Quantum Entropic Security and Approximate Quantum Encryption

Simon Pierre Desrosiers and Frédéric Dupuis

***Abstract*—An encryption scheme is said to be entropically secure if an adversary whose min-entropy on the message is upper bounded cannot guess any function of the message. Similarly, an encryption scheme is entropically indistinguishable if the encrypted version of a message whose min-entropy is high enough is statistically indistinguishable from a fixed distribution. We present full generalizations of these two concepts to the encryption of quantum states in which the quantum conditional min-entropy, as introduced by Renner, is used to bound the adversary's prior information on the message. A proof of the equivalence between quantum entropic security and quantum entropic indistinguishability is presented. We also provide proofs of security for two different ciphers in this model and a proof for a lower bound on the key length required by any such cipher. These ciphers generalize existing schemes for approximate quantum encryption to the entropic security model.**

***Index Terms*—Cryptography, entropic security, quantum information.**

I. Introduction

SEMANTIC security, whether it is computational, as introduced in [1], information theoretic in a classical setting, as introduced in [2] and [3], or information theoretic in a limited quantum setting, as introduced in [4], contrasts the capabilities of two adversaries: one (A) that has access to an encrypted version of the message, and another (A') that does not. Their abilities to predict a function on the initial message are compared. Of course A' seems to be at a tremendous disadvantage: it has access to nothing but the prior distribution of the plain text, whereas A also has access to an encrypted version of the plain text and could potentially use imperfections in the encryption scheme to gain an advantage. However, this can become a way to bound these imperfections: an encryption scheme is considered semantically secure if, for every adversary A, there exists an A' that can predict every function on the plaintext almost as well as A without even having access to the encrypted message. This is a very strong security criterion, especially in the information theoretic setting.

Perhaps surprisingly, it is possible to construct semantically secure encryption schemes which, depending on their setting, make very few assumptions on A and yet do not require keys to be as long as the message. In the computational setting, Goldwasser and Micali [1] had as a constraint that both A and A' were probabilistic polynomial-time machines. In their model, they could construct encryption schemes which, on all message distributions, would render A as useless as A'. In the information theoretic setting, introduced by Russell and Wang [2] and expanded upon by Dodis and Smith [3], no computational limitation is imposed on A or A'. In order to achieve significant key size reduction, a limit on the prior knowledge of A on the plain text space is assumed. In fact, a lower bound on the min-entropy of the message space is assumed: the most probable message is not too probable. For this reason, this concept is called *entropic security* in the context of information-theoretic security. In the quantum information theoretic setting, as introduced by Desrosiers [4], the exact same restriction on the min-entropy is imposed on A, except that this time messages are quantum states which are further assumed to be unentangled with any quantum system that the adversary might possess. If these two restrictions are satisfied, one can construct encryption schemes for the quantum setting which have exactly the same key size as in the classical setting: for an n-qubit message which is assumed to have a min-entropy of at least t, then we need $n - t + \log(1/\varepsilon)$ bits of key to encrypt it securely (where ε is a security parameter).

In this paper we remove one of those two restrictions. Of course, the limit on the min-entropy of the adversary on the message space is hard to remove: it is the essence of entropic security. However, it has to be modified in order to get robust definitions of security in the presence of entanglement between the sender and the adversary. The notion of quantum conditional min-entropy as introduced by Renner in [5] will be used to bound the prior "knowledge" of the adversary. This new notion of min-entropy allows us to remove the no-entanglement restriction and replace it by something more general. Indeed, if a state is not entangled, we have an implicit lower bound of zero on the conditional min-entropy, whereas in the general case, the conditional min-entropy of the adversary on an n-qubit system held by the sender ranges between $-n$ and n. It turns out that the key size remains the same in this model: for an n-qubit message about which the eavesdropper has a min-entropy of at least t, we still need a key of $n-t+\log(1/\varepsilon)$ bits. In the extreme case where we have no bound at all on the min-entropy, this reduces

Manuscript received January 14, 2008; revised February 22, 2010. Current version published June 16, 2010. This work was supported by QuantumWorks, CIFAR, and NSERC. The material in this paper was presented at Quantum Information Processing 2008, Delhi, India, December 2007.

S. P. Desrosiers is with McGill University, Montréal, QC H3A 2A7 Canada.

F. Dupuis was with the Université de Montréal, Montréal QC H3T 1J4 Canada and McGill University, Montreal, Quebec, Canada, H3A 2A7. He is now with the Institute for Theoretical Physics, ETH Zurich, Zurich, Switzerland.

Communicated by A. Winter, Associate Editor for Quantum Information Theory.

Digital Object Identifier 10.1109/TIT.2010.2048488

to $2n + \log(1/\varepsilon)$, which is in total agreement with the standard result of Ambainis, Mosca, Tapp, and de Wolf [6].

Note that this generalizes the existing literature on approximate quantum encryption. In [7], Hayden, Leung, Shor and Winter considered the task of approximately encrypting quantum states assuming that the adversary is not entangled with the sender. They showed, using a randomized argument, that, while we need $2n$ bits of key to perfectly encrypt an n-qubit quantum message, there exists a scheme requiring $n + \log n + 2\log(1/\varepsilon) + O(1)$ bits of key. Ambainis and Smith [8] then gave two explicit constructions of an approximate quantum encryption scheme under the same assumption requiring $n + 2\log n + 2\log(1/\varepsilon)$ and $n + 2\log(1/\varepsilon)$ bits of key respectively. Here we recover and generalize these results.

More recently, Fehr and Schaffner [9] gave a classical encryption scheme which is entropically secure against an adversary that has access to quantum information about the classical message. Our work also generalizes this result: when our encryption schemes are applied to a classical message, the resulting ciphertext remains classical, and the proof of security still works against quantum adversaries.

We introduce our model and definitions in Section III and show in Section IV that the two security definitions we give are equivalent. We also prove, in Section V, that two encryption schemes introduced by Ambainis and Smith [8] and by Dodis and Smith [3] (and generalized to the quantum world by Desrosiers [4]) are still secure using this new definition and require the same amount of key as in the limited quantum model of [4]. Finally, in Section VI, we generalize a proof of Dodis and Smith to show that an entropic scheme that can encrypt any n-qubit state having a conditional min-entropy of at least t requires at least $n - t - 1$ bits of uniform key.

II. Notation and Preliminaries

A quantum state ρ is defined as a positive semidefinite operator of trace equal to 1 over some Hilbert space $\mathcal{H}$. By the spectral decomposition theorem, $\rho = \sum_i \gamma_i |r_i\rangle\langle r_i|$, where the $|r_i\rangle$ form a basis for the space in which the quantum state lives and the γ_i are non-negative real numbers that sum up to one. This can be interpreted this way: if ρ is measured in the basis $\{|r_i\rangle\}$, then it behaves as a source that will output with probability γ_i the state $|r_i\rangle$.[1].

The partial trace can be seen as a kind of inverse to the tensor product operation. For any bipartite state ρ^{AB}, we have that $\rho^B = \mathrm{Tr}_A\left(\rho^{AB}\right)$; the normal interpretation for such an operator is that if a physical state ρ^{AB} lives in the space AB but one only has access to the system B to measure the state, then the statistics obtained are in agreement with ρ^B. The partial trace can be defined as:

$$\mathrm{Tr}_A(\rho^{AB}) \triangleq \sum_i (\langle r_i|^A \otimes \mathbb{I}^B)\rho^{AB}(|r_i\rangle^A \otimes \mathbb{I}^B) \qquad (1)$$

where the vectors $\{|r_i\rangle\}$ form any orthonormal basis for the subspace A. In fact, this is equivalent to doing a complete measurement of the A subsystem followed by a loss of the result and of the A subsystem; what is left in our hands is $\mathrm{Tr}_A(\rho^{AB})$.

[1]For a thorough introduction to quantum information theory, see [10]

Throughout this paper, we will use superscripts for density matrices to indicate on which subsystems they are defined; for example, ρ^{AB} is a density operator on the Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$. By convention, when we omit certain subsystems from the superscript, we mean that we take the partial trace over the subsystems that are absent; i.e., $\rho^B = \mathrm{Tr}_A\rho^{AB}$. We will refer to the dimension of the Hilbert space $\mathcal{H}_A$ by d_A.

We will use as our main distance measure the trace distance which is defined as

$$||\rho - \sigma||_1 \triangleq \mathrm{Tr}\left(|\rho - \sigma|\right) \qquad (2)$$

where $|A|$ is defined as $\sqrt{A^\dagger A}$, which is simply $\sum_i |\alpha_i|\,|a_i\rangle\langle a_i|$ for a Hermitian operator $A = \sum_i \alpha_i |a_i\rangle\langle a_i|$. As [11] and [10, Ch. 9] tell us, for any two states ρ and σ there exists an optimal adversary which can distinguish between them with probability $\frac{1}{2} + \frac{1}{4}||\rho - \sigma||_1$; no adversary can do better.

Another useful distance measure is known as the *fidelity*: given two density operators ρ and σ, their fidelity $F(\rho, \sigma)$ is defined as $\left\|\sqrt{\rho}\sqrt{\sigma}\right\|_1$. If σ is a pure state $|\psi\rangle\langle\psi|$, this is equal to $\sqrt{\langle\psi|\rho|\psi\rangle}$.

