Quantum entropic security

Simon Pierre Desrosiers

School of Computer Science
McGill University, Montréal

February 2009

A thesis submitted to the Faculty of Graduate Studies and Research in partial fulfilment of the requirements of the degree of Ph.D.

Abstract

We present full generalizations of entropic security and entropic indistinguishability, notions introduced by Russell and Wang and then Dodis and Smith, to the quantum world where no assumption other than a limit on the knowledge of the adversary is made. This limit is quantified using the quantum conditional min-entropy as introduced by Renner. In this fully generalized model, we allow any kind of entanglement or correlation between the Sender and the Eavesdropper.

A proof of equivalence between the two security definitions is presented. This proof of equivalence is much simpler and more powerful than what was previously done and is by itself a worthy contribution. We also provide proofs of security for two different ciphers in this model. These ciphers generalize existing schemes for approximate quantum encryption to the entropic security model. The key length requirement of these two schemes is exactly the same as their classical counterparts for separable states. It is also, as far as we know, the first time that one can prove security for encryption schemes while allowing entanglement with the adversary and yet not requiring perfect security.

Résumé

Une généralisation complète des notions de sécurité entropique et d'indistinguabilité entropique, telles que définies par Russell et Wang puis par Dodis et Smith, au monde quantique est présentée. Aucune autre hypothèse qu'une borne inférieure sur l'incertitude de l'adversaire, incertitude quantifiée par la notion de min-entropie conditionelle quantique telle que définie par Renner, n'est présumée. Ce modèle permet toute forme de corrélation ou d'intrication entre l'adversaire et l'émetteur du message. Une Démonstration de l'équivalence entre ces deux notions de sécurité est présentée qui est beaucoup plus simple que ce qui était connue au-paravant. Cette nouvelle simplicité est une contribution notable. Deux chiffres sont aussi généralisés à ce nouveau modèle de sécurité et leur sécurité est démontrée. La taille de la clef requise afin d'assurer la sécurité de ces deux chiffres est exactement la même que celle requise par leur équivalent classique. Ces chiffres sont sécuritaires même en présence d'intrication entre l'adversaire et l'émetteur, ce qui est, autant que nous le sachions, une première sans requérir une sécurité parfaite.

Acknowledgement

I am specially indebted to Claude Crépeau, my friend and director who suggested to me this wonderful subject, provided his support and showed patience. Special thanks must be given to Frédéric Dupuis with whom I had the pleasure to accomplish part of this work. I also must thank Patrick Hayden and Jean-Raymond Simard for insightful feedback and Ivan Savov for proof-reading.

Contributions of Authors

Most of the work contained in this thesis is bound to appear in two papers. Most of the content of §2 will appear in a journal published by Springer, quantum information processing , see [15], of which I am the sole author. Most of the content of §3 will appear in IEEE transaction on information theory, see [16], which is joint work with Frédéric Dupuis.

Contents

List of Figures

Chapter 1

Prolegomenon

1.1 Introduction

This work will focus on the oldest and purest part of cryptography, that is encryption. What is encryption? Loosely speaking, encryption is the science of privacy. If we have two parties, a sender and a receiver, encryption is meant to keep all messages as secret as possible against most adversaries and in most conditions. The first question which normally pops up in someone's mind is: "well what do we mean by secret". This is the central question investigated in this thesis: what is the security of an encryption scheme?

Currently, the most popular and practical schemes use computational assumptions. That is, we assume that anyone who intercepts an encrypted message and who does not know the key, is limited in his abilities to retrieve the message or part of the message. By limited, what we really mean is: if the adversary were given enough resources, time and space for example, then he would be able to recover at least parts of the message. Usually, we feel secure if for powerful adversary it would take a few centuries to retrieve part of the message. Of course, this is vague, but in practice this is exactly what is done.

In general, cryptographic schemes are constructed using trap-door one way permutations: a special kind of permutation which is really easy to compute one way, but believed to be hard to invert. It is easy to encrypt the message, but really hard to retrieve the message without the key (or the trap-door). We have good reasons to believe such functions (permutations) exist. Factorization appears to be such a problem. Brilliant minds have studied this problem for thousands of years and yet, we know of no efficient algorithm that can factor systematically a given large number (this is a gross oversimplification, not every large number is hard to factor, and of course, the meaning of *large* depends on the technology available). Factorization is therefore a good candidate to construct one-way function or permutation. There exists encryption schemes that are equivalent to factorization in difficulty. If there existed an adversary that could break the system efficiently, then one could use this hypothetical adversary to factor large numbers efficiently. If there existed an algorithm that could factor large numbers efficiently, then we could use this algorithm to break the system efficiently. This is what is meant by equivalent. Using these permutations, we can construct public-key schemes. That is a scheme in which a party creates two keys, a public key and a private key. The party obviously keeps the private key secret and publishes the public-key. Anyone can then use this public-key to encrypt messages and send them to the owner of the private key, who can then decrypt the messages.

Computational cryptography is nice in that the key length is independent of the message length. Furthermore, as long as the key has not been compromised, one can reuse the key again and again. But this is only valid in the world in which we live right now, that is a world where no quantum computer exists. No week goes by lately without new discoveries bringing us closer to having real quantum computers[1]. Scientists all around the world are working hard to instantiate that crazy theorist dream that is a quantum computer. And the day that happens, most of the classical

[1] A query on slashdot would return many examples: http://slashdot.org/search.pl?query=quantum

cryptography on which we rely today will suddenly become useless.

Even though quantum computers do not exist yet, computer scientists have been busy discovering their properties. It all began officially with the publication of a protocol by Bennett and Brassard in 1984 [8]. This protocol, called *Quantum Key Distribution*, or QKD, is a protocol that allows two parties, usually called Alice and Bob, to start from a small private key, and, using public conversation over a quantum channel, to expand this small key into a larger one with no limit on its final size (of course, the final size is dictated by the amount of conversation exchanged between the two parties). Furthermore, one can prove, albeit it took twenty years to do it convincingly [37], that if an adversary is trying to temper with this protocol, either Alice and Bob abort the protocol (which happens only if the adversary disturbed the communication more than a certain predefined threshold) or they finish the protocol and the resulting key they have is with overwhelming confidence perfectly secure (the adversary knows nothing about it). This is a task which classically cannot be done. It did not take too long before this protocol was proven feasible in the laboratory.

A second great boost came to the field when in 1994 Peter Shor presented an algorithm, [41] that would allow a quantum computer, if it existed, to factor large numbers efficiently. In the same paper, Shor also presented an algorithm that could compute the discrete logarithm on a quantum computer. This was a major achievement, but, at the same time, a major blow to modern cryptography. If one could construct such a machine, then most public-key protocols used today could be broken.

Of course private-key schemes like AES do not rely on those specific computational assumptions, but, then again, one does not know how to construct public-key cryptography with them and, very often, their security is left open. Other public-key schemes like the one based on coding theory from McEliece [34] are not yet affected by quantum computers. But their security assumptions are much younger than the factoring assumption. How much can we trust them? How long before someone finds a way to brake them using quantum computers?

Of course, one can choose to render quantum computers useless by requiring perfect security. Perfect security is defined using information theory as developed by Shannon in the forties [40]. Information is defined as a difference of two uncertainties. How uncertain is the adversary on the message sent before seeing the cipher-text and after seeing the cipher-text. If this difference is zero for all messages, then we say that the adversary has learned nothing and thus that the encryption scheme is perfectly secure. It has been known how to achieve perfect security since the forties (even earlier than that, but no proof of security was known [43]).

Perfect security sounds good but it has huge requirements in key size that renders it less practically appealing . Not only is it a symmetric scheme, that is both parties have to know the secret key before communicating —they must have met and exchanged it—, but the length of the key must be as large as the message itself. For a gigabyte of data, one needs to have previously exchanged in secret at least a gigabyte of key! This is the price of *perfectness*. But it gets worse, this is for classical messages. For quantum messages, the key has to be twice as long. One *qubit* (quantum bit) requires two classical bits of key to be encrypted [3].

For quantum messages, a relaxation on the perfect security criterion can be made in order to cut the key length. That is, if we require that the encryption scheme cannot be distinguished by any adversary for any *non-entangled* messages from the perfect scheme, then the key length can be reduced to roughly n bits of key for n qubits. This relaxation is pointless classically, the key length would be reduced by an insignificant amount (less than one bit).

This last relaxation has to work for all non-entangled messages. But what if we where to restrict what messages can be sent? What if the adversary was highly uncertain on which message is to be sent? That is, lots of messages can be sent and the probability that any given message is sent is never too large. Then, there is another relaxation that one can do. It is called entropic security. It was introduced in 2002 in the classical setting by Russell and Wang, see [39], and further studied by Dodis and Smith [4] two years later. It simply says that if the adversary has a large uncertainty of a special kind, that is *min-entropy*, then the encryption scheme is highly secure. Security is defined by saying that whatever the adversary could compute from seeing the cipher-text, then he could have computed it without seeing the cipher-text. Seeing the cipher-text does not help the adversary. This definition of security is reminiscent of semantic security. It is in fact very similar, the main difference is that the encryption scheme has to be secure against all adversaries, however powerful. Encryption schemes exist that achieve this definition and they are very simple to implement. The key length can be reduced by the amount of uncertainty by which the adversary is afflicted.

This definition is only valid for classical messages and adversaries that have no access to side-channels. A side-channel could be an electro-magnetic reading of the computer screen the sender is using to transmit the message for example. Coupled with the cipher-text, this reading could unlock many possibilities for the adversary. Although perfectly secure schemes remain secure, the definition of entropic security completely breaks down in such a case. There are reasonable scenarios where, with very low probability, the adversary could learn some information on the side-channel that would allow him to easily contradict the security assumption (a phenomenon akin to that of locking or unlocking, see [28, 33]). But most sampling of the side-channel would not influence the ability of the adversary to break the scheme. In such a case, it seems reasonable the scheme is mostly secure, but how can one prove this? In the past, in the absence of correct security definition, one would simply have chosen the worst case scenario and have made sure the encryption protected the user for that specific case even though this was an overkill in most cases. There was simply no security proofs to do otherwise.

