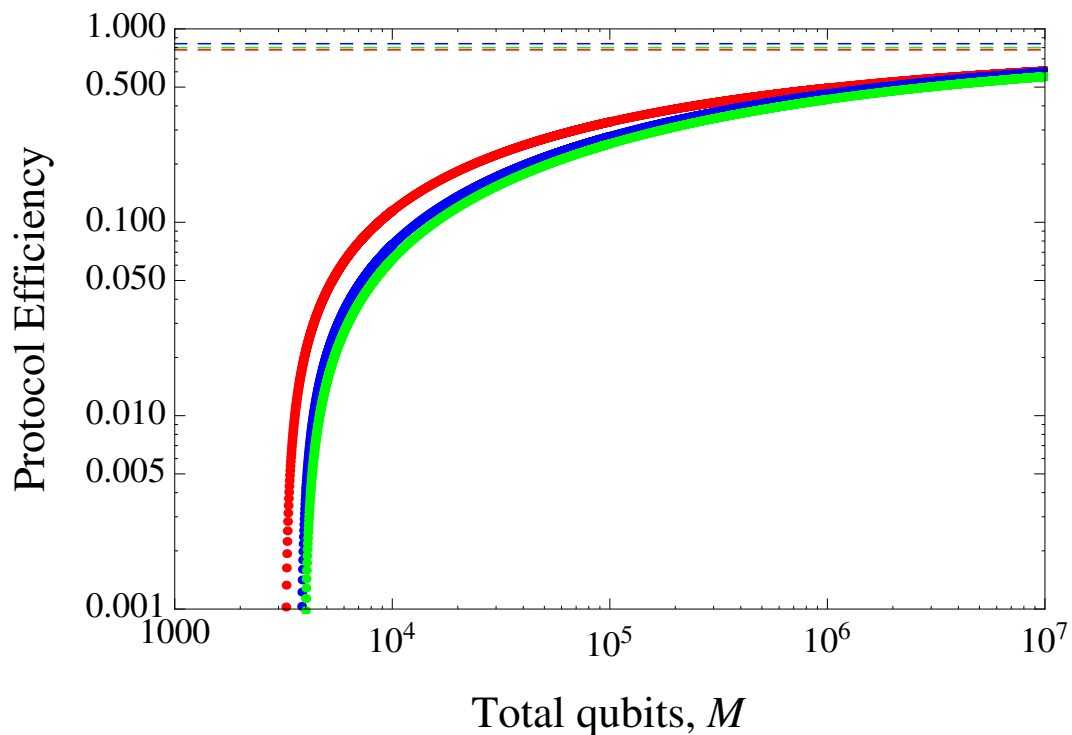


**Figure 5.** Efficiency for Asymmetrical BB84 (blue), LM05 (red) and SDC (green) against total qubit used, $M$ (for SDC, it is to be understood as total pairs used) for error rate $0.01$. The horizontal dashed lines represents the infinite key regime.
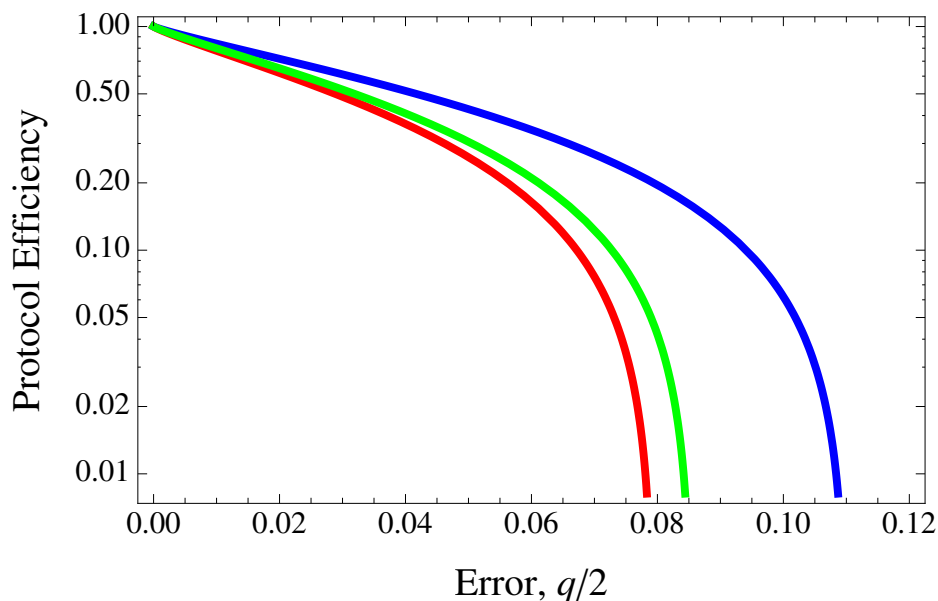
**Figure 6.** Efficiency for Asymmetrical BB84 (blue), LM05 (red) and SDC (green) against error rate $q/2$ given independent channels in the infinite key limit