We will also frequently make use of operator inequalities: given two Hermitian operators A and B, we will say that $A \geqslant B$ iff $A - B$ is positive semidefinite.

Also, we denote by $a||b$ the concatenation of the bit strings a and b. X^a, where $a = a_1 \cdots a_n$ is an n-bit string, means $X^a = X^{a_1} \otimes X^{a_2} \otimes \cdots \otimes X^{a_n}$. We shall also write $\mathcal{L}(\mathcal{H})$ for the space of linear operators on the Hilbert space $\mathcal{H}$. Finally, we denote by $a \odot b$ the inner product modulo 2 of the strings a and b: $\sum_i a_i b_i \bmod 2$.

III. Model and Definitions

Entropic security as introduced by Russell and Wang [2] and generalized by Dodis and Smith [3] uses the definition of classical min-entropy to represent the adversary's knowledge on the sender's message space. Let M be a random variable over the message space M and let M take value m with probability p_m. Then the min-entropy of M, written $H_\infty(M)$ is defined to be $-\log\max_m(p_m)$.

Desrosiers introduced in [4] a quantum version of these security definitions for the case where the eavesdropper and the sender are neither entangled nor correlated. In this setting, a message σ_i is chosen at random with probability p_i in a valid *interpretation* $\{(p_i, \sigma_i)\}$ of a state $\rho^A = \sum_i p_i\sigma_i$. Here the adversary's a priori uncertainty is quantified by the quantum min-entropy, $H_\infty(\rho^A) = -\log\max_j \gamma_j$ where $\sum \gamma_j |j\rangle\langle j|$ is the spectral decomposition of ρ^A. The joint system of the sender and the adversary was considered to contain no correlations: i.e., $\rho^{AE} = \sigma^A \otimes \tau^E$, where E represents the eavesdropper's system.

In this paper, we shall show that we can fully generalize these security definitions to the quantum setting, where no assumption on the entanglement between the sender and the adversary is made. The only restriction on the adversary will be quantified by the following definition introduced by Renner (see [5]) in his proof that the BB84 scheme, the original quantum key distribution protocol, is secure in the most general setting. We shall make no other assumption on the sender-eavesdropper system than the eavesdropper's conditional min-entropy.

Definition 1 (Quantum Conditional Min-Entropy): For any quantum state ρ^{AE} shared between the eavesdropper and the sender, we define the conditional min-entropy of A given E as

$$H_\infty(A|E)_\rho = -\log \min_{\sigma^E} \min\left\{\lambda : \lambda \mathbb{I}^A \otimes \sigma^E \geqslant \rho^{AE}\right\}$$

where σ^E ranges over all normalized density operators over $\mathcal{H}_E$.

According to [12], we can express the quantum conditional min-entropy as

$$2^{-H_\infty(A|E)_\rho} = d_A \max_{\mathcal{E}} \langle\Phi|\mathcal{E}(\rho^{AE})|\Phi\rangle$$

where the maximization is taken over all CPTP maps $\mathcal{E} : \mathcal{L}(\mathcal{H}_E) \rightarrow \mathcal{L}(\mathcal{H}_{A'})$ and where $\mathcal{H}_{A'} \cong \mathcal{H}_A$.

One can prove a few properties about conditional min-entropy which will be handy later on. First, this lemma is presented.

Lemma 1: Let the joint state of the sender and the adversary be $\rho^{AE} = \rho^A \otimes \rho^E$, then $H_\infty(A|E)_\rho = H_\infty(A)_\rho$.

Proof:

$$\begin{aligned} 2^{-H_\infty(A|E)_\rho} &= \min_{\sigma^E} \min\left\{\lambda : \lambda \mathbb{I}^A \otimes \sigma^E \geqslant \rho^A \otimes \rho^E\right\} \\ &\geqslant \min\left\{\lambda : \lambda \mathbb{I}^A \geqslant \rho^A\right\} \\ &= \min\left\{\lambda : \lambda \mathbb{I}^A \otimes \rho^E \geqslant \rho^A \otimes \rho^E\right\} \\ &\geqslant \min_{\sigma^E} \min\left\{\lambda : \lambda \mathbb{I}^A \otimes \sigma^E \geqslant \rho^A \otimes \rho^E\right\}. \end{aligned}$$

Since the first and last lines are the same, the two inequalities are, in fact, equalities, and, hence $2^{-H_\infty(A|E)_\rho} = \min\left\{\lambda : \lambda \mathbb{I}^A \geqslant \rho^A\right\} = 2^{-H_\infty(A)_\rho}$. ∎

We can conclude from this lemma that if the sender and the adversary are not correlated, then the earlier results of [4] can be used.

Furthermore, König, Renner, and Schaffner [12] show that for a state of the form $\rho^{AE} = \sum_i p_i |i\rangle\langle i|^A \otimes \rho_i^E$ (i.e., A holds classical information and E holds a quantum state containing partial information on A), the quantum conditional min-entropy $H_\infty(A|E)_\rho$ characterizes Eve's optimal probability of guessing A by measuring E:

$$p_{\text{guess}} = 2^{-H_\infty(A|E)_\rho}.$$

Note also that if the A and E systems are in a maximally entangled state $\sum_{i=1}^d \frac{1}{\sqrt{d}} |i\rangle^A |i\rangle^E$, where $n = \log d$, then

$$H_\infty(A|E)_\rho = -n. \tag{3}$$

Hence, the quantum conditional min-entropy ranges from $-n$ to n for an n-qubits system and, as is the case with the von Neumann conditional entropy, negative values arise from purely quantum effects.

In our model, we will consider a protocol to be secure if the adversary is incapable of obtaining classical information about the message encoded in any basis. We will therefore model the adversary as a POVM on the encrypted message together with the adversary's side information. Since entropic security, even in the classical case (see [3]), does not have good composability properties (i.e., the security of the scheme does not necessarily imply that it can be securely embedded in a larger cryptographic protocol), we will not consider adversaries that keep quantum information without measuring it in the hopes of mounting a more effective attack later after having received more information. We are interested in the predictive capabilities of an adversary that was given $\mathcal{E}(\sigma_i)$—see below for the formal definition of a cipher $\mathcal{E}$—compared to those of an adversary that was not given such a state in predicting a function of i. Since our adversary is a POVM, we take its output to be a prediction of the function f. We shall denote the random variable that is the output of A on any given state γ by $\mathsf{A}(\gamma)$; that is, if $\{A_i\}_{i\in I}$ is the set of POVM elements associated with A, then $\mathsf{A}(\gamma)$ is a random variable which takes the value i with probability $\mathrm{Tr}[A_i\gamma]$.

An encryption scheme $\mathcal{E}$ is a set of superoperators $\{\mathcal{E}_k\}$ indexed by a uniformly distributed key $k \in \{1, \ldots, K\}$ such that for each k there exists an inverting operator $\mathcal{D}_k$ such that for all ρ^{AE}, with probability one we have

$$(\mathcal{D}_k \otimes \mathbb{I})((\mathcal{E}_k \otimes \mathbb{I})(\rho)) = \rho. \tag{4}$$

The view of the adversary is then $(\mathcal{E} \otimes \mathbb{I})(\rho^{AE}) \triangleq \frac{1}{K}\sum_{k=1}^K (\mathcal{E}_k \otimes \mathbb{I})(\rho^{AE})$. To simplify the notation, we will write $\mathcal{E}(\rho^{AE})$ instead of $(\mathcal{E} \otimes \mathbb{I})(\rho^{AE})$ from now on. Note that in general, $\mathcal{E}$ maps systems on space AE to systems on space $A'E$; the dimension of A' could be larger than the dimension of A.

Both [3] and [4] presented security definitions equivalent in their respective models to the following two security definitions.

Note that throughout this paper, we shall be mostly concerned with encryption schemes where the message to be sent consists of n qubits; therefore, $n = \log d_A$ from now on.

Definition 2 (Entropic Security): An encryption system $\mathcal{E}$ is (t, ε)-entropically secure if for all states ρ^{AE} such that $H_\infty(\rho^{AE}|\rho^E) \geqslant t$, all interpretations $\{(p_i, \sigma_i^{AE})\}$, all adversaries A and all functions f, there exists an A' such that we have:[2]

$$\left|\Pr[\mathsf{A}(\mathcal{E}(\sigma_i^{AE})) = f(i)] - \Pr[\mathsf{A}'(\sigma_i^E) = f(i)]\right| \leqslant \varepsilon. \tag{5}$$

Note that everywhere, we take probabilities over all i and all randomness used by the adversaries and the cipher.

Definition 3 (Entropic Indistinguishability): An encryption system $\mathcal{E}$ is (t, ε)-indistinguishable if there exists a state $\Omega^{A'}$ such that for all states ρ^{AE} such that $H_\infty(A|E)_\rho \geqslant t$ we have that:

$$\left\|\mathcal{E}(\rho^{AE}) - \Omega^{A'} \otimes \rho^E\right\|_1 < \varepsilon. \tag{6}$$

IV. Equivalence Between the Two Security Definitions

This section will show that an encryption scheme which is entropically secure is entropically indistinguishable, and *vice-versa*, up to small variations in the t and ε parameters. Before presenting these proofs, however, we will need an additional definition and a technical lemma. The following variation on entropic security will prove to be useful in the sequel.