This is the problem we intent to solve in this thesis. We shall propose security definitions and encryption schemes achieving them that are resilient to side-channel attacks of any type, including entanglement of the adversary and the message sent. As long as one can bound the uncertainty of the adversary (this uncertainty has to be carefully defined) then we can guarantee security. Of course bounding this uncertainty in practice is a problem in itself which is out of the scope of this thesis but that would deserve more attention.

More specifically, we build these definitions in two steps. In a first step, we allow the sender to send quantum messages which are not entangled with the adversary. We model the adversary in the most general way allowed by quantum physics, that is a POVM. We make two restrictions on the adversary: he has a certain amount of uncertainty on the message sent and he is not correlated (he does not have access to any side-channel). In the first model, §2, we propose generalizations of classical entropic security definitions and two ciphers that achieve them. These ciphers do not use more key than their classical entropically-secure counterparts. We also introduce new proof techniques that greatly simplify proving the equivalence between two different security definitions and that also work classically. This chapter is an important intellectual step toward full generalization of the security definitions to all side-channels.

In §3 we fully generalize the simpler model of chapter §2. We need to redefine uncertainty, for that purpose, we use a definition of entropy introduced by Renner [37] to help prove that the BB84 protocol is indeed secure. This definition allows us to correctly quantify the uncertainty for any type of correlation between the adversary and the sender: that is any kind of side-channel including entanglement. From this, we can rebuild a structure of relations between the security definitions similar to §2 but in this more general model. We generalize all security definitions and prove equivalence between them and also prove that two simple (the same as in §2) encryption schemes can in fact achieve these definitions whilst reducing the key length compared to perfect security.

Chapter §3 bridges the gap between perfect security and approximate-encryption which are the two different quantum information theoretic definitions that existed before. The first one requires $2n$ bits of key to encrypt any quantum state, and security is achived even if the eavesdropper is *entangled* or correlated with the state.

The latter definition can achieve encryption of any *separable* (unentangled) state using roughly n bits of key for n qubits. Equipped with the definitions and technique presented in this thesis, we can now smoothly go from n to $2n$ bits of key depending on the uncertainty of the adversary.

1.2 Historical perspective and contributions

Let us start by defining what an **encryption scheme** (or **cipher**) is. We will be interested only in quantum schemes (classical schemes will be a natural restriction of everything done here). Hence the messages the sender emits are quantum by nature, therefore we shall call a generic message ρ, where ρ is a density operator[2]. We shall also use m and M for classical messages and classical random variables representing the message distribution.

Definition 1 (Encryption scheme) *An encryption scheme $\mathcal{E}$ is a set of super-operators*[3] $\{\mathcal{E}_k\}_k$ *indexed by a uniformly distributed key* $k \in \{1, \ldots, |K|\} = K$ *such that for each* k*, there exists an inverting super-operator* $\mathcal{D}_k$ *such that for all states* ρ *we have*

$$\mathcal{D}_k(\mathcal{E}_k(\rho)) = \rho. \tag{1.1}$$

The set K is called the key space. In classical cryptography, we would replace the set of super-operators by a set of channels or algorithms. This definition obviously applies to most encryption scheme everyone knows. Still, it says nothing about security, secrecy or privacy! So how could we define security? One solution is to ask for perfect security. This is what Shannon did with information theoretic perfect security [40]. This security definition simply requires that the adversary acquires no information whatsoever on the message from the encrypted version of that message, or:

[2] See §1.3 for formal definition of most concepts of this section.

[3] See [14] and [35] for characterization of admissible operators.

Definition 2 (Perfect classical security) *Let M be a random variable describing the eves-dropper's view, then a cipher is perfectly secure if for all such variables M we have*

$$I(M:\mathcal{E}(M)) \triangleq H(M) - H(M|\mathcal{E}(M)) = 0. \tag{1.2}$$

Here information is defined as a difference of uncertainties, the uncertainty on the message before seeing the encrypted text and after seeing the encrypted text and of course, for this to make sense, the messages are classical. This definition does not make any assumption, it does not depend on the computing power, time or even information; if the adversary knows half the message before seeing its encrypted version, then after seeing the encrypted version, the adversary still only knows the same half and nothing more. There is a caveat: in order to achieve this security definition the key size required by a cipher is, in general, as large as the message, or

$$H(K) \geqslant H(M). \tag{1.3}$$

If one wants to send quantum messages, then the situation is even worse, perfect secrecy requires the key length to be twice as large as the message length [3]. If one relaxes condition (1.2) in the classical setting (i.e classical messages and classical encryption schemes) so that $I(M:\mathcal{E}(M)) < \epsilon$, then one can only reduce the key size by ϵ bit. What might seem surprising is that if one does a similar relaxation for quantum encryption schemes applied to quantum state, then one can cut the key size almost by one-half [28].

Definition 3 (ϵ-randomizing security) *An encryption scheme $\mathcal{E}$ is ϵ-randomizing if for all states ρ we have*

$$\left\|\mathcal{E}(\rho) - \frac{\mathbb{I}}{d}\right\|_\infty \leqslant \frac{\epsilon}{d} \tag{1.4}$$

where d is the dimension of the message space to encrypt.

The $\|\sigma\|_\infty$ notation means the operator distance: it is the largest eigenvalue of the operator σ. Definition 3 immediately implies that $\|\mathcal{E}(\rho) - \mathbb{I}/d\|_1 \leqslant \epsilon$. This characterization is more similar to Definition 1.2 since Definition 1.2 can be restated as $\|\mathcal{E}(\rho) - \mathbb{I}/d\|_1 = 0$. In [28], it was showed that there exist schemes that achieve Definition 3 which require $n + \log n + \log(1/\epsilon^2) + 8$ bits of key. The only assumption on the adversary is that he is in a separable state with the sender (i.e. he is not entangled with the sender). Other than that, only a relaxation of the security definition is made; hence this model is still information theoretically secure. This result was later improved by Dickinson and Nayak, in [17], by a factor $\log n$. That is they showed that any random sequence of operators taken from a perfect scheme (hence they could be random Pauli operators) indexed by a key of size $n + \log\log(15/\epsilon) + \log 1/\epsilon^2 + 6$ is secure (if the trace norm is used and this with high probability).

The first efficient constructions were proposed by [4]. They used diverse constructions of δ-biased sets and families, see [1], to prove secure three different encryption schemes using the trace norm. The first scheme is length preserving (the cipher text and the message in clear have the same length) and uses $n + 2\log n + 2\log(1/\epsilon) + \mathcal{O}(1)$ bits of key. The second one is not length preserving but has smaller key requirements, that is $n + 2\log(1/\epsilon)$ bits of key. And the third scheme is a hybrid construction over *qupits*. Their result was later improved by Dickenson and Nayak, see [17], who noticed that a different construction for δ-biased set found in [1] would bring better key requirements: that is $n + 2\log(1/\epsilon) + 2$ while being a length preserving scheme. They actually reused the exact same proof as in [4].

Another traditional security definition is... not having one. Take RSA [38] for example. In this famous paper, no definition of security is used, none whatsoever. Another good example is DES [42], no real security definition is given. Hence no proof of security can be given. Of course, for RSA, the authors had the idea of a one way function (or permutation), but no real reduction is made in their original paper. Security is only addressed by saying, if one could do one of a few things, then their scheme would fail, but no one knows how to do these and they do not know how to break it; so they dare us to try.

It is only a few years after RSA that Goldwasser and Micali proposed believable, intuitive and, as far as we know, correct security definitions [23, 24] — of course the security definition depends in its details on the model of interest. In this next definition, the adversary A is modeled by an algorithm.

Definition 4 *An encryption scheme $\mathcal{E}$ is semantically secure if for every probabilistic polynomial-time algorithm A, there exists a probabilistic polynomial-time algorithm A' such that for every random variable M on messages of length n, every function f and every positive polynomial p and all sufficiently large n we have*

$$\Pr[\mathsf{A}(\mathcal{E}(m)) = f(m)] < \Pr[\mathsf{A}'(\cdot) = f(m)] + \frac{1}{p(n)}, \tag{1.5}$$

where the probabilities are taken over all coins thrown by A, A' and $\mathcal{E}$.

For a more formal definition, see §5 in [22]. This security definition in itself is a great contribution but it has one caveat. How does one prove that a given cipher $\mathcal{E}$ is semantically secure? As far as we know, no direct way of doing this is known. This is why the second great contribution of this seminal article is so important: they propose a second security definition and then show that those two definitions are in fact equivalent. This new definition has the nice property that it is easy (easier) to prove that a given encryption scheme achieves it.

Definition 5 *An encryption scheme $\mathcal{E}$ has indistinguishable encryptions if for every probabilistic polynomial-time algorithm A, every positive polynomial p, all sufficiently large n and every $x, y \in \{0,1\}^{poly(n)}$ (i.e $|x| = |y|$) we have*

$$\Big|\Pr[\mathsf{A}(\mathcal{E}(x)) = 1] - \Pr[\mathsf{A}(\mathcal{E}(y)) = 1]\Big| < \frac{1}{p(n)}, \tag{1.6}$$

where the probabilities are taken over all coins thrown by A and $\mathcal{E}$.

In this definition, the adversary really is a distinguisher between two values, or random variables ($\mathcal{E}(x)$ and $\mathcal{E}(y)$). Again see §5 in [22] for details. Using these two definitions, they were able to show that based on the existence of a one-way function or trap-door one-way permutation, one could devise semantically secure private-key or public-key encryption schemes. In particular, one can construct an encryption scheme which security is equivalent to the problem of factorization. Note that RSA can be transformed into a semantically secure encryption scheme provided that RSA is itself a one-way permutation. Maybe the nicest thing about semantic security, is that its definition can be adapted to different adversarial models: passive eavesdropping, chosen plain text attack, chosen cipher text attack and non-malleable encryption schemes. Of course, all of this was not instantly done in 1982, but still, it is a tribute to the fundamental robustness of the definition. Semantically secure encryption schemes are also called *probabilistic encryption schemes*, as Definition 1.6 requires encryption of two known messages to be indistinguishable even in a public-key scheme.