## 4.2. Correlated Channels

In Figures 7 and 8 we present the results for implementations of the SDC and LM05 for correlated channels compared to the asymmetrical BB84 in terms of their efficiencies against errors in the channel. We reiterate that we consider a particular model for correlated channels; *i.e.*, specified by $e_1 = e_2 = e_m$ and the error rates for SDC and LM05 in EM are given by $q/2$ and $q/4$ respectively [5].
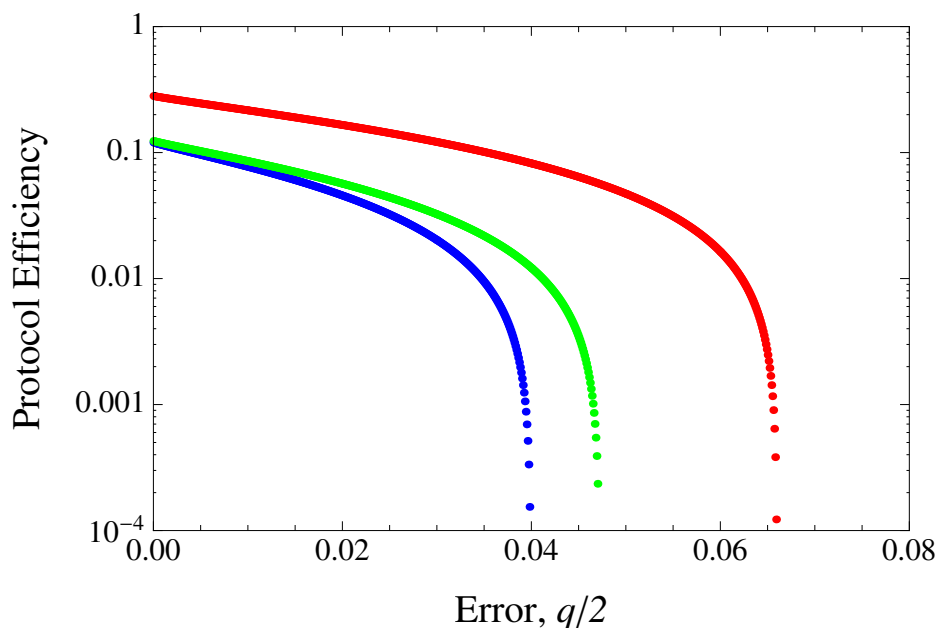