[2]One can also get an equivalent definition by using functions on the states σ_i^{AE} rather than on the indices i.

Definition 4 (Strong Entropic Security): An encryption system $\mathcal{E}$ is strongly (t,ε)-entropically secure if for all states ρ^{AE} such that $H_\infty(\rho^{AE}|\rho^E) \geqslant t$, all interpretations $\{(p_i,\sigma_i^{AE})\}$, all adversaries A, and all functions f, we have

$$\left|\Pr[\mathsf{A}(\mathcal{E}(\sigma_i^{AE}))=f(i)]-\Pr[\mathsf{A}(\mathcal{E}(\rho^A)\otimes\sigma_i^E)=f(i)]\right|\leqslant\varepsilon. \tag{7}$$

Note that in this case both uses of $\mathcal{E}$ are independent. Strong (t,ε)-entropic security clearly implies regular (t,ε)-entropic security, since A used on σ_i^E and an encrypted message independent of σ_i^E (which can be prepared by Eve in her lab) is a valid choice for A'.

The following lemma says that one does not need to consider all possible functions, but one can restrict the analysis to predicates as follows.

Lemma 2: Let ρ^{AE} be a state, $\{(p_i,\sigma_i^{AE})\}$ be an interpretation, $\mathcal{E}$ be a cipher, f be a function and A be an adversary such that

$$\left|\Pr[\mathsf{A}(\mathcal{E}(\sigma_i^{AE}))=f(i)]-\Pr[\mathsf{A}(\mathcal{E}(\rho^A)\otimes\sigma_i^E)=f(i)]\right|>\varepsilon$$

then there exist an adversary B and a predicate h such that

$$\left|\Pr[\mathsf{B}(\mathcal{E}(\sigma_i^{AE}))=h(i)]-\Pr[\mathsf{B}(\mathcal{E}(\rho^A)\otimes\sigma_i^E)=h(i)]\right|>\frac{\varepsilon}{2}.$$

Proof: Let our predicate be a Goldreich-Levin predicate [13], that is $h_r(x)=r\odot f(x)$. Let $p=\Pr[\mathsf{A}(\mathcal{E}(\sigma_i^{AE}))=f(i)]$ and $q=\Pr[\mathsf{A}(\mathcal{E}(\rho^A)\otimes\sigma_i^E)=f(i)]$. Then we know that $|p-q|>\varepsilon$. Let us compute [see (8) at the bottom of the page], where the expectation is taken over all r of adequate size. We need two observations. First, when A predicts correctly, then $p=\Pr[r\odot\mathsf{A}(\mathcal{E}(\sigma_i^{AE}))=h_r(i)]$. Second, when A does not predict correctly, the probability that $r\odot\mathsf{A}(\mathcal{E}(\sigma_i))=h_r(i)$ is exactly one half. Hence (8) reduces to

$$\begin{aligned}E&=\left|1\cdot p+\frac{1}{2}\cdot(1-p)-\left(1\cdot q+\frac{1}{2}\cdot(1-q)\right)\right|\\&=\left|\frac{p-q}{2}\right|>\frac{\varepsilon}{2}.\end{aligned}\tag{9}$$

Thus there exists at least one value r such that the following is true (see the second equation at the bottom of the page). The lemma is proven if adversary $\mathsf{B}(\cdot)$ is defined, using this appropriate r, as $r\odot\mathsf{A}(\cdot)$. ■

Theorem 1: $(t-1,\varepsilon/2)$-entropic indistinguishability implies strong (t,ε)-entropic security for all functions.

Proof: We shall prove the contrapositive. Suppose there exists an adversary B, a state ρ^{AE} such that $H_\infty(A|E)_\rho\geqslant t$, an interpretation $\left\{(p_j,\sigma_j^{AE})\right\}$ for ρ^{AE} and a function f such that

$$\left|\Pr[\mathsf{B}(\mathcal{E}(\sigma_i^{AE}))=f(i)]-\Pr[\mathsf{B}(\mathcal{E}(\rho^A)\otimes\sigma_i^E)=f(i)]\right|>\varepsilon. \tag{10}$$

Then we know from Lemma 2 that there exists another adversary and a predicate h such that strong $(t,\varepsilon/2)$-entropic security is violated. Let's call this adversary A and let us define the sets E_0 and E_1 as follows:

$$E_0=\{i|h(i)=0\} \tag{11}$$
$$E_1=\{i|h(i)=1\}. \tag{12}$$

Define the following:

$$\begin{aligned}r_0&=\sum_{i\in E_0}p_i,\\r_1&=\sum_{i\in E_1}p_i,\\\tau_0^{AE}&=\frac{1}{r_0}\left(\sum_{i\in E_0}p_i\sigma_i^{AE}\right)\\\tau_1^{AE}&=\frac{1}{r_1}\left(\sum_{i\in E_1}p_i\sigma_i^{AE}\right).\end{aligned}$$

Note that $\rho^{AE}=r_0\tau_0^{AE}+r_1\tau_1^{AE}$. Now, define the following states:

$$\tilde{\tau}_0^{AE}=r_0\tau_0^{AE}+r_1\rho^A\otimes\tau_1^E \tag{13}$$
$$\tilde{\tau}_1^{AE}=r_1\tau_1^{AE}+r_0\rho^A\otimes\tau_0^E, \tag{14}$$

where, as usual, $\tau_i^E=\mathrm{Tr}_A[\tau_i^{AE}]$. We need the following lemma to finish the proof.

Lemma 3: Assuming $H_\infty(A|E)_\rho\geqslant t$, we then have that both $H_\infty(A|E)_{\tilde{\tau}_0}$ and $H_\infty(A|E)_{\tilde{\tau}_1}$ are at least $t-1$.

$$E=\left|\mathbb{E}_r\left[\Pr[r\odot\mathsf{A}(\mathcal{E}(\sigma_i))=h_r(i)]-\Pr[r\odot\mathsf{A}(\mathcal{E}(\rho^A)\otimes\sigma_i^E)=h_r(i)]\right]\right| \tag{8}$$

$$\left|\Pr[r\odot\mathsf{A}(\mathcal{E}(\sigma_i^{AE}))=h_r(i)]-\Pr[r\odot\mathsf{A}(\mathcal{E}(\rho^A)\otimes\sigma_i^E)=h_r(i)]\right|>\frac{\varepsilon}{2}$$

Proof: We have that

$$\begin{aligned} d_A \max_{\mathcal{E}} &\langle\Phi|\mathcal{E}(\tilde{\tau}_0^{AE})|\Phi\rangle \\ &\leqslant r_0 d_A \max_{\mathcal{E}} \langle\Phi|\mathcal{E}(\tau_0^{AE})|\Phi\rangle \\ &\quad + r_1 d_A \max_{\mathcal{E}} \langle\Phi|\rho^A \otimes \mathcal{E}(\tau_1^E)|\Phi\rangle \\ &\leqslant d_A \max_{\mathcal{E}} \langle\Phi|\mathcal{E}(\rho^{AE})|\Phi\rangle \\ &\quad + d_A \max_{\mathcal{E}} \langle\Phi|\rho^A \otimes \mathcal{E}(\rho^E)|\Phi\rangle \\ &\leqslant 2^{-t} + d_A \max_{\mathcal{E}} \langle\Phi|\rho^A \otimes \mathcal{E}(\rho^E)|\Phi\rangle. \end{aligned} \tag{15}$$

We now bound the second term using the original definition of the conditional min-entropy:

$$\begin{aligned} &\min_{\sigma^E} \min\left\{\lambda : \lambda \mathbb{I}^A \otimes \sigma^E \geqslant \rho^A \otimes \rho^E\right\} \\ &\quad \leqslant \min\left\{\lambda : \lambda \mathbb{I}^A \otimes \rho^E \geqslant \rho^A \otimes \rho^E\right\} \\ &\quad = \min\left\{\lambda : \lambda \mathbb{I}^A \geqslant \rho^A\right\} \\ &\quad \leqslant \min_{\sigma^E} \min\left\{\lambda : \lambda \mathbb{I}^A \otimes \sigma^E \geqslant \rho^{AE}\right\} \\ &\quad \leqslant 2^{-t}. \end{aligned} \tag{16}$$

Substituting this into the last line of (15) yields $H_\infty(A|E)_{\tilde{\tau}_0} \geqslant t-1$. Of course, an identical calculation yields the same result for $\tilde{\tau}_1^{AE}$. ∎

To finish the proof of Theorem 1 , we want to show that A can distinguish $\mathcal{E}(\tilde{\tau}_0^{AE})$ from $\mathcal{E}(\tilde{\tau}_1^{AE})$ with probability strictly better than $1/2 + \varepsilon/4$. Let's denote by η the probability that A will correctly distinguish $\mathcal{E}(\tau_0^{AE})$ from $\mathcal{E}(\tau_1^{AE})$ in an r_0, r_1 mixture, and by α the probability that A will correctly distinguish $\mathcal{E}(\rho^A) \otimes \tau_0^E$ from $\mathcal{E}(\rho^A) \otimes \tau_1^E$ in an r_0, r_1 mixture. Also assume without loss of generality that $\eta > \alpha$ (otherwise consider an adversary identical to A but which returns the opposite answer). Now assume that we feed it $\mathcal{E}(\tilde{\tau}_0^{AE})$ with probability $1/2$ and $\mathcal{E}(\tilde{\tau}_1^{AE})$ with probability $1/2$. Observe that this is exactly as if we gave it an $r_0,\ r_1$ mixture of $\mathcal{E}(\tau_0^{AE})$ and $\mathcal{E}(\tau_1^{AE})$ with probability $1/2$ and an $r_0,\ r_1$ mixture of $\mathcal{E}(\rho^A) \otimes \tau_0^E$ and $\mathcal{E}(\rho^A) \otimes \tau_1^E$ with probability $1/2$. We then have that the probability of distinguishing $\mathcal{E}(\tilde{\tau}_0^{AE})$ from $\mathcal{E}(\tilde{\tau}_1^{AE})$ using A is

$$\frac{1}{2}\eta + \frac{1}{2}(1-\alpha) = \frac{1}{2} + \frac{1}{2}(\eta - \alpha)$$

since the correct answer is reversed for $\mathcal{E}(\rho^A) \otimes \tau_0^E$ and $\mathcal{E}(\rho^A) \otimes \tau_1^E$.