In 2002 Russell and Wang [39] introduced the notion of semantic security (which they renamed entropic security) into the information theoretic model. Of course, some assumption has to be made somewhere on the adversary abilities. They introduced an entropy assumption. That is, for a random variable M, an assumption on the min-entropy of M from the adversary's perspective. Sadly, their results are limited to predicates (and not all functions), their proofs are hard to decipher and there is no notion of indistinguishability. Still, this was a great achievement. It must be mentioned that similar concepts for hash functions had already been developed by Canetti et al. in [11, 12]. These hash function do not reveal any information on their input through their output as long as the input has sufficiently high min-entropy. Two years later, Dodis and Smith introduced in [18] the notion of entropic-indistinguishability and entropic security for all functions which we now present.

Definition 6 (Classical entropic security) *An encryption scheme $\mathcal{E}$ is said to be (t, ϵ)-entropically secure if for all random variables M such that $H_\infty(M) \geqslant t$, every adversary A, there exists an adversary A' such that for all functions f we have*

$$\Big|\Pr[\mathsf{A}(\mathcal{E}(m)) = f(m)] - \Pr[\mathsf{A}'(\cdot) = f(m)]\Big| < \epsilon, \tag{1.7}$$

where $m \in_R M$.

In this definition, $\mathsf{A}'(\cdot)$ means an adversary A' which has no input, just the a priori knowledge of the message distribution.

Definition 7 (Classical entropic indistinguishability) *An encryption scheme $\mathcal{E}$ is (t, ϵ)-entropically indistinguishable if there exists a random variable G such that for all random variables M such that $H_\infty(M) \geqslant t$ we have*

$$\|\mathcal{E}(M) - G\| \leqslant \epsilon, \tag{1.8}$$

where $\| \cdot \|$ is the variational distance or statistical distance between the two distributions.

Using these definitions, they were able to prove that certain simple schemes that were entropically-secure could significantly reduce the necessary key length compared with perfect secrecy. Instead of requiring about n bits of key to encrypt n-bit messages, they could instead use only $n - t + 2\log(1/\epsilon) + \mathcal{O}(1)$ bits of key. This model is still information theoretically secure, since, for any one that controls somewhat his message distribution, there is nothing to fear from any adversary, however powerful that adversary may be, and this with overwhelming probability.

Here is where all our contributions fit in. We propose generalizations of the definition of entropic security and entropic indistinguishability to the quantum world and prove their equivalence. We also prove that two encryption schemes are in fact entropically secure. One quantum scheme was proposed in [4] as an approximate quantum encryption scheme and the other scheme is generalization of a classically entropically secure scheme that appears in [18]. The model proposed and many proof techniques or tricks are new to this work and many such proofs are much simpler and powerful than the previous state of the art; this in itself is an important contribution. In section 2, we introduce all these concepts in a non-entangled, non-correlated model. Most results of this section have been published in [15] In section 3 we present all these concepts in a fully generalized model where the adversary can be entangled and/or correlated in any complicated fashion with the sender. By correlated, we mean that the adversary has access to a side-channel of some sort that is not necessarily incarnated by entanglement. Although all results in the general model subsume the non-correlated model, we still feel that it is more pedagogical to introduce everything in a simpler model since most of the ideas are already there. This eases comprehension of the general model with entanglement. Most results of §3 have been published in [16], which is joint work with Frédéric Dupuis.

In [18], Dodis and Smith observed that (t, ϵ)-indistinguishable schemes are in fact *extractors* which happens to be invertible. Extractors are deterministic algorithms which given n bits comming from a source of sufficiently high min-entropy and a perfect smaller key, output m almost perfectly random bits, where $m \leqslant n$. Concurrently to the work contained in this thesis, Fehr and Schaffner showed in [19] that one of the scheme contained in [4, 15] is in fact a classical extractor (classical algorithm processing classical bits) secure against non-entangled quantum adversaries (this adversary could have some quantum information on the classical input of the extractor). Although extractors are not the focus (framework) of this thesis, [16] generalizes this result to quantum procedures processing quantum inputs such that they are secure against all quantum adversaries provided sufficiently high quantum conditional min-entropy.

Quantum extractors were formally introduced byBen-Aroya and Ta-Shma in [7]. The authors proved that constructions based on Cayley graphs are quantum extractors.

The extractors are efficient when the graph is abelian. Our definition of indistinguishability in the non-correlated model is compatible with the definition of extractor proposed in [7]. The definition of indistinguishability in the fully generalized model also generalized the definition of extractor given [7]. More constructions of quantum extractors were provided later on in [27] and [26].

Finally, in 2007 Bellare, Boldyreva and O'Neill introduced the notion of *deterministic encryptions* in [6]. Deterministic encryption is a hybrid between entropic-encryption and semantic-encryption. That is, by postulating both a high min-entropy on the message space and a power limit on the adversary (the adversary is a polynomial-probabilistic time machine), then they can get deterministic encryption which hides any partial information on the message. The proofs of [6] are done in the *random oracle* model. Boldyreva, Fehr and O'Neill removed the necessity of the random oracle model in [10] by introducing an indistinguishability-based definition of deterministic security. Their proof of equivalence between their different notions of security uses techniques developed here to prove equivalence between entropic-security and entropic-indistinguishability.

1.3 Mathematical Preliminaries

A certain number of definitions were given in the last chapter which sometimes refer to objects which have not been defined yet. For quantum information theorists, they need not be defined in a separate chapter, but for more casual readers, we feel it is necessary to define these objects and their main properties, as they are numerous. Most mathematical properties of the objects described in this chapter can, of course, be found in [36]. The rest comes from [9, 13, 30, 31].

First, our main object of study are quantum states and quantum channels. We briefly discussed the latter but we still have to fix notation and meaning of the former. Let

$\mathcal{X}$ be a complex linear space. For any unit length vector $x \in \mathcal{X}$, we shall write $|x\rangle$. This notation, called braket notation and introduced by Dirac, is a shortcut for a norm one column vector, where the norm is according to the usual euclidean inner product. For the complex transpose we shall write $\langle x| = \overline{|x\rangle}^T$. The euclidean inner product is thus only $\langle x||x\rangle = \langle x, x\rangle$. Since $\mathcal{X}$ is a linear space, one can find bases for it. Let the set $\{|z_i\rangle\}_i$ be an orthonormal basis for $\mathcal{X}$. Then for any $x \in \mathcal{X}$ we can find complex coefficient a_i's such that $x = \sum_i a_i|z_i\rangle$.

Linear operators from $\mathcal{X}$ to $\mathcal{X}$ are denoted by $\mathcal{L}(\mathcal{X})$. A quantum state is simply a trace one, positive linear operator that belongs to $\mathcal{L}(\mathcal{X})$; we shall denote this set with $\mathcal{D}(\mathcal{X})$. Let $\rho \in \mathcal{D}(\mathcal{X})$. So a quantum state has three important characteristics: first it belongs to $\mathcal{L}(\mathcal{X})$; secondly, for any basis $\{|z_i\rangle\}_i$ of $\mathcal{X}$ then

$$\mathrm{Tr}\,[\rho] \triangleq \sum_i \langle z_i|\rho|z_i\rangle = 1 \tag{1.9}$$

which is also the definition of the trace operator; and thirdly, for any unit vector $|x\rangle \in \mathcal{X}$ we have that

$$\langle x|\rho|x\rangle \geqslant 0. \tag{1.10}$$

If for all $|x\rangle$ we have a greater instead of greater or equal sign, then we say the state is **positive definite**. It then has full rank and is invertible, see [30]. If the result is sometimes zero, then the rank of ρ is not maximum and thus ρ is not invertible, the operator is then said to be **positive**. Such operators are called **density operators**. Every physical system can be described by a density operator. It will thus be the basic object that we manipulate.

The spectral decomposition theorem tells us that any density operator ρ can be written this way:

$$\rho = \sum_i p_i\,|z_i\rangle\langle z_i|\,, \tag{1.11}$$

where the $|z_i\rangle$'s form an orthonormal basis of $\mathcal{X}$ and the p_i's sum up to one. The expression $|z_i\rangle\langle z_i|$ denotes the outer-product of $|z_i\rangle$ and $\langle z_i|$ which is simply a projector on $|z_i\rangle$. The $|z_i\rangle$'s are eigen-vectors of ρ and the p_i's are eigen-values of ρ. Note that any normal operator, that is an operator M such that $MM^\dagger = M^\dagger M$, has a spectral decomposition as in equation (1.11). Hermitian operators, that is $M = M^\dagger$, have real eigen-values. Projectors, $M = M^2$, have zero or one as eigen-values. Positive operators have real non-negative eigen-values, which in the case of density operators can be interpreted as probabilities.

One interacts with quantum system through **measurements**, for a good overview see §2 in [36]. In this thesis we shall use two formalisms: **POVM**'s, which stands for positive operator-valued measure, and **observables**. The first one, well described in §2.2.6 in [36], is simply a set of positive operator $\{E_m\}_m$ that produces classical output m when applied to a given state ρ. The only condition is that $\sum_m E_m = \mathbb{I}$. A POVM is used mostly when one does not care about the quantum state that results of the measurement. The probability of observing the value m when one applies a given POVM to a state ρ is simply

$$\mathrm{Tr}\left[E_m \rho\right]. \tag{1.12}$$

The POVM formalism is as general as can be, we shall therefore use it to model the adversary.

An observable is a full rank Hermitian operator, see §2 in [13]. When an observable $\mathcal{O} = \sum_m \lambda_m |\psi_m\rangle\langle\psi_m|$ is applied to state ρ the output is simply the eigen-value λ_m and this with probability $\mathrm{Tr}\left[|\psi_m\rangle\langle\psi_m|\,\rho\right]$. The residual quantum state is the associated eigen-state $|\psi_m\rangle\langle\psi_m|$ of $\mathcal{O}$. Note that the expected value for the observed value when an observable $\mathcal{O}$ is applied to a state ρ is simply given by $\mathrm{Tr}\left[\mathcal{O}\rho\right]$. Note also that the operator $\mathcal{O}\rho$ is no longer physical. We shall overload the symbol $\mathcal{O}$ for observable with the big-O notation, the meaning will always be clear from the context.