**Figure 7.** Efficiency for Asymmetrical BB84 (blue), LM05 (red) and SDC (green) against error rate $q/2$ for total qubit used as $M = 10^4$ for correlated channels specified by $e_1 = e_2 = e_m$.
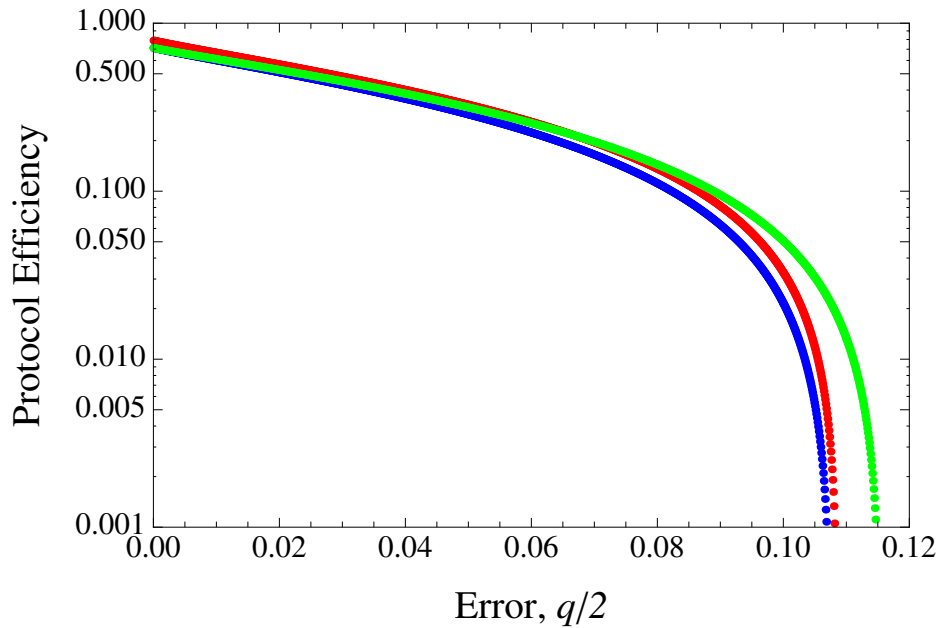
**Figure 8.** Efficiency for Asymmetrical BB84 (blue), LM05 (red) and SDC (green) against error rate $q/2$ for total qubit used as $M = 10^7$ for correlated channels specified by $e_1 = e_2 = e_m$.

In both the figures we see LM05 outperforming BB84 though in the second only marginally. This can be understood as due to going to infinite key limit where the two efficiencies should converge (binary entropic function for the bits to be discarded for both protocols in correlated channels is essentially given by the same form). This is illustrated in Figure 9 for increasing qubits used and further highlighted in Figure 10 where the black curve represents both the LM05 and BB84's key rate. However what is interesting is the fact that for finite number of qubits used, LM05 exceeds BB84 in terms of a higher tolerance towards errors clearly exemplified in Figure 7. This is almost unexpected as looking at the key rate formulas, one would imagine that the amount of bits to be discarded due to error correction and privacy amplification are essentially the same (relative to the key rates). However, a difference exists when considering the statistical fluctuation term. As LM05 allows for a larger number of bits to be salvaged in EM, thus a greater number of bits in CM (compared to BB84) may be used for error estimation in bounding Eve's information in the entropic relation. This allows for $\mu(n_e, k_e) < \mu(n, k)$ implying

$$h_2\left(\frac{q}{2} + \mu(n, k)\right) > h_2\left(\frac{q}{2} + \mu(n_e, k_e)\right). \tag{27}$$

Hence, for the same error in a channel, BB84 discards more bits than LM05, explaining LM05's higher error tolerance. This would be essentially the same reasoning for LM05's performance over SDC's in Figure 6.

SDC's better performance when compared to BB84's in both figures and LM05's in Figure 7 is mainly due to the error correction term. In this particular model for correlated channels, the following inequality holds,