But by the assumption that A violates entropic security, we know that

$$\begin{aligned} \eta - \alpha &= \Pr[\mathsf{A}(\mathcal{E}(\tau_i^{AE})) = i] \\ &\quad - \Pr\left[\mathsf{A}\left(\mathcal{E}(\rho^A) \otimes \tau_i^E\right) = i\right] \\ &> \frac{\varepsilon}{2}. \end{aligned}$$

Hence, the probability of distinguishing $\mathcal{E}(\tilde{\tau}_0^{AE})$ from $\mathcal{E}(\tilde{\tau}_1^{AE})$ is at least $1/2 + \varepsilon/4$, which implies that for all $\Omega^{A'}$ we have

$$\begin{aligned} \varepsilon &< \left\|\mathcal{E}(\tilde{\tau}_0^{AE}) - \mathcal{E}(\tilde{\tau}_1^{AE})\right\|_1 \\ &= \left\|\left(\mathcal{E}(\tilde{\tau}_0^{AE}) - \Omega^{A'} \otimes \rho^E\right) - \left(\mathcal{E}(\tilde{\tau}_1^{AE}) - \Omega^{A'} \otimes \rho^E\right)\right\|_1 \\ &\leqslant \left\|\mathcal{E}(\tilde{\tau}_0^{AE}) - \Omega^{A'} \otimes \rho^E\right\|_1 + \left\|\mathcal{E}(\tilde{\tau}_1^{AE}) - \Omega^{A'} \otimes \rho^E\right\|_1 \end{aligned}$$

and, therefore, either $\left\|\mathcal{E}(\tilde{\tau}_0^{AE}) - \Omega^{A'} \otimes \rho^E\right\|_1 > \varepsilon/2$ or $\left\|\mathcal{E}(\tilde{\tau}_1^{AE}) - \Omega^{A'} \otimes \rho^E\right\|_1 > \varepsilon/2$, which is a violation of $(t-1, \varepsilon/2)$-indistinguishability. ∎

Theorem 2: (t, ε)-entropic security implies $(t-1, 6\varepsilon)$-indistinguishability as long as $t \leqslant n-1$.

Proof: We will prove the contrapositive. Let $\mathcal{E}(\mathbb{I}/d_A) = \Omega^{A'}$ and let ρ^{AE} be a state such that $H_\infty(A|E)_\rho \geqslant t-1$ and $\left\|\mathcal{E}(\rho^{AE}) - \Omega^{A'} \otimes \rho^E\right\|_1 > 6\varepsilon$. Consider the following state

$$\hat{\rho}^{AE} = \frac{1}{3}\rho^{AE} + \frac{2}{3}\frac{\mathbb{I}}{d_A} \otimes \rho^E.$$

We show that $H_\infty(A|E)_{\hat{\rho}} \geqslant t$:

$$\begin{aligned} d_A \max_{\mathcal{E}} &\langle\Phi|\mathcal{E}(\hat{\rho}^{AE})|\Phi\rangle \\ &\leqslant \frac{1}{3} d_A \max_{\mathcal{E}} \langle\Phi|\mathcal{E}(\rho^{AE})|\Phi\rangle \\ &\quad + \frac{2}{3} d_A \max_{\mathcal{E}} \langle\Phi|\left(\frac{\mathbb{I}^A}{2^n} \otimes \mathcal{E}(\rho^E)\right)|\Phi\rangle \\ &\leqslant \frac{1}{3} 2^{-(t-1)} + \frac{2}{3} d_A \langle\Phi|\left(\frac{\mathbb{I}^{AE}}{2^n}\right)|\Phi\rangle \\ &\leqslant \frac{1}{3} 2^{-(t-1)} + \frac{2}{3} \cdot \frac{1}{2^n} \\ &= \frac{2}{3}\left(2^{-t} + \frac{1}{2^n}\right) \\ &\leqslant \frac{2}{3}\left(2^{-t} + \frac{2^{-t}}{2}\right) \\ &= 2^{-t}. \end{aligned}$$

Since $\left\|\mathcal{E}(\rho^{AE}) - \Omega^{A'} \otimes \rho^E\right\|_1 > 6\varepsilon$, we know that there exists an adversary that can distinguish $\mathcal{E}(\rho^{AE})$ from $\Omega^{A'} \otimes \rho^E$ with probability at least $\frac{1}{2} + \frac{3}{2}\varepsilon$. Let's call this adversary A, and let's assume that it gives the right answer with probability η_1 when it is given $\mathcal{E}(\rho^{AE})$ and with probability η_2 when it is given $\Omega^{A'} \otimes \rho^E$. We then have $\frac{1}{2}(\eta_1 + \eta_2) > \frac{1}{2} + \frac{3}{2}\varepsilon$.

Now, consider the following interpretation of $\hat{\rho}^{AE}$:

$$\hat{\rho}^{AE} = \frac{1}{3}\sigma_1^{AE} + \frac{1}{3}\sigma_2^{AE} + \frac{1}{3}\sigma_3^{AE} \tag{17}$$

where $\sigma_1^{AE} = \rho^{AE}$ and $\sigma_2^{AE} = \sigma_3^{AE} = \frac{\mathbb{I}}{d_A} \otimes \rho^E$. We shall show that A violates entropic security for $\hat{\rho}^{AE}$, with this interpretation and the function $h(i) = i$.

First of all, it is clear that by having access only to Eve's system, no adversary can guess the value of h with a probability greater than 1/3. Let us now determine what A can do by having access to the encrypted version of $\hat{\rho}^{AE}$. One possible strategy

for A is to try to distinguish between $\mathcal{E}(\rho^{AE})$ and $\Omega^{A'} \otimes \rho^E$ and return 1 when it gets $\mathcal{E}(\rho^{AE})$ and randomly return either 2 or 3 when it gets $\Omega^{A'} \otimes \rho^E$. We then have

$$\begin{aligned}\Pr[\mathsf{A}(\mathcal{E}(\sigma_i^{AE})) = h(i)] &= \frac{1}{3}\eta_1 + \frac{2}{3}\frac{\eta_2}{2} \\ &= \frac{1}{3}(\eta_1 + \eta_2) \\ &> \frac{1}{3}(1 + 3\varepsilon) \\ &= \frac{1}{3} + \varepsilon.\end{aligned}$$

Finally we get that for all adversaries A',

$$\left|\Pr[\mathsf{A}(\mathcal{E}(\sigma_i^{AE})) = h(i)] - \underbrace{\Pr[\mathsf{A}'(\sigma_i^E) = h(i)]}_{=\frac{1}{3}}\right| > \varepsilon$$

a violation of entropic security. ∎

V. Two Encryption Schemes

Before presenting the ciphers, we will give some definitions and technical lemmas which will be used in the presentation of both encryption schemes.

First, we define the following shortcut for any matrix σ^{AE}:

$$M_{uv}^{\sigma} := \mathrm{Tr}_A\left[\left(\frac{Z^v X^u}{\sqrt{d_A}} \otimes \mathbb{I}\right)\sigma^{AE}\right]. \tag{18}$$

We also define

$$\tilde{\rho}^{AE} := \rho^{AE} - \frac{\mathbb{I}}{d_A} \otimes \rho^E \tag{19}$$

for any state ρ^{AE}, where σ^E is a state such that $\rho^{AE} \leqslant 2^{-H_\infty(A|E)_\rho}\mathbb{I}^A \otimes \sigma^E$.

Lemma 4: For every density matrix σ^{AE}, we have that $\sigma^{AE} = \sum_{uv} \frac{X^u Z^v}{\sqrt{d_A}} \otimes M_{uv}^{\sigma}$.