How do we describe multiple quantum states? Let us imagine two parties: a **sender** S and an **adversary** A. They each hold a quantum state in their hands. We shall denote the full quantum state describing both states at once by ρ^{SA}, where the notation is self-explicative. Of course ρ^S and ρ^A then denote the state held by the sender and the adversary respectively: that is if one looks only at the sender's state without access to the adversary's state. Now if both the sender and the adversary have two totally independent states from one another, then one can write that $\rho^{SA} = \rho^S \otimes \rho^A$, where the symbol $\otimes$ stands for **"tensor" product**.

In general for two operators $M = (m_{ij})$ and N the tensor product is defined by

$$M \otimes N = \begin{pmatrix} m_{11}N & m_{12}N & \dots & m_{1n}N \\ m_{21}N & m_{22}N & \dots & m_{2n}N \\ & & \dots & \\ m_{m1}N & m_{m2}N & \dots & m_{mn}N \end{pmatrix}. \tag{1.13}$$

The tensor product, also called Kronecker product, has intuitive properties, see §4 in [31]. It is nice with scalars $(\alpha M) \otimes N = M \otimes (\alpha N) = \alpha(M \otimes N)$. It is nice with most usual matrix operation: $(M \otimes N)^T = (M^T \otimes N^T)$, $\overline{(M \otimes N)} = (\overline{M} \otimes \overline{N})$ and $(M \otimes N)^\dagger = (M^\dagger \otimes N^\dagger)$. It is associative, $(M \otimes N) \otimes P = M \otimes (N \otimes P)$. It is also distributive on addition: $(M+N)\otimes P = M\otimes P + N \otimes P$. Most importantly, it can be mixed with the standard multiplication: $(M \otimes N)(O \otimes P) = (MO \otimes NP)$. The tensor product of Hermitian operators, unitary operators or projectors, gives respectively a Hermitian operator, unitary operator or projector. Finally if $\{|y_i\rangle^S\}_i$ is a basis for the S space and $\{|z_j\rangle^A\}_j$ is a basis for the A space, then $\{|y_i\rangle \otimes |z_j\rangle\}_{i,j}$ is a basis for the SA space.

There is a corresponding operation that let's us go from states on the SA space to states on the subspaces S and A: ρ^{SA} to ρ^S or ρ^A. This operation is called the partial trace and is denoted $\mathrm{Tr}_S\left[\rho^{SA}\right]$, which gives us a state on the A subspace only, that is ρ^A, and $\mathrm{Tr}_A\left[\rho^{SA}\right]$ gives us a state on the S subspace only, ρ^S. Take any basis for the A space, let us say $\{|z_j\rangle\}_j$ then

$$\rho^S \triangleq \mathrm{Tr}_A\left[\rho^{SA}\right] \triangleq \sum_j (\mathbb{I}^S \otimes \langle z_j|^A)\rho^{SA}(\mathbb{I}^S \otimes |z_j\rangle^A). \tag{1.14}$$

Note that it is not always true that $\rho^{SA} = \text{Tr}_A\left[\rho^{SA}\right] \otimes \text{Tr}_S\left[\rho^{SA}\right] = \rho^S \otimes \rho^A$. When this is true we say that ρ^{SA} is a tensor product state. We say that ρ^{SA} is separable if there exist probabilities $\{p_i\}_i$ and sets of states $\{\sigma_i^S\}_i$ and $\{\gamma_i^A\}_i$ such that

$$\rho^{SA} = \sum_i p_i \sigma_i^S \otimes \gamma_i^A.$$

Otherwise we say the state is entangled. We shall not discuss here the meaning of these three definitions. They are fundamental and very important, but one of the goal of the present work is to show that one can ignore them in certain contexts.

We did not mention it yet, but the trace operator is cyclic, that is $\text{Tr}\left[ABCD\right] = \text{Tr}\left[DABC\right]$. Be careful, operators do not commute, that is $\text{Tr}\left[ABCD\right] \neq \text{Tr}\left[ACBD\right]$, they rotate. As Lemma 13 shows, we can generalize this to work on part of the space, that is $\text{Tr}\left[AB \otimes CD\right] = \text{Tr}\left[BA \otimes CD\right]$.

The notion of distance between two operators is another very important concept that will be used. We will start by defining the norm of an operator. We shall call a function $\|\cdot\| : \mathcal{L} \longrightarrow \mathbb{R}$ a norm if it satisfies the following properties for all M and $N \in \mathcal{L}$:

1. $\|M\| \geqslant 0$,
2. $\|M\| = 0$ if and only if $M = 0$,
3. $\|cM\| = c\|M\|$ for all complex scalars c,
4. $\|M + N\| \leqslant \|M\| + \|N\|$,
5. $\|MN\| \leqslant \|M\|\|N\|$.

We shall use one norm throughout this work: the trace norm. For any normal operator M, the trace norm $\|M\|_{tr}$ is simply the sum of the eigen-values of the absolute value of M. More mathematically, $\|M\|_{tr} \triangleq \text{Tr}\left[|M|\right]$, where $|M| \triangleq \sqrt{MM^\dagger}$. Thus, if

$M = \sum_i \lambda_i \,|i\rangle\langle i|$, then $\|M\|_{tr} = \sum_i \sqrt{\lambda_i \overline{\lambda_i}}$. Using this notation we can define our distance between two operators M and N to be the trace norm of their difference, or $D(M, N) \triangleq \|M - N\|_{tr}$. We thus get a few properties for free: $D(M, N)$ is never negative, $D(M, N)$ is zero if and only if $M = N$ and $D(M, N)$ obeys the triangle inequality. Most of the time, we shall abbreviate $\|\cdot\|_{tr}$ by $\|\cdot\|$ since we really use only one norm. Sometimes, we could also write $\|\cdot\|_1$ as it is also called the L_1 norm in literature.

For any two states ρ and σ, if their distance $D(\rho, \sigma)$ is equal to δ, then the best POVM, or algorithm, that could distinguish between the two can do so with probability at most $1/2 + \delta/4$. That is if this distinguisher realized by the best POVM possible is given ρ with probability one half and is given σ with probability one half, then the probability that the POVM guesses correctly which state it received is simply $1/2 + \delta/4$, see [36, 29] for details.

Chapter 2

Uncorrelated Cryptography

In this section, we shall discuss security definitions and ciphers in a model where the adversary is neither correlated nor entangled with the sender.

We are interested in the following scenario. The sender chooses a message from a known message space and encrypts that message. We want that whenever an adversary intercepts an encrypted message it cannot predict any function on the message. More formally, let $\rho = \sum_j \gamma_j |z_j\rangle\langle z_j|$ be a mixed state. An **interpretation** of ρ is an ensemble $\{(p_i, \sigma_i)\}_i$ such that $\rho = \sum_i p_i \sigma_i$; we say σ_i is **compatible** with ρ. From the adversary's point of view, the sender chooses (receives) a message σ_i with probability p_i and send an encrypted version to the receiver. This is the eavesdropper's view of the message space — *i*.e. the a priori knowledge of the adversary is given by the ensemble $\{(p_i, \sigma_i)\}_i$, which consists of all the possible messages (by which we mean valid density operators, or physically possible messages) with non-zero probability along with their probability. We want that whenever the sender chooses a message σ_i and encrypts it using a cipher $\mathcal{E}$, then no eavesdropper which intercepts $\mathcal{E}(\sigma_i)$ can guess any function of σ_i. We will require this property to hold for all ρ with sufficiently high min-entropy.

$$\begin{tikzcd} \boxed{\rho = \sum_i p_i \sigma_i} \arrow[r, "\sigma_i"] & \mathsf{S} \arrow[r, "\mathcal{E}(\sigma_i)"] & \mathsf{A} \arrow[r] & f(\sigma_i) \end{tikzcd}$$

Figure 2.1: Uncorrelated Model

Definition 8 (Quantum min-Entropy) *For a state ρ which has spectral decomposition $\sum_j \gamma_j |z_j\rangle\langle z_j|$, the quantum min-entropy is defined by $-\log \max_j \gamma_j$ and is written $H_\infty(\rho)$*[1].

One can see a quantum state $\gamma = \sum_j p_j \, |z_j\rangle\langle z_j|$ as a classical probability distribution if one measures it in the $\{|z_j\rangle\langle z_j|\}_j$ basis. Then, $H_\infty(\rho)$ is simply the negative binary logarithm of the event with maximum probability; the one on which one would bet if one had to guess the output of the measurement.

Definition 9 (Entropic Security) *An encryption system $\mathcal{E}$ is (t, ε)-entropically secure if for all states ρ such that $H_\infty(\rho) \geqslant t$, all interpretations $\{(p_i, \sigma_i)\}_i$ and every adversary A, there exists an adversary A' such that for every function f, we have*

$$\left| \Pr_i[\mathsf{A}(\mathcal{E}(\sigma_i)) = f(\sigma_i)] - \Pr_i[\mathsf{A}'(\cdot) = f(\sigma_i)] \right| \leqslant \varepsilon. \tag{2.1}$$

Explanations are in order. First, in this equation, only one state is physical, that is, $\mathcal{E}(\sigma_i)$. For this equation to be meaningful, all other states are not considered to be physical but purely mathematical. By this we mean that the σ_i's are considered to be strings of bits that can be interpreted (parsed) as density operators. This is reasonable since A' never gets his hands on any ciphers, exactly as in the classical indistinguishability security definition, see [24, 22]. Hence, $\{(p_i, \sigma_i)\}_i$ is the a priori knowledge of A and A' on the message space from which the sender samples. We therefore naturally consider that the output of $f(\sigma_i)$ is simply a string of bits.[2] Furthermore we do not impose any restriction on f. In particular, we do not require that

[1] All logarithms throughout this work are taken base 2.