$$h_2(q/2) \geq h_4(q/4), \tag{28}$$

where less bits are discarded for error correction in SDC and equality holds only for $q = 0$. The infinite key regime of Figure 8 sees identical performance for both LM05 and BB84 while SDC exceeds both.
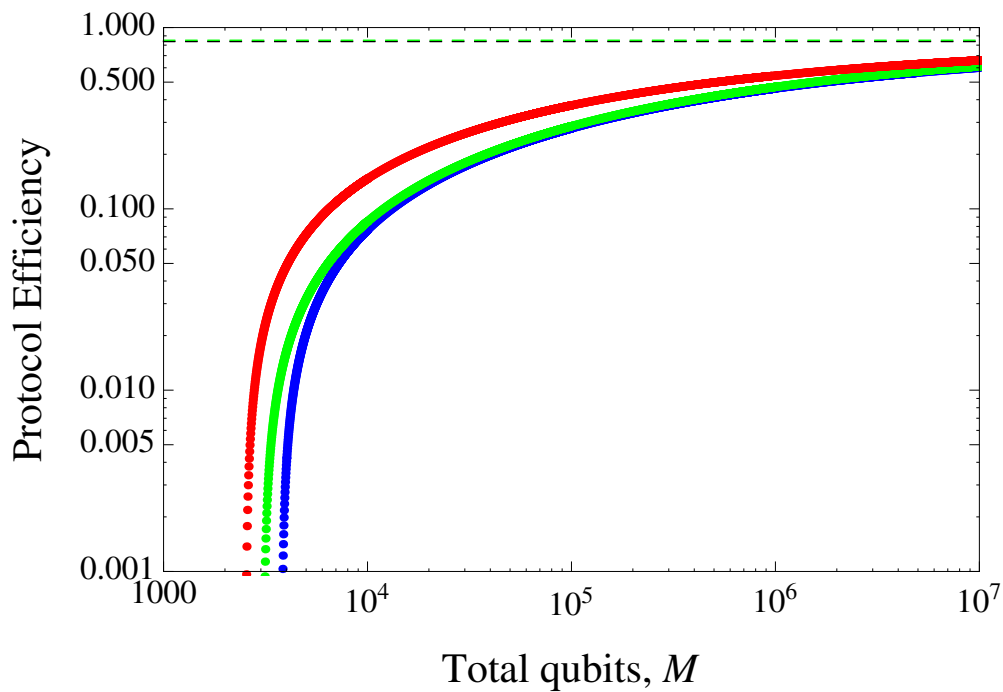


**Figure 9.** Efficiency for Asymmetrical BB84 (blue), LM05 (red) and SDC (green) against total qubit used, $M$ (for SDC, it is to be understood as total pairs used) for error rate $0.01$ for correlated channels specified by $e_1 = e_2 = e_m$. The horizontal dashed lines represents the infinite key regime.
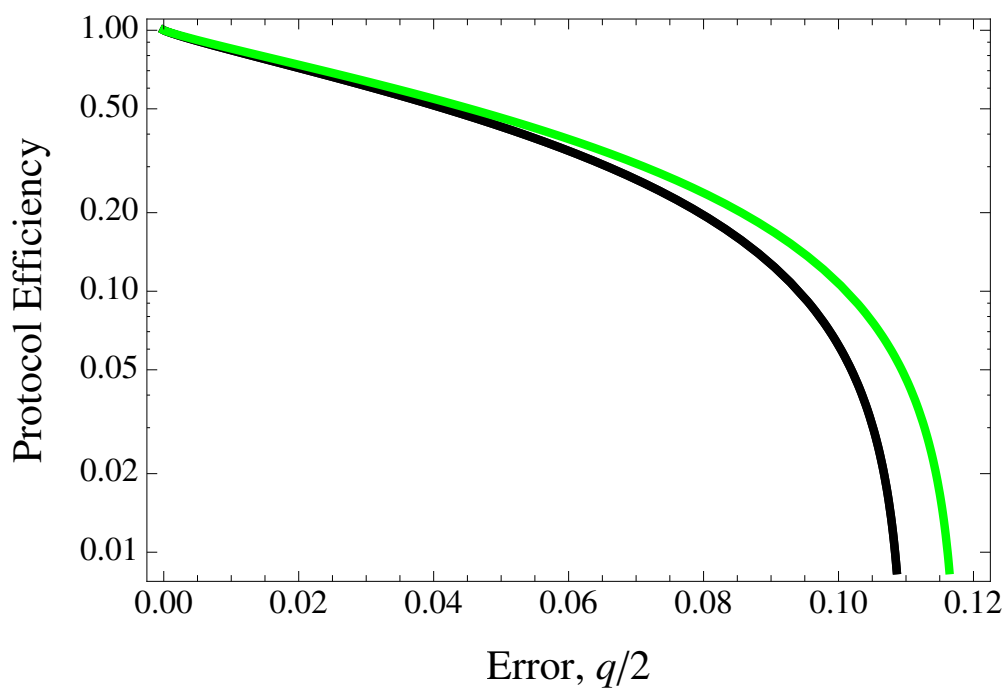


**Figure 10.** Efficiency for Asymmetrical BB84, LM05 (both black) and SDC (green) against error rate $q/2$ for correlated channels specified by $e_1 = e_2 = e_m$ in the infinite key limit.