Proof: Let $\{E_j\}$ be an orthonormal basis for $\mathcal{L}(\mathcal{H}_E)$. Since Pauli matrices form an orthonormal basis for $\mathcal{L}(\mathcal{H}_A)$, we have

$$\begin{aligned}\sigma^{AE} &= \sum_{uvj} \frac{X^u Z^v}{\sqrt{d_A}} \otimes E_j \mathrm{Tr}\left[\left(\frac{Z^v X^u}{\sqrt{d_A}} \otimes E_j^\dagger\right)\sigma^{AE}\right] &(20)\\ &= \sum_{uvj} \frac{X^u Z^v}{\sqrt{d_A}} \otimes E_j \mathrm{Tr}\left[E_j^\dagger M_{uv}^{\sigma}\right] &(21)\\ &= \sum_{uv} \frac{X^u Z^v}{\sqrt{d_A}} \otimes \left\{\sum_j E_j \mathrm{Tr}\left[E_j^\dagger M_{uv}^{\sigma}\right]\right\} &(22)\\ &= \sum_{uv} \frac{X^u Z^v}{\sqrt{d_A}} \otimes M_{uv}^{\sigma}. &(23)\end{aligned}$$

∎

We will also make use of the following lemma ([5, Lemma 5.1.3]):

Lemma 5: Let S be a Hermitian operator and let σ be any positive definite operator. Then

$$\|S\|_1 \leqslant \sqrt{\mathrm{Tr}\,(\sigma)\,\mathrm{Tr}\left(S\sigma^{-1/2}S\sigma^{-1/2}\right)}.$$

A. A Scheme Based on δ-Biased Sets

In [8], Ambainis and Smith introduced an approximate quantum encryption scheme based on δ-biased sets. Here, we shall show that if $H_\infty(A|E)_\rho \geqslant t$, then the Ambainis-Smith scheme is (t,ε)-secure using $n - t + 2\log n + 2\log(\frac{1}{\varepsilon})$ bits of key, where n is the logarithm of d_A as usual.

Definition 5 (δ-Biased Set): A set $S \subseteq \{0,1\}^n$ is said to be δ-biased if and only if for every $s' \in \{0,1\}^n, s' \neq 0^n$, we have that $\left|\frac{1}{|S|}\sum_{s\in S}(-1)^{s\odot s'}\right| \leqslant \delta$.

There exist several efficient constructions of δ-biased sets ([14]–[16]); following [3], we will use the one from [16], which yields sets of size n^2/δ^2 (note that Dickinson and Nayak [17] improve this to $\leqslant 16/\delta^2$).

The Ambainis-Smith scheme consists of applying an operator at random from the set

$$\left\{X^a Z^b : a\|b \in S \text{ and } |a| = |b| = n\right\}$$

where S is a δ-biased set containing strings of length $2n$. The shared private key is used to index one of the operators. In other words, the encryption operator is

$$\mathcal{E}(\rho^{AE}) = \frac{1}{|S|}\sum_{a\|b\in S}(X^a Z^b \otimes \mathbb{I})\rho^{AE}(Z^b X^a \otimes \mathbb{I}).$$

We shall now prove that this scheme is secure in our framework. The following lemma contains most of the proof, and the main theorem follows.

Lemma 6: For any state ρ^{AE} with $H_\infty(A|E)_\rho \geqslant t$, we have that

$$\left\|\mathcal{E}(\rho^{AE}) - \frac{\mathbb{I}}{d_A} \otimes \rho^E\right\|_1 \leqslant \delta\sqrt{d_A 2^{-t}}. \tag{24}$$

Proof: Let σ^E be a state such that $\rho^{AE} \leqslant 2^{-t}\mathbb{I}^A \otimes \sigma^E$ and write

$$\left\|\mathcal{E}(\rho^{AE}) - \frac{\mathbb{I}}{d_A} \otimes \rho^E\right\|_1 \leqslant \sqrt{d_A \mathrm{Tr}\left[\mathcal{E}(\tilde{\rho}^{AE})(\mathbb{I} \otimes \sigma^{E^{-\frac{1}{2}}})\mathcal{E}(\tilde{\rho}^{AE})(\mathbb{I} \otimes \sigma^{E^{-\frac{1}{2}}})\right]}. \tag{25}$$

This is due to Lemma 5, with $\sigma = \mathbb{I} \otimes \sigma^E$; without loss of generality, we can assume that ρ^E has full rank by considering $\mathcal{H}_E$ to be the support of ρ^E. We continue by applying Lemma 4 on $\tilde{\rho}^{AE}$:

$$\tilde{\rho}^{AE} = \sum_{uv} \frac{X^u Z^v}{\sqrt{d_A}} \otimes M_{uv}^{\tilde{\rho}} \tag{26}$$

and therefore

$$\mathcal{E}(\tilde{\rho}^{AE}) = \sum_{uv} \mathcal{E}\left(\frac{X^u Z^v}{\sqrt{d_A}}\right) \otimes M^{\tilde{\rho}}_{uv} \tag{27}$$

$$= \sum_{uv} \alpha_{uv} \frac{X^u Z^v}{\sqrt{d_A}} \otimes M^{\tilde{\rho}}_{uv} \tag{28}$$

where $\alpha_{uv} = \frac{1}{|S|}\sum_{a||b\in S}(-1)^{v||u\odot a||b}$, and since $\mathrm{Tr}[\tilde{\rho}^{AE}] = 0$, we can neglect the term $v||u = 0^{2n}$, and, hence, $|\alpha_{uv}| \leqslant \delta$.

We now compute the trace in (25) as follows: [see (29) at the bottom of the page] where

- (a) comes from the fact that $(\mathbb{I}\otimes\sigma^{E^{-\frac{1}{2}}})\mathcal{E}(\tilde{\rho}^{AE})(\mathbb{I}\otimes\sigma^{E^{-\frac{1}{2}}})$ is Hermitian, hence taking its adjoint leaves it unchanged;
- (b) is true because terms in which the u, v pairs are not the same in both sums disappear when we take the trace;
- (c) because $\alpha_{uv}^2 \geqslant \delta^2$ and every term in the sum has a nonnegative trace since $\mathrm{Tr}[M^{\tilde{\rho}}_{uv}\sigma^{E^{-\frac{1}{2}}}M^{\tilde{\rho}}_{uv}{}^{\dagger}\sigma^{E^{-\frac{1}{2}}}] = \mathrm{Tr}[(\sigma^{-\frac{1}{4}}M^{\tilde{\rho}}_{uv}\sigma^{-\frac{1}{4}})(\sigma^{-\frac{1}{4}}M^{\tilde{\rho}}_{uv}\sigma^{-\frac{1}{4}})^{\dagger}]$.
- (d) is justified below;
- (e) is due to Lemma 4; and
- (f) comes from the fact that $\rho^{AE} \leqslant 2^{-t}\mathbb{I}\otimes\sigma^E \Rightarrow (\mathbb{I}\otimes\sigma^{E^{-\frac{1}{2}}})\rho^{AE}(\mathbb{I}\otimes\sigma^{E^{-\frac{1}{2}}}) \leqslant 2^{-t}\mathbb{I}^{AE}$.

To justify (d), we first observe that $M^{\rho}_{uv} = M^{\tilde{\rho}}_{uv} + M^{\tau}_{uv}$, where $\tau = \frac{\mathbb{I}}{d_A}\otimes\rho^E$. Hence

$$\begin{aligned}
&\mathrm{Tr}\left[\sum_{uv}\frac{\mathbb{I}^A}{d_A}\otimes M^{\rho}_{uv}\sigma^{E^{-\frac{1}{2}}}M^{\rho}_{uv}{}^{\dagger}\sigma^{E^{-\frac{1}{2}}}\right] \\
&\quad= \mathrm{Tr}\left[\sum_{uv}\frac{\mathbb{I}^A}{d_A}\otimes M^{\tilde{\rho}}_{uv}\sigma^{E^{-\frac{1}{2}}}M^{\tilde{\rho}}_{uv}{}^{\dagger}\sigma^{E^{-\frac{1}{2}}}\right] \\
&\qquad+ \mathrm{Tr}\left[\sum_{uv}\frac{\mathbb{I}^A}{d_A}\otimes M^{\tilde{\rho}}_{uv}\sigma^{E^{-\frac{1}{2}}}M^{\tau}_{uv}{}^{\dagger}\sigma^{E^{-\frac{1}{2}}}\right] \\
&\qquad+ \mathrm{Tr}\left[\sum_{uv}\frac{\mathbb{I}^A}{d_A}\otimes M^{\tau}_{uv}\sigma^{E^{-\frac{1}{2}}}M^{\tilde{\rho}}_{uv}{}^{\dagger}\sigma^{E^{-\frac{1}{2}}}\right] \\
&\qquad+ \mathrm{Tr}\left[\sum_{uv}\frac{\mathbb{I}^A}{d_A}\otimes M^{\tau}_{uv}\sigma^{E^{-\frac{1}{2}}}M^{\tau}_{uv}{}^{\dagger}\sigma^{E^{-\frac{1}{2}}}\right].
\end{aligned} \tag{30}$$

Step (d) then follows when we combine this with the observation that $M^{\tau}_{00} = \rho^E$, $M^{\tau}_{uv} = 0$ if $uv \neq 00$, and $M^{\tilde{\rho}}_{00} = 0$: the first sum is what we want to bound; the two sums in the middle evaluate to the zero matrix; and in the last sum, only the 00 term remains, which clearly has a positive trace.