[2] Note that instead of considering functions on strings of bits, one could consider that the function f acts on the indices i of the σ_i and get an equivalent framework.

f be a physical process, hence f is not required to be linear or to be a function on operators ($g(\rho) = \sum_i g(\gamma_j) |z_j\rangle\langle z_j|$). We are not interested in a quantum output for two reasons. First, if such an output were useful to some post-processing that would help in predicting the function f, then any such post-processing could be included in the original POVM. Second, it is already known that entropic security does not compose very well, see [18], since we are not interested in any more complicated model like universal composability, then this is of no consequence.

In this model, the goal of A is to predict the output of the function f on the string of bits that represents the state σ_i, which is unknown to A, by only analyzing $\mathcal{E}(\sigma_i)$ which is a physical state — no restriction is put on A, we only require it to be a physical process, *i*.e a POVM. The adversary A' does not get this chance, he must predict the same function f on the same bit string but having access to nothing else than the message interpretation $\{(p_i, \sigma_i)\}_i$. The obvious best strategy for A' is to bet on the most probable output for f, since all other outputs have a smaller chance of occurring. In this case, by definition $\mathrm{Pr}_i[\mathsf{A}'(\cdot) \text{ is right}] = \mathrm{Max}_f \triangleq \max_z \mathrm{Pr}_i[f(\sigma_i) = z]$ where $Z = \{z\}$ is the set of possible outputs for the interpretation $\{(p_i, \sigma_i)\}_i$. Note that we assume A and A' know the correct interpretation which is considered to be the message space. Quantum entropic security states that if A can predict the function f with a given probability, then this probability can be matched by A' up to ϵ, equivalently $\mathrm{Pr}_i[\mathsf{A}(\mathcal{E}(\sigma_i)) = f(\sigma_i)] \leqslant \mathrm{Max}_f + \epsilon$. Of course, the definition does not specify that A' should be the best adversary possible, but, usually, one wants to do better with the cipher text than without the cipher text, hence it is a natural comparison.

The intuition behind this choice of model comes from quantum state tomography. Quantum state tomography, QST, is a procedure which takes multiple copies of a state γ and produces a string of bits which can be parsed as the complex coefficient of the matrix that represents the density operator of a single state γ. Once we know that matrix, we can predict everything about γ (statistically speaking). For the sake of arguing, let us dream up the procedure of instant quantum state tomography, IQST, an impossible task that takes one copy of a given state γ and outputs all the coefficients of the density operator in a single string. We think of the function f as a function that is applied to the output of IQST. Or that $\mathsf{A}(\mathcal{E}(\sigma_i))$ tries to guess the value $f(IQST(\sigma_i))$.

We shall introduce a strong version of Definition 9 that will use f only as a pretext[3]. This should bring comfort to those uneasy with definition 9 and its interpretation.

Definition 10 (Strong Entropic Security) *An encryption system $\mathcal{E}$ is said to be (t, ε)-strongly entropically secure if for all states ρ such that $H_\infty(\rho) \geqslant t$, all interpretations $\{(p_j, \sigma_j)\}_j$ and every adversary A we have that for all functions f*

$$\left| \Pr_i[\mathsf{A}(\mathcal{E}(\sigma_i)) = f(\sigma_i)] - \Pr_i[\mathsf{A}(\mathcal{E}(\rho)) = f(\sigma_i)] \right| \leqslant \varepsilon. \tag{2.2}$$

The only difference with Definition 9 is that we have restricted the notion of A': this adversary is now the same as A but it receives a forged encryption of ρ, the mixture of all messages. Basically, Equation (2.2) means that whatever A can compute from $\mathcal{E}(\sigma_i)$, the real message, with probability up to ϵ he could have computed it using only an oracle serving an encryption of ρ which is totally independent of σ_i. This strategy is clearly worse than the optimal one, since

$$\Pr_i[\mathsf{A}(\mathcal{E}(\sigma_i)) = f(\sigma_i)] \leqslant \Pr_i[\mathsf{A}(\mathcal{E}(\rho)) = f(\sigma_i)] + \epsilon \leqslant \mathrm{Max}_f + \epsilon, \tag{2.3}$$

because no strategy can do better than Max_f without seeing the cipher text. This is why we say that this last definition is stronger than entropic security. We argued that definition 9 really compares A's ability to predict f with that of the best adversary that has not seen the cipher text, call it A_{max}. Of course, since A_{max} is the best adversary, then if we call A with a dummy state, here $\mathcal{E}(\rho)$ instead of $\mathcal{E}(\sigma_i)$, then $\mathsf{A}(\mathcal{E}(\rho))$ cannot be better than A_{max} at guessing $f(i)$. Yet the encryption scheme is

[3] This becomes apparent in the proof of equivalence.

secure and $\mathsf{A}(\mathcal{E}(\sigma_i))$ is not much better at predicting $f(i)$ than $\mathsf{A}(\mathcal{E}(\rho))$. Then, it must be that definition 10 requires an encryption scheme that is certainly no weaker than the encryption scheme achieving Definition 9. Hence the use of the term "stronger". Also, as Lemma 2 shows, strong entropic security implies entropic security.

As in [24] and [18], we can introduce a notion of indistinguishability and then show that indistinguishability and entropic security are equivalent.

Definition 11 (Entropic Indistinguishability) *A cipher $\mathcal{E}$ is said to be (t, ε)-indistinguishable if there exists a state Ω such that for all states ρ for which $H_\infty(\rho) \geqslant t$ we have*

$$\|\mathcal{E}(\rho) - \Omega\|_1 \leqslant \varepsilon. \tag{2.4}$$

For most practical ciphers, Ω will simply be the perfectly mixed state $\mathbb{I}/d$. It is also easy to see, using the triangle inequality, that Definition 11 implies this next one:

Definition 12 (Weak Entropic Indistinguishability) *An encryption scheme $\mathcal{E}$ is said to be weakly (t, ϵ)-indistinguishable if for all operators ρ and ρ', such that $H_\infty(\rho) \geqslant t$ and $H_\infty(\rho') \geqslant t$, we have*

$$\|\mathcal{E}(\rho) - \mathcal{E}(\rho')\|_1 \leqslant 2\epsilon. \tag{2.5}$$

One final comment on all these definitions. Contrary to the classical case, it is not the probability of each message in the interpretation which is important, but the largest eigen-value of the mixture. In fact, the interpretation could have only two messages, both happening with probability one-half, and yet, one could still get very high security provided the mixture of both has small eigen-values. This is not a quantum phenomenon but simply the consequence of generalizing the messages to distributions. There might be classical situations where having to distinguish between distributions, or trying to guess functions on distributions would be reasonable, then surely the same effect would manifest itself.

As is traditionally the case in semantic security, Definition 9 carries the meaning of what is considered a secure encryption scheme. Definition 11 will allow us to prove that a given scheme is secure and Definition 10 will let us show more easily that these two definitions are equivalent for all functions and not just for predicates.

2.1 Equivalence of the definitions

In this section we show equivalence between all 4 definitions of security that were given in the preceding section: that is entropic security (ES), strong-entropic security (SES), Indistinguishability (I) and Weak-Indistinguishability (WI).

Figure 2.2 shows the graph of implications that we shall prove. An arrow signifies implication. For example, strong entropic security implies entropic security as was argued in the previous section. The fact that indistinguishability implies weak indistinguishability was also already argued. The graph does not show how the ϵ and t parameters in the proofs vary.

Lemma 1 *Weak (t, ϵ)-indistinguishability implies $(t, 2\epsilon)$-indistinguishability.*

Proof:
Just fix Ω to be $\mathcal{E}(\frac{\mathbb{I}}{d})$. The state $\frac{\mathbb{I}}{d}$ has maximum min entropy, that is $n = \log d$, hence all state $\mathcal{E}(\rho)$, where $H_\infty(\rho)$ is sufficiently high, must be 2ϵ close to this state. QED

Lemma 2 *Strong (t, ε)-entropic security implies (t, ε)-entropic security.*

Proof:
In Strong entropic security not only does there exists an adversary, but we know how to build it. This immediately implies that one exists. QED

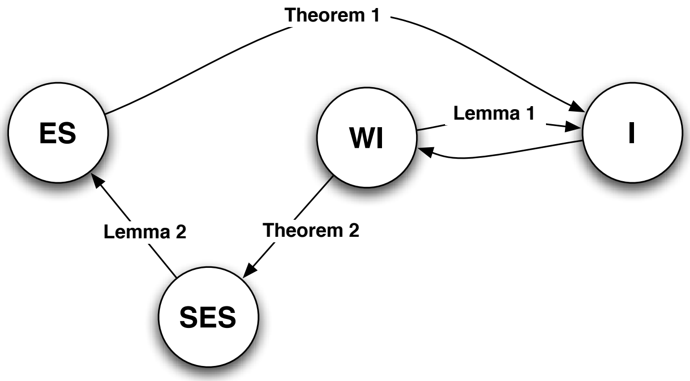

Figure 2.2: Graph of implications

We shall now prove a restricted version that entropic security implies indistinguishability: that is we shall prove it only for ciphers for which the perfectly mixed state is an eigen-state. We shall prove the general case in the next chapter. Although this proof is less general, it is a stronger result (parameters wise) and since practical schemes all have this property, they get better guaranty from this proof than the general proof presented in chapter §3.

Theorem 1 *If $t \leq n-1$, then if $\mathcal{E}(\mathbb{I}/d) = \mathbb{I}/d$ we have that (t, ϵ)-entropic security implies $(t-1, 4\epsilon)$-indistinguishability.*

Proof:

We are translating, and improving, for this lemma the proof from Dodis and Smith to the quantum setting. The last part, for non-orthonormal states, is new to this work and can be applied to the classical proof. It is well known that a classical t-source[4] can be decomposed into a convex combination of flat sources over 2^t points[5]. Moreover the two are linked in an easy way: if X is a classical t-source, and Y is an equiprobable

[4] A t-source is a random variable with min-entropy no less than t.