## 5. Conclusions

Protocols making use of bidirectional quantum channels like the ones described in this work have the interesting feature of encodings being embedded in a unitary transformation as opposed to the preparation of a quantum state as well as the added advantage of how a decoding procedure should not see wastage due to bases mismatch unlike the conventional BB84. By conventional we refer to the BB84 in its original form where the choice of bases is equiprobable, resulting in only half of qubits transmitted could be used as a raw key. While asymmetric BB84 is proposed as a remedy and is expected to not perform any less than the two "deterministic" protocols in the infinite key regime, the scenario for finite keys can be different; thus the motivation for this work.

Noting how the choice of relevant probability distribution for EM and CM is immediately analogous to the asymmetric BB84's choice for the preferred basis and non preferred basis respectively in [9], we extend the security proof based on purified versions of the SDC and LM05 in [5] to the use of smooth entropies for a finite key analysis. We provide for secure key rates in terms of efficiency for the protocols.

In a relatively small number of qubits resources used (order of $10^4$) as well as lower depolarization of channels, we observe an obvious advantage in LM05 due to having more bits for raw key purpose (derived from EM). This results from LM05's encoding/decoding process which is independent of Bob's choice of bases for measurement processes; which is in fact the 'deterministic' merit claim of the protocol. This advantage does however diminish in the region of asymptotically long keys when compared to BB84 (as well as the SDC).

The SDC is in some sense very similar to the asymmetric BB84 as bits for key purposes can only be salvaged when both Alice's and Bob's encoding and decoding processes respectively coincide (unlike LM05 where Bob's measurements in CM would be equally meaningful as a decoding measurement in the EM). The only real advantage SDC has over BB84 would be in the correlated channels case due to the error correction procedure. However, one must bear in mind that while efficiency for LM05 and BB84 is measured as key bits per-qubits transmitted, SDC's is measured as key bits per-entangled pairs used. Practically, this may not set to provide for a promising scenario as quantum memories become a necessity. Apart from our study of independent as well as a specific correlated channels, It is possible to consider variant cases of the latter beyond the one modeled here. Despite how any results thereof would depend strongly on the nature of the correlations, one may roughly deduce that having errors in EM lower than that provided by independent channels may very well result in a higher key rate for SDC and LM05 against BB84. Conversely, when the errors in EM is higher, it is likely the case that LM05 may not perform better than BB84 except for possible very small error rates. We conclude saying that a finite key analysis would be enlightening also for two-way QKD in the framework of continuous variable [29].

## Author Contributions

The authors have equally contributed to the paper. All authors have read and approved the final manuscript.

## Conflicts of Interest

The authors declare no conflicts of interest.

## References and Notes

1. Lucamarini, M.; Mancini, S. Quantum key distribution using a two-way quantum channel. *Theor. Comput. Sci.* **2014**, *560*, 46–61.
2. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **2002**, *74*, 145–195.
3. Boström, K.; Felbinger, T. Deterministic Secure Direct Communication Using Entanglement. *Phys. Rev. Lett.* **2002**, *89*, 187902.
4. Lu, H.; Fung, C.-H.F.; Ma, X.; Cai, Q.-Y. Unconditional security proof of a deterministic quantum key distribution with a two-way quantum channel. *Phys. Rev. A* **2011**, *84*, 042344.
5. Beaudry, N.J.; Lucamarini, M.; Mancini, S.; Renner, R. Security of two-way quantum key distribution. *Phys. Rev. A* **2013**, *88*, 062302.
6. Lucamarini, M.; Mancini, S. Secure Deterministic Communication without Entanglement. *Phys. Rev. Lett.* **2005**, *94*, 140501.
7. Hayashi, M. Practical evaluation of security for quantum key distribution. *Phys. Rev. A* **2006**, *74*, 022307.
8. Scarani, V.; Renner, R. Quantum Cryptography with Finite Resources: Unconditional Security Bound for Discrete-Variable Protocols with One-Way Postprocessing. *Phys. Rev. Lett.* **2008**, 100, 200501.
9. Tomamichel, M.; Lim, C.C.W.; Gisin, N.; Renner, R. Tight finite-key analysis for quantum cryptography. *Nat. Commun.* **2012**, *3*, doi:10.1038/ncomms1631.
10. Lo, H.-K.; Chau, H.F.; Ardehali, M. Efficient quantum key distribution scheme and a proof of its unconditional security. *J. Cryptol.* **2005**, 18, 133–165.
11. Cai, Q.-Y.; Li, B.-W. Improving the capacity of the Boström-Felbinger protocol. *Phys. Rev. A* **2004**, *69*, 054301.
12. Bechmann-Pasquinucci, H.; Tittel, W. Quantum cryptography using larger alphabets. *Phys. Rev. A* **2000**, *61*, 062308.
13. Lo, H.K.; Chau, H.F. Unconditional security of quantum key distribution over arbitrarily long distances. *Science* **1999**, *283*, 2050–2056.
14. This is referred to as a purification of Alice's encoding in [5].
15. Maassen, H.; Uffink, J.B.M. Generalized Entropic Uncertainty Relations. *Phys. Rev. Lett.* **1988**, *60*, 1103–1106.