Substituting the end result of (29) in (25), we obtain

$$\left\|\mathcal{E}(\rho^{AE}) - \frac{\mathbb{I}}{d_A}\otimes\rho^E\right\|_1 \leqslant \delta\sqrt{d_A 2^{-t}}. \tag{31}$$

■

$$\begin{aligned}
&\mathrm{Tr}\left[\mathcal{E}(\tilde{\rho}^{AE})(\mathbb{I}\otimes\sigma^{E^{-\frac{1}{2}}})\mathcal{E}(\tilde{\rho}^{AE})(\mathbb{I}\otimes\sigma^{E^{-\frac{1}{2}}})\right] \\
&\quad= \mathrm{Tr}\left[\left(\sum_{uv}\alpha_{uv}\frac{X^uZ^v}{\sqrt{d_A}}\otimes M^{\tilde{\rho}}_{uv}\right)\left(\sum_{uv}\alpha_{uv}\frac{X^uZ^v}{\sqrt{d_A}}\otimes\sigma^{E^{-\frac{1}{2}}}M^{\tilde{\rho}}_{uv}\sigma^{E^{-\frac{1}{2}}}\right)\right] \\
&\quad\overset{(a)}{=} \mathrm{Tr}\left[\left(\sum_{uv}\alpha_{uv}\frac{X^uZ^v}{\sqrt{d_A}}\otimes M^{\tilde{\rho}}_{uv}\right)\left(\sum_{uv}\alpha_{uv}\frac{Z^vX^u}{\sqrt{d_A}}\otimes\sigma^{E^{-\frac{1}{2}}}M^{\tilde{\rho}}_{uv}{}^{\dagger}\sigma^{E^{-\frac{1}{2}}}\right)\right] \\
&\quad\overset{(b)}{=} \mathrm{Tr}\left[\sum_{uv}\alpha_{uv}^2\frac{\mathbb{I}^A}{d_A}\otimes M^{\tilde{\rho}}_{uv}\sigma^{E^{-\frac{1}{2}}}M^{\tilde{\rho}}_{uv}{}^{\dagger}\sigma^{E^{-\frac{1}{2}}}\right] \\
&\quad\overset{(c)}{\leqslant} \delta^2\mathrm{Tr}\left[\sum_{uv}\frac{\mathbb{I}^A}{d_A}\otimes M^{\tilde{\rho}}_{uv}\sigma^{E^{-\frac{1}{2}}}M^{\tilde{\rho}}_{uv}{}^{\dagger}\sigma^{E^{-\frac{1}{2}}}\right] \\
&\quad\overset{(d)}{\leqslant} \delta^2\mathrm{Tr}\left[\sum_{uv}\frac{\mathbb{I}^A}{d_A}\otimes M^{\rho}_{uv}\sigma^{E^{-\frac{1}{2}}}M^{\rho}_{uv}{}^{\dagger}\sigma^{E^{-\frac{1}{2}}}\right] \\
&\quad= \delta^2\mathrm{Tr}\left[\left(\sum_{uv}\frac{X^uZ^v}{\sqrt{d_A}}\otimes M^{\rho}_{uv}\right)\left(\sum_{uv}\frac{Z^vX^u}{\sqrt{d_A}}\otimes\sigma^{E^{-\frac{1}{2}}}M^{\rho}_{uv}{}^{\dagger}\sigma^{E^{-\frac{1}{2}}}\right)\right] \\
&\quad\overset{(e)}{=} \delta^2\mathrm{Tr}\left[\rho^{AE}\left((\mathbb{I}\otimes\sigma^{E^{-\frac{1}{2}}})\rho^{AE}(\mathbb{I}\otimes\sigma^{E^{-\frac{1}{2}}})\right)^{\dagger}\right] \\
&\quad= \delta^2\mathrm{Tr}\left[\rho^{AE}(\mathbb{I}\otimes\sigma^{E^{-\frac{1}{2}}})\rho^{AE}(\mathbb{I}\otimes\sigma^{E^{-\frac{1}{2}}})\right] \\
&\quad\overset{(f)}{\leqslant} \delta^2\mathrm{Tr}\left[\rho^{AE}2^{-t}\mathbb{I}^{AE}\right] = \delta^2 2^{-t}
\end{aligned} \tag{29}$$

The main theorem now easily follows.

Theorem 3: If $H_\infty(A|E)_\rho \geqslant t$, then the Ambainis-Smith scheme is (t,ε)-secure using $n-t+2\log n+2\log(\frac{1}{\varepsilon})+2$ bits of key, where $n=\log d_A$.

Proof: If we choose $\delta=\varepsilon/2^{(n-t)/2}$ and construct S using the method of [16] such that $|S|=(2n)^2/\delta^2$, by Lemma 6 we obtain $\left\|\mathcal{E}(\rho^{AE})-\frac{\mathbb{I}}{d_A}\otimes\rho^E\right\|_1\leqslant\varepsilon$ using $n-t+2\log n+2\log(\frac{1}{\varepsilon})+2$ bits of key. ∎

B. A Scheme Based on XOR-Universal Functions

Our second scheme based on XOR-universal functions can be considered as a quantum version of the scheme given in [3]. This scheme can also be viewed as a generalization of the second scheme of [8].

Definition 6: Let $\mathsf{H}_n=\{h_i\}_{i\in I}$ be a finite family of functions from n-bit strings to n-bit strings. We say the family H_n is strongly-XOR-universal if for all n-bit strings a, x, and y such that $x\neq y$ we have

$$\Pr_i[h_i(x)\oplus h_i(y)=a]=\frac{1}{2^n},$$

where i is distributed uniformly over I. The family proposed in [3] naturally possesses this property if one allows i to be zero.

We define our second cipher as follows. Let H_{2n} be a strongly XOR-universal family of functions. The encryption operator for the key k is defined as

$$\mathcal{E}_k(\rho)=\frac{1}{|I|}\sum_{i\in I}|i\rangle\langle i|^{A'}\otimes(X^aZ^b\otimes\mathbb{I}^E)\rho^{AE}(Z^bX^a\otimes\mathbb{I}^E) \quad (32)$$

where $a||b=h_i(k)$, $|a|=|b|=n$, $h_i\in\mathsf{H}_{2n}$ and k is the secret key selected uniformly at random from a set $K\subseteq\{0,1\}^{2n}$. The overall cipher can be described by the superoperator

$$\mathcal{E}(\rho)=\frac{1}{|I||K|}\sum_{i\in I,k\in K}|i\rangle\langle i|^{A'}\otimes(X^aZ^b\otimes\mathbb{I}^E)\rho^{AE}(Z^bX^a\otimes\mathbb{I}^E). \quad (33)$$

The structure of K is irrelevant; only its cardinality matters for the security of the scheme. Not that this scheme is not length preserving since the ancillary system A' is part of the ciphertext. We now prove that this scheme is secure with the following theorem.

Theorem 4: $\mathcal{E}$ is (t,ε)-indistinguishable if $\log|K|\geqslant n-t+2\log(1/\varepsilon)$.

Proof: To show that the cipher is (t,ε)-indistinguishable, we must show that for all states ρ^{AE} such that $H_\infty(A|E)_\rho\geqslant t$

$$\left\|\mathcal{E}(\rho^{AE})-\frac{\mathbb{I}^{AA'}}{|I|d_A}\otimes\rho^E\right\|_1\leqslant\varepsilon. \quad (34)$$

As in the proof of our other scheme, we use Lemma 5 with $\sigma=\mathbb{I}^{AA'}\otimes\rho^E$ to bound this

$$\left\|\mathcal{E}(\rho^{AE})-\frac{\mathbb{I}^{AA'}}{|I|d_A}\otimes\rho^E\right\|_1\leqslant\sqrt{|I|d_A\mathrm{Tr}\left[\mathcal{E}(\tilde{\rho}^{AE})(\mathbb{I}\otimes\sigma^{E^{-\frac{1}{2}}})\mathcal{E}(\tilde{\rho}^{AE})(\mathbb{I}\otimes\sigma^{E^{-\frac{1}{2}}})\right]}. \quad (35)$$

To compute the trace in the above expression, we first express $\mathcal{E}(\tilde{\rho}^{AE})$ using Lemma 4

$$\mathcal{E}(\tilde{\rho}^{AE})=\sum_{uv}\mathcal{E}\left(\frac{X^uZ^v}{\sqrt{d_A}}\right)\otimes M^{\tilde{\rho}}_{uv} \quad (36)$$

$$=\sum_{uvki}\alpha_{uvki}|i\rangle\langle i|\otimes\frac{X^uZ^v}{\sqrt{d_A}}\otimes M^{\tilde{\rho}}_{uv} \quad (37)$$

where $\alpha_{uvki}=\frac{1}{|I||K|}(-1)^{v||u\odot a||b}$ where $a||b=h_i(k)$.