[5] A flat t-source, is a uniform distribution over 2^t points.

distribution on the first 2^t points (the order is arbitrary), then there exists $\{P_i\}_i$ such that $X = \sum_i p_i P_i Y$, where $\sum_i p_i = 1$ and the P_i's are permutation matrices.

It is less known, yet also true, that we can say the same thing about density operators. Let ρ be a state such that $H_\infty(\rho) \geqslant t$ and let σ be a perfectly mixed state with $H_\infty(\sigma) = H(\sigma) = t$ (*i*.e the support of σ has size 2^t). Then we can decompose ρ this way

$$\rho = \sum_i p_i U_i \sigma U_i^\dagger, \tag{2.6}$$

where $\sum_i p_i = 1$ and the U_i's are unitary operators. It must also be said that if ρ and σ commute, then the U_i's are just permutation matrices.[6]

These observations will allow us to prove the lemma for flat $t-1$ sources only. Indeed, $\mathcal{E}$ can not decrease entropy, so $H_\infty(\mathcal{E}(\rho)) \geqslant t$ and $\mathbb{I}/d$ is of course a t-source. So we can write $\rho = \sum_i p_i X_i$ where $X_i = U_i \sigma U_i^\dagger$, the U_i's are permutation matrices and σ is a flat $(t-1)$-source which we choose in the eigen-basis of ρ. Similarly, we can write $\mathbb{I}/d = \sum_j q_j Y_j$, where $Y_j = V_j \sigma V_j^\dagger$ (the reader should keep in mind that we can diagonalize $\mathbb{I}/d$ in the basis of our choice, so we choose the eigen-basis of ρ, hence ρ, $\mathbb{I}/d$ and σ all commute with one another). We know that $\mathcal{E}(\mathbb{I}/d) = \mathbb{I}/d$.

So $\|\mathcal{E}(\rho) - \mathcal{E}(\mathbb{I}/d)\| = \left\|\mathcal{E}(\sum_i p_i X_i) - \mathcal{E}(\sum_j q_j Y_j)\right\|$. Since $\sum_i p_i = \sum_j q_j = 1$, we can write this:

$$\left\|\mathcal{E}((\sum_j q_j)\sum_i p_i X_i) - \mathcal{E}((\sum_i p_i)\sum_j q_j Y_j)\right\|$$

which can be simplified to

$$\left\|\mathcal{E}(\sum_{i,j} p_i q_j X_i) - \mathcal{E}(\sum_{i,j} p_i q_j Y_j)\right\|.$$

Since $\mathcal{E}$ is a linear operator we can rewrite everything this way:

$$\left\|\sum_{i,j} p_i q_j \mathcal{E}(X_i) - \sum_{i,j} p_i q_j \mathcal{E}(Y_j)\right\|,$$

[6] For proofs of all these statements, read the section on majorization theory in [36]: §12.5.1.

which we can simplify to $\left\|\sum_{i,j} p_i q_j (\mathcal{E}(X_i) - \mathcal{E}(Y_j))\right\|$. Using the triangle inequality, we can conclude that:

$$\|\mathcal{E}(\rho) - \mathcal{E}(\mathbb{I}/d)\| \leqslant \sum_{i,j} p_i q_j \left\|\mathcal{E}(X_i) - \mathcal{E}(Y_j)\right\|. \tag{2.7}$$

This equation tells us that if every term $\|\mathcal{E}(X_i) - \mathcal{E}(Y_j)\|$ is less than 4ϵ, then Equation (2.7) is bounded by 4ϵ.

Fix any i and j and let W_0 be X_i, where $\rho = \sum_i p_i X_i$, and let W_1 be Y_j. Assume for now that they have orthonormal support. Consider the operator $Z = \frac{1}{2}W_0 + \frac{1}{2}W_1$: an equal mixture of the 2 given operators. By construction, $H_\infty(Z) = t$. Let g be the predicate that maps W_b to b; it is not necessary to define the value of g for any other state. Any adversary, A, that can predict g given $\mathcal{E}(W_b)$, for $b \in_R \{0,1\}$, is therefore a distinguisher between $\mathcal{E}(W_0)$ and $\mathcal{E}(W_1)$.

It is common knowledge (see [36, 29]) that, at best, such an adversary can distinguish between the two with probability:

$$\Pr[\mathsf{A}(\mathcal{E}(W_b)) = g(W_b) = b] = \frac{1}{2} + \frac{1}{4}\left\|\mathcal{E}(W_0) - \mathcal{E}(W_1)\right\|_1. \tag{2.8}$$

We can now invoke the entropic security, definition (2.1). Thus we can also write:

$$\Pr[\mathsf{A}(\mathcal{E}(W_b)) = g(W_b) = b] \leqslant \Pr[\mathsf{A}'(\cdot) = g(W_b) = b] + \epsilon = \frac{1}{2} + \epsilon. \tag{2.9}$$

By construction, no adversary A' can guess the correct answer with probability better than one half. Using Equations (2.8) and (2.9), we can conclude:

$$\left\|\mathcal{E}(W_0) - \mathcal{E}(W_1)\right\|_1 \leqslant 4\epsilon. \tag{2.10}$$

We are almost done. Let us now suppose that W_0 and W_1 are not orthogonal but not equal either and remember that they commute. Since they have an intersection, then $H_\infty(Z) = t - 1$. So we need to work a little more to get back decent min-entropy.

Define three mutually orthogonal projectors Π_0, Π_1 and Π_{01} such that

$$W_0 = \frac{1}{2^{t-1}}\Pi_0 + \frac{1}{2^{t-1}}\Pi_{01}$$

and

$$W_1 = \frac{1}{2^{t-1}}\Pi_1 + \frac{1}{2^{t-1}}\Pi_{01}.$$

This tells us that Π_{01} projects on the intersection of W_0 and W_1. Now, choose a fourth projector Π_+ orthogonal to the first three projectors and such that $\operatorname{rank}\Pi_{01} = \operatorname{rank}\Pi_+$ (note that since $t \leqslant n-1$, we always have enough space to choose such a projector) and define the two new states:

- $W_0' = \frac{1}{2^{t-1}}\Pi_0 + \frac{1}{2}\left(\frac{1}{2^{t-1}}\Pi_{01} + \frac{1}{2^{t-1}}\Pi_+\right)$
- $W_1' = \frac{1}{2^{t-1}}\Pi_1 + \frac{1}{2}\left(\frac{1}{2^{t-1}}\Pi_{01} + \frac{1}{2^{t-1}}\Pi_+\right)$.

Obviously, these are valid states, and we simply increased the rank of their intersection without increasing its *measure*. Let us compute the distance of their image under $\mathcal{E}$.

$$\begin{aligned}\|\mathcal{E}(W_0') - \mathcal{E}(W_1')\| &= \left\|\mathcal{E}\left(\frac{1}{2^{t-1}}\Pi_0 + \frac{1}{2^t}(\Pi_{01}+\Pi_+)\right) - \mathcal{E}\left(\frac{1}{2^{t-1}}\Pi_1 + \frac{1}{2^t}(\Pi_{01}+\Pi_+)\right)\right\| \\ &= \left\|\mathcal{E}\left(\frac{1}{2^{t-1}}(\Pi_0 - \Pi_1)\right) + \mathcal{E}\left(\frac{1}{2^t}(\Pi_{01}+\Pi_+) - \frac{1}{2^t}(\Pi_{01}+\Pi_+)\right)\right\| \\ &= \left\|\mathcal{E}\left(\frac{1}{2^{t-1}}(\Pi_0 - \Pi_1)\right)\right\|,\end{aligned}$$

whilst,

$$\begin{aligned}\|\mathcal{E}(W_0) - \mathcal{E}(W_1)\| &= \left\|\mathcal{E}\left(\frac{1}{2^{t-1}}(\Pi_0 + \Pi_{01})\right) - \mathcal{E}\left(\frac{1}{2^{t-1}}(\Pi_1 + \Pi_{01})\right)\right\| \\ &= \left\|\mathcal{E}\left(\frac{1}{2^{t-1}}(\Pi_0 - \Pi_1)\right) + \mathcal{E}\left(\frac{1}{2^{t-1}}(\Pi_{01} - \Pi_{01})\right)\right\| \\ &= \left\|\mathcal{E}\left(\frac{1}{2^{t-1}}(\Pi_0 - \Pi_1)\right)\right\|.\end{aligned}$$

We conclude that $\|\mathcal{E}(W_0') - \mathcal{E}(W_1')\| = \|\mathcal{E}(W_0) - \mathcal{E}(W_1)\|$. And now define the state

$$Z' = \frac{1}{2}W_0' + \frac{1}{2}W_1' = \frac{1}{2^t}\Pi_0 + \frac{1}{2^t}\Pi_1 + \frac{1}{2^t}\Pi_{01} + \frac{1}{2^t}\Pi_+,$$

an equal mixture of W_0' and W_1'. From the previous equation, we deduce that $H_\infty(Z') = t$. We can use this Z', define a predicate $g'(W_b') = b$ and then use the same reasoning that led us to equation (2.8) and (2.9). We conclude that

$$\|\mathcal{E}(W_0) - \mathcal{E}(W_1)\| = \|\mathcal{E}(W_0') - \mathcal{E}(W_1')\| \leqslant 4\epsilon.$$

Hence we have shown that for every state ρ such that $H_\infty(\rho) \geqslant t$,

$$\|\mathcal{E}(\rho) - \mathcal{E}(\mathbb{I}/d)\| \leqslant 4\epsilon,$$

therefore (t, ϵ)-entropic-security implies $(t-1, 4\epsilon)$-indistinguishability where Ω is equal to $\mathcal{E}(\mathbb{I}/d)$. QED

Note that this last proof can be reinterpreted to say that (t, ϵ)-entropic-security implies $(t-1, 8\epsilon)$-indistinguishability if Ω is not equal to the perfectly mixed state.

Theorem 2 *If $t \leqslant n-1$, then $(t-1, \varepsilon/4)$- weak indistinguishability implies (t, ε)-strong entropic security.*

To prove this theorem we shall use a few intermediate results.