16. Renes, J.M.; Boileau, J.C. Conjectured strong complementary information tradeoff. *Phys. Rev. Lett.* **2009**, *103*, 020402.

17. Berta, M.; Christandl, M.; Colbeck, R.; Renes, J.M.; Renner, R. The uncertainty principle in the presence of quantum memory. *Nat. Phys.* **2010**, *6*, 659–662.

18. Coles, P.J.; Yu, L.; Gheorghiu, V.; Griffiths, R.B. Information theoretic treatment of tripartite systems and quantum channels. *Phys. Rev. A* **2011**, *83*, 062338.

19. Devetak, I.; Winter, A. Distillation of secret key and entanglement from quantum states. *Proc. R. Soc. A* **2005**, *461*, 207–235.

20. Tomamichel, M.; Renner, R. Uncertainty relation for smooth entropies. *Phys. Rev. Lett.* **2011**, *106*, 110506.

21. Tomamichel, M.; Colbeck, R.; Renner, R. Duality between smooth min- and max-entropies. *IEEE Trans. Inf. Theory* **2010**, *56*, 4674–4681.

22. According to a distance that is based on the same notion of purified distance, for the classical register $X$ arising from POVM $\mathbb{X}$ on $B$, given quantum side information $E$ [31].

23. The results should coincide with Alice's measurement in CM when their bases coincide.

24. A similar case for correlations between errors in the forward and backward path in CM was studied in [32].

25. While for LM05 only a single qubit travels to and fro between the communicating parties, the case for SDC makes use of entangled pairs. Thus $M(n,k)$ for SDC must be understood as number of qubit pairs.

26. It is possible to consider a more practical scenario, for example for a bit string with error rate $e$, a cofactor would be multiplied to the amount bits needed for such a purpose given by $h_2(e)$.

27. Tomamichel, M.; Schaffner, C.; Smith, A.; Renner, R. Leftover Hashing Against Quantum Side Information. *IEEE Trans. Inf. Theory* **2011**, 57, 5524–5535.

28. Cabello, A. Efficient Quantum Cryptography. *Rec. Res. Dev. Phys.* **2001**, *2*, 249–257.

29. Pirandola, S.; Mancini, S.; Lloyd, S.; Braunstein, S.L. Continuous-variable quantum cryptography using two-way quantum communication. *Nat. Phys.* **2008**, *4*, 726–730.

30. An ideal error correction efficiency is considered for convenience; which is also the case for LM05 in the ensuing subsection.

31. Tomamichel, M. A Framework for Non-Asymptotic Quantum Information Theory. Ph.D. Thesis, Dissertation ETH No. 20213, ETH Zurich, Zurich, Switzerland.

32. Shaari, J.S.; Lucamarini, M.; Mancini, S. Checking noise correlations for safer two-way quantum key distribution. *Quantum. Inf. Process.* **2014**, *13*, 1139–1153.