We are now ready to evaluate the trace in (35): [see (38) at the bottom of the page] where

- (a) comes from the fact that $(\mathbb{I}\otimes\sigma^{E^{-\frac{1}{2}}})\mathcal{E}(\tilde{\rho}^{AE})(\mathbb{I}\otimes\sigma^{E^{-\frac{1}{2}}})$ is Hermitian, hence taking its adjoint leaves it unchanged;
- (b) is true because terms in which the u,v,i triples are not the same in both sums disappear when we take the trace.

$$\begin{aligned}
&\mathrm{Tr}\left[\mathcal{E}(\tilde{\rho}^{AE})(\mathbb{I}\otimes\sigma^{E^{-\frac{1}{2}}})\mathcal{E}(\tilde{\rho}^{AE})(\mathbb{I}\otimes\sigma^{E^{-\frac{1}{2}}})\right]\\
&=\mathrm{Tr}\left[\left(\sum_{uvki}\alpha_{uvki}|i\rangle\langle i|\otimes\frac{X^uZ^v}{\sqrt{d_A}}\otimes M^{\tilde{\rho}}_{uv}\right)\left(\sum_{uvki}\alpha_{uvki}|i\rangle\langle i|\otimes\frac{X^uZ^v}{\sqrt{d_A}}\otimes\sigma^{E^{-\frac{1}{2}}}M^{\tilde{\rho}}_{uv}\sigma^{E^{-\frac{1}{2}}}\right)\right]\\
&\overset{(a)}{=}\mathrm{Tr}\left[\left(\sum_{uvki}\alpha_{uvki}|i\rangle\langle i|\otimes\frac{X^uZ^v}{\sqrt{d_A}}\otimes M^{\tilde{\rho}}_{uv}\right)\left(\sum_{uvki}\alpha_{uvki}|i\rangle\langle i|\otimes\frac{Z^vX^u}{\sqrt{d_A}}\otimes\sigma^{E^{-\frac{1}{2}}}M^{\tilde{\rho}\,\dagger}_{uv}\sigma^{E^{-\frac{1}{2}}}\right)\right]\\
&\overset{(b)}{=}\mathrm{Tr}\left[\sum_{uvkk'i}\alpha_{uvki}\alpha_{uvk'i}\frac{\mathbb{I}^A}{d_A}\otimes M^{\tilde{\rho}}_{uv}\sigma^{E^{-\frac{1}{2}}}M^{\tilde{\rho}\,\dagger}_{uv}\sigma^{E^{-\frac{1}{2}}}\right]\\
&\overset{(c)}{=}\frac{1}{|I||K|}\mathrm{Tr}\left[\sum_{uv}\frac{\mathbb{I}^A}{d_A}\otimes M^{\tilde{\rho}}_{uv}\sigma^{E^{-\frac{1}{2}}}M^{\tilde{\rho}\,\dagger}_{uv}\sigma^{E^{-\frac{1}{2}}}\right]\\
&\overset{(d)}{\leqslant}\frac{2^{-t}}{|I||K|}
\end{aligned} \quad (38)$$

Taking the partial trace on the subsystem containing $|i\rangle\langle i|$ then yields this.

- (c) is justified below
- (d) follows exactly the same argument as in equation block (29) from line (d) onwards.

We now justify step (c). We first consider the terms of the sum in which $k \neq k'$. In the following, let $a\|b = h_i(k)$ and $c\|d = h_i(k')$. If $k \neq k'$, we have

$$\begin{aligned}&\sum_{i\in I}\alpha_{uvki}\alpha_{uvk'i}\\&\quad=\sum_{i\in I}\frac{1}{|I|^2|K|^2}(-1)^{v\|u\odot a\|b}(-1)^{v\|u\odot c\|d}\\&\quad=\sum_{i\in I}\frac{1}{|I|^2|K|^2}(-1)^{(v\|u\odot a\|b)\oplus(v\|u\odot c\|d)}\\&\quad=\sum_{i\in I}\frac{1}{|I|^2|K|^2}(-1)^{v\|u\odot(a\|b\oplus c\|d)}.\end{aligned}\tag{39}$$

However, by Definition 6, $a\|b\oplus c\|d$ is uniformly distributed over all $2n$-bit strings when i is chosen uniformly at random. This sum is therefore equal to zero whenever $u\|v \neq 0^{2n}$, and to $\frac{1}{|I||K|^2}$ when $u\|v = 0^{2n}$. However, we observe that $M^{\tilde{\rho}}_{00} = 0$, and hence those terms also disappear from the sum inside the trace.

To take care of the case where $k = k'$, it can easily be shown that $\alpha^2_{uvki} = \frac{1}{|I|^2|K|^2}$. Summing over all i and k, step (c) follows.

Now, by hypothesis, we have $\log|K| \geqslant n - t + 2\log(1/\varepsilon)$, which can be transformed into $-\log|K| - t \leqslant \log(\varepsilon^2) - \log d_A$. Exponentiating both sides yields $\frac{2^{-t}}{|K|} \leqslant \frac{\varepsilon^2}{d_A}$. Combining this bound with (38) and substituting in (35) concludes the proof. ■

VI. Minimum Requirement for the Key Length

We can generalize the proof for the lower bound on the key length found in [3] to the quantum world and the conditional min-entropy definition.

Theorem 5: Any quantum encryption scheme which is (t,ε)-indistinguishable for inputs of n qubits requires a key of length at least $n - t - 1$ as long as $\varepsilon \leqslant 1/2$.

Proof: We prove this by constructing a state with conditional min-entropy t which provably requires at least $n - t - 1$ bits of key to be securely encrypted. Consider the state $\rho^{A\hat{A}E} = |\Phi^+\rangle\langle\Phi^+|^{AE} \otimes \frac{\mathbb{I}^{\hat{A}}}{d_{\hat{A}}}$ where $|\Phi^+\rangle^{AE} = \sum_{i=1}^{d_A}|i\rangle^A|i\rangle^E$ is a maximally entangled state; Alice wants to send both A and $\hat{A}$ to Bob securely. Furthermore, let $d_A = d_E = 2^{(n-t)/2}$ and $d_{\hat{A}} = 2^{(n+t)/2}$, hence, $d_{A\hat{A}} = 2^n$. It is easy to compute the conditional min-entropy of this state

$$\begin{aligned}H_\infty(A\hat{A}|E)_\rho &= H_\infty(A|E)_{|\Phi^+\rangle\langle\Phi^+|} + H_\infty(\hat{A})_{\mathbb{I}^{\hat{A}}/d_{\hat{A}}}\\&= -\frac{(n-t)}{2} + \frac{(n+t)}{2}\\&= t.\end{aligned}$$

Now, it is clear that this state requires at least as much key to encrypt as $|\Phi^+\rangle\langle\Phi^+|^{AE}$ alone, since one could securely encrypt $|\Phi^+\rangle\langle\Phi^+|^{AE}$ using a protocol to encrypt $\rho^{A\hat{A}E}$ by adding $(n+t)/2$ random qubits to the input state. However, as the following theorem proves, $|\Phi^+\rangle\langle\Phi^+|^{AE}$ requires at least $(n-t)-1$ bits of key to encrypt. ■

Theorem 6: Let $\mathcal{E}^{\tilde{A}\longrightarrow A}$ be a cipher such that for all states $\rho^{\tilde{A}E}$, there exists some state Ω^A such that

$$\left\|(\mathcal{E}^{\tilde{A}}\otimes\mathbb{I}^E)(\rho^{\tilde{A}E}) - \Omega^A\otimes\rho^E\right\|_1 \leqslant \varepsilon\tag{40}$$

then $\mathcal{E}$ requires at least $2\log(d_{\tilde{A}}) - 1$ bits of key, or $2n-1$ bits of key for an n-qubit system, whenever $\varepsilon \leqslant 1/2$.

Before proving this, we first need a technical lemma which says that by conditioning on a classical system, we cannot reduce the min-entropy by more than the dimension of the system.

Lemma 7: Given a state $\omega^{AEK} = \sum_k p_k\omega_k^{AE}\otimes\omega_k^K$, we have that $H_\infty(E|AK)_\omega \geqslant H_\infty(E|A)_\omega - \log|K|$.

Proof:

$$\begin{aligned}&2^{-H_\infty(E|AK)}\\&\quad=\min_{\sigma^{AE}}\min\left\{\lambda:\lambda\mathbb{I}^E\otimes\sigma^{AK}\geqslant\omega^{AEK}\right\}\\&\quad\leqslant\min_{\sigma^{A}}\min\left\{\lambda:\lambda\mathbb{I}^E\otimes\sigma^{A}\otimes\frac{\mathbb{I}^K}{|K|}\geqslant\omega^{AEK}\right\}\\&\quad=|K|\min_{\sigma^{A}}\min\left\{\lambda:\lambda\mathbb{I}^{EK}\otimes\sigma^{A}\geqslant\omega^{AEK}\right\}\\&\quad\leqslant|K|\min_{\sigma^{A}}\min\left\{\lambda:\lambda\mathbb{I}^{E}\otimes\sigma^{A}\geqslant\omega^{AE}\right\}\\&\quad=|K|2^{-H_\infty(E|A)}\end{aligned}$$

where the second inequality holds due to the fact that

$$\begin{aligned}&\omega^{AE}\leqslant\lambda\mathbb{I}^E\otimes\sigma^A\\&\quad\Rightarrow\omega^{AE}\otimes\mathbb{I}^K\leqslant\lambda\mathbb{I}^{EK}\otimes\sigma^A\\&\quad\Rightarrow\omega^{AEK}\leqslant\lambda\mathbb{I}^{EK}\otimes\sigma^A.\end{aligned}$$

The last implication is true since the classicality of K ensures that $\omega^{AEK}\leqslant\omega^{AE}\otimes\mathbb{I}^K$. ■

Proof of Theorem 6: Let $\mathcal{H}_{\tilde{A}} \cong \mathcal{H}_E$, and let $\rho^{\tilde{A}E} = |\Phi^+\rangle\langle\Phi^+|^{\tilde{A}E}$. Then, by the Fuchs-van de Graaf inequalities [18][3], we have that

$$F\left(\mathcal{E}(\rho),\Omega^A\otimes\frac{\mathbb{I}^E}{2^n}\right)^2 \geqslant 1-\varepsilon.\tag{41}$$

Now, let ζ^{AEK} be a state such that $\mathrm{Tr}_K[\zeta^{AEK}] = \mathcal{E}(\rho)$ and in which the K register holds the key

$$\zeta^{AEK} = \frac{1}{|K|}\sum_k\mathcal{E}_k(\rho^{\tilde{A}E})\otimes|k\rangle\langle k|^K.$$

Then, by Uhlmann's theorem ([19], or see [10, Theorem 9.4])

$$F\left(\mathcal{E}(\rho),\Omega\otimes\frac{\mathbb{I}}{2^n}\right)^2 = \max_{\sigma,\mathrm{Tr}_K[\sigma]=\Omega\otimes\frac{\mathbb{I}}{2^n}}F\left(\zeta^{AEK},\sigma^{AEK}\right)^2.$$

Now, let σ^{AEK} be a state such that $\mathrm{Tr}_K[\sigma^{AEK}] = \Omega\otimes\frac{\mathbb{I}}{2^n}$ that maximizes the above fidelity. Also, let $\omega^{AEKK'} = V\sigma^{AEK}V^\dagger$ and $\xi^{AEKK'} = V\zeta^{AEK}V^\dagger$, where $V^{K\longrightarrow KK'} = \sum_k|kk\rangle\langle k|$,

[3]See also Eq. 9.110 in Nielsen and Chuang.

$\mathcal{H}_K \cong \mathcal{H}_{K'}$ and $\{|k\rangle\}_{k\in K}$ is the computational basis on $\mathcal{H}_K$. Note that this ensures that ω^{AEK} is classical on K. We then have:

$$\begin{aligned} F\left(\mathcal{E}(\rho), \Omega \otimes \frac{\mathbb{I}}{2^n}\right)^2 &= F\left(\zeta^{AEK}, \sigma^{AEK}\right)^2 \\ &= F\left(\xi^{AEKK'}, \omega^{AEKK'}\right)^2 \\ &\leqslant F\left(\xi^{AEK}, \omega^{AEK}\right)^2 \\ &\leqslant F\left(\Phi^{\tilde{A}E}, \mathcal{D}(\omega^{AEK})\right)^2 \\ &\leqslant \max_{\mathcal{G}^{AK}\longrightarrow \tilde{A}} F\left(\Phi^{\tilde{A}E}, \mathcal{G}(\omega^{AEK})\right)^2 \\ &= \frac{2^{-H_\infty(E|AK)_\omega}}{2^n} \end{aligned}$$

where $\mathcal{D}^{AK\longrightarrow \tilde{A}}$ is a superoperator which decrypts and then forgets the key. Now, by Lemma 7 above, we have that for any state ω^{AEK} such that $\mathrm{Tr}_K[\omega^{AEK}] = \Omega^A \otimes \frac{\mathbb{I}^E}{2^n}$ that is classical on K, $H_\infty(E|AK)_\omega \geqslant n - \log|K|$. Hence

$$1-\varepsilon \leqslant F\left(\mathcal{E}(\rho), \Omega \otimes \frac{\mathbb{I}}{2^n}\right)^2 \tag{42}$$

$$\leqslant \frac{2^{-n+\log|K|}}{2^n} \tag{43}$$

$$= |K| \cdot 2^{-2n} \tag{44}$$

and, therefore, $|K| \geqslant 2^{2n}(1-\varepsilon)$. Hence $\log|K| \geqslant 2n + \log(1-\varepsilon) \geqslant 2n-1$ if, as assumed, $\varepsilon \leqslant \frac{1}{2}$. ∎

The tighter bound of [3] for schemes using public coins, given there as proposition 3.8, cannot be similarly generalized.

VII. Conclusion

We have shown how to fully generalize the notions of entropic security and entropic indistinguishability without making any assumption on the entanglement between the sender and the adversary. Furthermore, we proved that the two approximate quantum encryption scheme presented in [8] are also secure in this model. Is it possible to prove a general theorem showing that every quantum encryption scheme is entropically secure? If it is true, it would require different techniques than the ones used here, since our proofs rely on the fact that the ciphers give guarantees in the 2-norm, and not only in the 1-norm as in the definition of an approximate cipher. We leave this as an open problem.

Acknowledgment

The authors would like to thank the following people for enlightening discussions and/or useful comments on the draft of this paper: G. Brassard, C. Crépeau, P. Hayden, D. Leung, J.-R. Simard, and A. Smith. They would also like to thank the referee for pointing out a flaw in an earlier version of this paper.

References

[1] S. Goldwasser and S. Micali, "Probabilistic encryption," *J. Comput. Syst. Sci.*, vol. 28, no. 2, pp. 270–299, 1984.

[2] A. Russell and H. Wang, "How to fool an unbounded adversary with a short key," in *EUROCRYPT'02: Proc. Int. Conf. Theory and Appl. Cryptogr. Tech.*, London, U.K., 2002, pp. 133–148. [Online]. Available: http://ieeexplore.ieee.org/iel5/18/33700/01603776.pdf?arnumber=1603776

[3] Y. Dodis and A. Smith, Entropic Security and the Encryption of High Entropy Messages, Cryptology ePrint Archive 2004, Report 2004/219.

[4] S. P. Desrosiers, "Entropic security in quantum cryptography," *Quantum Inf. Process.*, vol. 8, no. 4, pp. 331–345, 2009.

[5] R. Renner, "Security of quantum key distribution," Ph.D. dissertation, Swiss Fed. Inst. Technol., Lausanne, 2005.

[6] A. Ambainis, M. Mosca, A. Tapp, and R. de Wolf, "Private quantum channels," in *Proc. IEEE Symp. Found. Comput. Sci.*, 2000, pp. 547–553 [Online]. Available: citeseer.nj.nec.com/article/ambainis00private.html

[7] P. Hayden, D. Leung, P. Shor, and A. Winter, "Randomizing quantum states: Constructions and applications," *Commun. Math. Phys.*, vol. 250, no. 2, pp. 371–391, 2004.

[8] A. Ambainis and A. Smith, "Small pseudo-random families of matrices: Derandomizing approximate quantum encryption," in *APPROX-RANDOM, ser. Lecture Notes in Comput. Sci.*, K. Jansen, S. Khanna, J. D. P. Rolim, and D. Ron, Eds. New York: Springer, 2004, vol. 3122, pp. 249–260.

[9] S. Fehr and C. Schaffner, *Randomness Extraction via Delta-Biased Masking in the Presence of a Quantum Attacker,* 2007 [Online]. Available: http://www.springerlink.com/content/t33304541k4p1110/

[10] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*. New York: Cambridge Univ. Press, 2000.

[11] C. W. Helstrom, "Quantum detection and estimation theory," *J. Statist. Phys.*, vol. 1, no. 2, pp. 231–252, 1969.

[12] R. König, R. Renner, and C. Schaffner, "The operational meaning of min- and max-entropy," *IEEE Trans. Inf. Theory*, vol. 55, no. 9, pp. 4337–4347, Sep. 2009.

[13] O. Goldreich and L. A. Levin, "A hard-core predicate for all one-way functions," in *STOC'89: Proc. 21st Ann. ACM Symp. Theory Comput.*, New York, 1989, pp. 25–32.

[14] J. Naor and M. Naor, "Small-bias probability spaces: Efficient constructions and applications," *SIAM J. Comput.*, vol. 22, no. 4, pp. 838–856, 1993.

[15] N. Alon, J. Bruck, J. Naor, M. Naor, and R. Roth, "Constructions of asymptotically good low-rate error- correcting codes through pseudo-random graphs," *IEEE Trans. Inf. Theory*, vol. 38, pp. 509–516, 1992.

[16] N. Alon, O. Goldreich, J. Håstad, and R. Peralta, "Simple constructions of almost k-wise independent random variables," *Random Struct. Algorithms*, vol. 3, no. 3, pp. 289–304, 1992.

[17] P. Dickinson and A. Nayak, "Approximate randomization of quantum states with fewer bits of key, quantum computing back action, IIT kanpur," in *Proc. AIP Conf.*, India, Mar. 6–12, 2006.

[18] C. A. Fuchs and J. van de Graaf, "Cryptographic distinguishability measures for quantum-mechanical states," *IEEE Trans. Inf. Theory*, vol. 45, pp. 1216–1227, May 1999.

[19] A. Uhlmann, "The transition probability in the state space of a *-algebra," *Rep. Math. Phys.*, vol. 9, p. 273, 1976.

Simon Pierre Desrosiers received the Ph.D. degree from McGill University, Montréal, QC, Canada, in 2009.

His main research interests include classical and quantum cryptography.

Frédéric Dupuis was pursuing the Ph.D. degree with the Computer Science Department, Université de Montréal, Montréal, QC, Canada, while this work was produced.

He is now a Postdoctoral Researcher with the Institute for Theoretical Physics, ETH Zurich, Switzerland. His main research interests are quantum information theory and quantum cryptography.