Lemma 3 *Let A be a binary physical adversary, i.e. a POVM with two elements, that has advantage ϵ at guessing h on a state $\rho = p_0\tau_0 + p_1\tau_1$, where $h(i) = i$. Then for any sub-interpretation of τ_0 and τ_1 and a predicate g that partitions the output space as in the original interpretation, A's advantage is still ϵ at guessing $g(i)$ in the new interpretation.*

Proof:
Let us expand the lemma's statement. We know that $\rho = p_0\tau_0 + p_1\tau_1$ and that

$$|\mathrm{Pr}_k[\mathsf{A}(\tau_k) = h(k)] - \mathsf{A}'(\cdot)| = \epsilon, \tag{2.11}$$

where h is a predicate, $\mathsf{A} = \{\mathsf{A}_0, \mathsf{A}_1\}$ (A is a POVM with two elements: A_0 and A_1) and $\Pr[\mathsf{A}(\tau_k) = h(k)] = \mathrm{Tr}\left[\mathsf{A}_{h(k)}\tau_k\right]$. The statement also talks of a second interpretation $\rho = \sum_i q_i\sigma_i$ and of a second predicate g that partitions the indices i into two sets: $F_0 \triangleq \{\sigma_i | g(\sigma_i) = 0\}_i$ and $F_1 \triangleq \{\sigma_i | g(\sigma_i) = 1\}_i$, such that $p_0\tau_0 = \sum_{i\in F_0} q_i\sigma_i$ and $p_1\tau_1 = \sum_{i \in F_1} q_i\sigma_i$.

Let us compute the advantage of A over A' with this new interpretation:

$$\begin{aligned}
|\mathrm{Pr}_i[\mathsf{A}(\sigma_i) = g(i)] - \mathsf{A}'(\cdot)| &= \left|\sum_i q_i \mathrm{Pr}[\mathsf{A}(\sigma_i) = g(i)] - \mathsf{A}'(\cdot)\right| \\
&= \left|\sum_{i \in F_0} q_i \mathrm{Pr}[\mathsf{A}(\sigma_i) = 0] + \sum_{i \in F_1} q_i \mathrm{Pr}[\mathsf{A}(\sigma_i) = 1] - \mathsf{A}'(\cdot)\right| \\
&\overset{(a)}{=} \left|\sum_{i \in F_0} q_i \mathrm{Tr}\left[\mathsf{A}_0 \sigma_i\right] + \sum_{i \in F_1} q_i \mathrm{Tr}\left[\mathsf{A}_1 \sigma_i\right] - \mathsf{A}'(\cdot)\right| \\
&= \left|\mathrm{Tr}\left[\mathsf{A}_0 \left(\sum_{i \in F_0} q_i \sigma_i\right)\right] + \mathrm{Tr}\left[\mathsf{A}_1 \left(\sum_{i \in F_1} q_i \sigma_i\right)\right] - \mathsf{A}'(\cdot)\right| \\
&= \left|\mathrm{Tr}\left[\mathsf{A}_0 p_0 \tau_0\right] + \mathrm{Tr}\left[\mathsf{A}_1 p_1 \tau_1\right] - \mathsf{A}'(\cdot)\right| \\
&= \left|p_0 \mathrm{Tr}\left[\mathsf{A}_0 \tau_0\right] + p_1 \mathrm{Tr}\left[\mathsf{A}_1 \tau_1\right] - \mathsf{A}'(\cdot)\right| \\
&= |p_0 \mathrm{Pr}[\mathsf{A}(\tau_0) = 0] + p_1 \mathrm{Pr}[\mathsf{A}(\tau_1) = 1] - \mathsf{A}'(\cdot)| \\
&= |\mathrm{Pr}_k[\mathsf{A}(\tau_k) = k] - \mathsf{A}'(\cdot)| \\
&= \epsilon,
\end{aligned}$$

where (a) follows from equation (1.12). Note that the probability that A' predicts correctly is unchanged in this new interpretation. QED

Lemma 4 *Let A be a binary physical adversary, i.e. a POVM with two elements, that has advantage ϵ at guessing h on a state $\rho = p_0\tau_0 + p_1\tau_1$, where $h(i) = i$, in the strong-entropic setting. Then for any sub-interpretation of τ_0 and τ_1 and a predicate g that partitions the output space as in the original interpretation, A's advantage is still ϵ at guessing $g(i)$ in the new interpretation.*

Proof:

We have the same context as in Lemma 3. The only difference is that we wish to show, using the following two facts: $\rho = \sum_j q_j \sigma_j = \sum_l p_l \tau_l$ and $\mathrm{Pr}_i[\mathsf{A}(\rho) = g(i)] = \mathrm{Pr}_{i,j}[\mathsf{A}(\sigma_j) = g(i)]$, that

$$\begin{aligned}
|\mathrm{Pr}_i[\mathsf{A}(\sigma_i) = g(i)] - \mathrm{Pr}_{i,j}[\mathsf{A}(\sigma_j) = g(i)]| &= |\mathrm{Pr}_k[\mathsf{A}(\tau_k) = h(k)] - \mathrm{Pr}_{k,l}[\mathsf{A}(\tau_l) = h(k)]| \\
&= \epsilon, \qquad (2.12)
\end{aligned}$$

We already know from the previous proof that

$$\mathrm{Pr}_i[\mathsf{A}(\sigma_i) = g(i)] = \mathrm{Pr}_k[\mathsf{A}(\tau_k) = h(k)] \tag{2.13}$$

So we only need the following to finish the proof :

$$\begin{aligned}
\mathrm{Pr}_{i,j}[\mathsf{A}(\sigma_j) = g(i)] &= \sum_i q_i \mathrm{Pr}_j[\mathsf{A}(\sigma_j) = g(i)] \\
&= \sum_{i \in F_0} q_i \mathrm{Pr}_j[\mathsf{A}(\sigma_j) = 0] + \sum_{i \in F_1} q_i \mathrm{Pr}_j[\mathsf{A}(\sigma_j) = 1] \\
&= \sum_{i \in F_0} q_i \sum_j q_j \mathrm{Pr}[\mathsf{A}(\sigma_j) = 0] + \sum_{i \in F_1} q_i \sum_j q_j \mathrm{Pr}[\mathsf{A}(\sigma_j) = 1] \\
&= \sum_{i \in F_0} q_i \left(\sum_{j \in F_0} q_j \mathrm{Tr}\left[\mathsf{A}_0 \sigma_j\right] + \sum_{j \in F_1} q_j \mathrm{Tr}\left[\mathsf{A}_0 \sigma_j\right] \right) \\
&\qquad + \sum_{i \in F_1} q_i \sum_j q_j \mathrm{Pr}[\mathsf{A}(\sigma_j) = 1] \\
&= \sum_{i \in F_0} q_i \left(p_0 \mathrm{Tr}\left[\mathsf{A}_0 \tau_0\right] + p_1 \mathrm{Tr}\left[\mathsf{A}_0 \tau_1\right] \right) + \sum_{i \in F_1} q_i \sum_j p_j \mathrm{Pr}[\mathsf{A}(\sigma_j) = 1] \\
&= \sum_{i \in F_0} q_i \mathrm{Pr}_l[\mathsf{A}(\tau_l) = 0] + \sum_{i \in F_1} q_i \sum_j p_j \mathrm{Pr}[\mathsf{A}(\sigma_j) = 1] \\
&= p_0 \mathrm{Pr}_l[\mathsf{A}(\tau_l) = 0] + \sum_{i \in F_1} q_i \sum_j p_j \mathrm{Pr}[\mathsf{A}(\sigma_j) = 1] \\
&= p_0 \mathrm{Pr}_l[\mathsf{A}(\tau_l) = 0] + p_1 \mathrm{Pr}_l[\mathsf{A}(\tau_l) = 1] \\
&= \mathrm{Pr}_{k,l}[\mathsf{A}(\tau_l) = k].
\end{aligned}$$

Both terms being equal, the difference must be equal. QED

Lemma 5 *An adversary* A *cannot have an advantage in the strong-entropic security setting for constant predicate and binary interpretation.*

Proof:
Without loss of generality let $h(i) = 0$. Let $\gamma_0 = \mathrm{Pr}[A(\sigma_0) = 0]$ and $\gamma_1 = \mathrm{Pr}[A(\sigma_1) = 0]$. Observe that γ_0 and γ_1 are fixed values that depend only on A and σ_0 and σ_1. Then, using the fact that $\sum_k p_k = 1$,

$$\left| \mathrm{Pr}_i[A(\sigma_i) = h(i)] - \mathrm{Pr}_{i,j}[A(\sigma_j) = h(i)] \right| = \left| \sum_k p_k \mathrm{Pr}_i[A(\sigma_i) = h(i)] - \mathrm{Pr}_{i,j}[A(\sigma_j) = h(i)] \right|$$

becomes, using the fact that $\forall i, h(i) = 0$:

$$p_0(p_0\gamma_0 + p_1\gamma_1) + p_1(p_0\gamma_0 + p_1\gamma_1) - \Big(p_0(p_0\gamma_0 + p_1\gamma_1) + p_1(p_0\gamma_0 + p_1\gamma_1)\Big),$$

which is simply zero. QED

Lemma 6 *Let ρ be a state such that $H_\infty(\rho) \geqslant t$ and let $\{(p_i, \sigma_i)\}_i$ be an interpretation of ρ. Then for every i we have that $p_i \cdot \lambda_{max_i} \leqslant 2^{-t}$, where λ_{max_i} is the largest eigenvalue of σ_i.*

Proof:

Suppose, on the contrary, that $p_i \cdot \lambda_{max_i} > 2^{-t}$. Since λ_{max_i} is an eigenvalue of σ_i, there exists a vector $|v\rangle$ such that $\langle v|\sigma_i|v\rangle = \lambda_{max_i}$. These two statements together let us conclude that $\langle v|\rho|v\rangle \geqslant p_i\langle v|\sigma_i|v\rangle > 2^{-t}$. We also know that $\rho = \sum_k \gamma_k\, |k\rangle\langle k|$, so $\langle v|\rho|v\rangle = \sum_k \gamma_k \langle v|k\rangle\langle k|v\rangle \leqslant \sum_k 2^{-t}\langle v|k\rangle\langle k|v\rangle = 2^{-t}$. Hence we conclude that $2^{-t} < \langle v|\rho|v\rangle \leqslant 2^{-t}$, which is obviously a contradiction. QED

Theorem 3 *Let ρ be a state, $\{(p_i, \sigma_i)\}_i$ be an interpretation, $\mathcal{E}$ be a cipher, f be a function and A be an adversary such that*

$$\Big|\mathrm{Pr}_i[\mathsf{A}(\mathcal{E}(\sigma_i)) = f(\sigma_i)] - \mathrm{Pr}_i[\mathsf{A}(\mathcal{E}(\rho)) = f(\sigma_i)]\Big| > \epsilon,$$

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

$$\Big|\mathrm{Pr}_i[\mathsf{B}(\mathcal{E}(\sigma_i)) = h(\sigma_i)] - \mathrm{Pr}_i[\mathsf{B}(\mathcal{E}(\rho)) = h(\sigma_i)]\Big| > \frac{\epsilon}{2}.$$

Proof:

Let our predicate be a Goldreich-Levin predicate [21], that is $h_r(x) = r \odot f(x)$, where $\odot$ denotes the scalar product of the binary vectors represented by the strings $f(x)$ and r. Let $p = \mathrm{Pr}_i[\mathsf{A}(\mathcal{E}(\sigma_i)) = f(\sigma_i)]$ and $q = \mathrm{Pr}_i[\mathsf{A}(\mathcal{E}(\rho)) = f(\sigma_i)]$. Then we know that $|p - q| \geq \epsilon$. Let us compute

$$E = \Big|\mathbb{E}_r\left[\mathrm{Pr}_i[r \odot \mathsf{A}(\mathcal{E}(\sigma_i)) = h_r(\sigma_i)] - \mathrm{Pr}_i[r \odot \mathsf{A}(\mathcal{E}(\rho)) = h_r(\sigma_i)]\right]\Big|, \qquad (2.14)$$

where the expectation is taken over all r of adequate size and uniformly distributed. We need two observations. First, when A predicts correctly, then $r \odot \mathsf{A}(\mathcal{E}(\sigma_i)) = h_r(\sigma_i)$ for every r. Second, when A does not predict correctly, the probability over all r that $r \odot \mathsf{A}(\mathcal{E}(\sigma_i)) = h_r(\sigma_i)$ is exactly one half. Hence Equation (2.14) reduces to

$$E = \left| 1 \cdot p + \frac{1}{2} \cdot (1-p) - \left(1 \cdot q + \frac{1}{2} \cdot (1-q) \right) \right| = \left| \frac{p-q}{2} \right| > \frac{\epsilon}{2}. \tag{2.15}$$

There exists at least one value r such that the following is true:

$$\Big| \mathrm{Pr}_i[r \odot \mathsf{A}(\mathcal{E}(\sigma_i)) = h_r(\sigma_i)] - \mathrm{Pr}_i[r \odot \mathsf{A}(\mathcal{E}(\rho)) = h_r(\sigma_i)] \Big| > \frac{\epsilon}{2}.$$

The lemma is proven if we define adversary B as $r \odot \mathsf{A}$ for this appropriate r.
QED

We need one last result which is Theorem 9.1 in [36].

Theorem 4 *The trace distance has the following characterization:*

$$\|\rho - \sigma\|_1 = \max_{\{E_m\}_m} \left[\sum_m \Big| \mathrm{Tr}\left[E_m(\rho - \sigma) \right] \Big| \right],$$

where the maximization is taken over all possible POVMs $\{E_m\}_m$ and E_m is a POVM element.

Proof of Theorem 2:

The proof technique used in this Theorem is, as far as we know, new to this work. Suppose that there exists an adversary B, a state ρ such that $H_\infty(\rho) \geqslant t$, an interpretation $\{(p_i, \sigma_i)\}_i$ for ρ and a function f such that

$$|\mathrm{Pr}_i\left[\mathsf{B}(\mathcal{E}(\sigma_i)) = f(\sigma_i)\right] - \mathrm{Pr}_i[\mathsf{B}(\mathcal{E}(\rho)) = f(\sigma_i)]| > \epsilon. \tag{2.16}$$

We want to show that this adversary implies that the encryption scheme $\mathcal{E}$ is not $(t-1, \epsilon/4)$-indistinguishable. From Theorem 3, we know that there exists another adversary A and a predicate h such that strong $(t, \epsilon/2)$-entropic security is violated.

Let us define two sets E_0 and E_1 this way:

- $E_0 = \{i | h(\sigma_i) = 0\}_i$
- $E_1 = \{i | h(\sigma_i) = 1\}_i$,

where by Lemma 5 we can claim that both sets are non-empty. Let $r_0 = \sum_{i \in E_0} p_i$ and $r_1 = \sum_{i \in E_1} p_i$. Let $\tau_0 = \left(\sum_{i \in E_0} p_i \sigma_i\right)/r_0$ and $\tau_1 = \left(\sum_{i \in E_1} p_i \sigma_i\right)/r_1$. Obviously, ρ is equal to $r_0\tau_0 + r_1\tau_1$ and both τ_0 and τ_1 are valid density operators. Using Lemma 4 which states that A's advantage is as large with this new interpretation of ρ as it was before, we can restate the entropic security violation in terms of the τ_i, we get

$$\left|\Pr_i\left[\mathsf{A}(\mathcal{E}(\tau_i)) = h(\tau_i)\right] - \Pr_i\left[\mathsf{A}(\mathcal{E}(\rho)) = h(\tau_i)\right]\right| > \frac{\epsilon}{2}, \tag{2.17}$$

where $h(\tau_i) = i$. The adversary A is a POVM with two elements — A_0 and A_1—, so we can rewrite equation (2.17) this way:

$$\left|\sum_{i=0,1} r_i \Big(\mathrm{Tr}\left[\mathsf{A}_i \mathcal{E}(\tau_i)\right] - \mathrm{Tr}\left[\mathsf{A}_i \mathcal{E}(\rho)\right]\Big)\right| > \frac{\epsilon}{2} \tag{2.18}$$

where $\mathrm{Tr}\left[\mathsf{A}_k \gamma\right]$ is the probability that A outputs k on input γ. In our case, there are only two possible outputs: zero and one. From the last equation, since there are only two terms in the sum, we can conclude that there exists i such that

$$\left| r_i \Big(\mathrm{Tr}\left[\mathsf{A}_i \mathcal{E}(\tau_i)\right] - \mathrm{Tr}\left[\mathsf{A}_i \mathcal{E}(\rho)\right]\Big)\right| > \frac{\epsilon}{4}. \tag{2.19}$$

Let us assume without loss of generality that i is in fact zero and let us construct the two following states (choosing i to be one, would lead to a similar argument):

- $\tau_0' \triangleq r_0\tau_0 + r_1\frac{\mathbb{I}}{d}$
- $\rho' \triangleq r_0\rho + r_1\frac{\mathbb{I}}{d}$

We claim that ρ' and τ_0' are in contradiction with $(t-1, \epsilon/4)$-weak-indistinguishability. Obviously, ρ' is a t-source since it is a convex combination of two t-sources that commute. On the other hand, the largest eigen-value of τ_0' cannot be larger than $2^{-t} + r_1 \cdot \frac{1}{d}$ (we have used Lemma 6, and the fact that we can decompose $\mathbb{I}/d$ in the same basis as the eigen basis of τ_0). Since $r_1/d \leqslant 2^{-t}$, we conclude that the largest eigen-value of τ_0' is not larger than $2^{-(t-1)}$. Hence, $H_\infty(\tau_0') \geqslant t-1$.

Let us now compute the following expression:

$$\left|\mathrm{Tr}\left[\mathsf{A}_0\mathcal{E}(\tau_0')\right] - \mathrm{Tr}\left[\mathsf{A}_0\mathcal{E}(\rho')\right]\right| = \left|\mathrm{Tr}\left[\mathsf{A}_0\Big(\mathcal{E}(\tau_0') - \mathcal{E}(\rho')\Big)\right]\right|, \tag{2.20}$$

which will give us a lower bound on the trace distance between $\mathcal{E}(\tau_0')$ and $\mathcal{E}(\rho')$ as Theorem 4 tells us, since A_0 is a fixed POVM element, we get:

$$\begin{aligned}
&\left|\mathrm{Tr}\left[\mathsf{A}_0\mathcal{E}(\tau_0')\right] - \mathrm{Tr}(\mathsf{A}_0\mathcal{E}(\rho'))\right| \\
&= \left|\mathrm{Tr}\left[\mathsf{A}_0\mathcal{E}\left(r_0\tau_0 + r_1\frac{\mathbb{I}}{d}\right)\right] - \mathrm{Tr}\left[\mathsf{A}_0\mathcal{E}\left(r_0\rho + r_1\frac{\mathbb{I}}{d}\right)\right]\right| \\
&= \left|\mathrm{Tr}\left[\mathsf{A}_0\mathcal{E}\left(r_0\tau_0\right)\right] + \mathrm{Tr}\left[\mathsf{A}_0\mathcal{E}\left(r_1\frac{\mathbb{I}}{d}\right)\right] - \mathrm{Tr}\left[\mathsf{A}_0\mathcal{E}\left(r_0\rho\right)\right] - \mathrm{Tr}\left[\mathsf{A}_0\mathcal{E}\left(r_1\frac{\mathbb{I}}{d}\right)\right]\right| \\
&= \left|r_0\Big(\mathrm{Tr}\left[\mathsf{A}_0\mathcal{E}\left(\tau_0\right)\right] - \mathrm{Tr}\left[\mathsf{A}_0\mathcal{E}\left(\rho\right)\right]\Big)\right| \\
&> \frac{\epsilon}{4},
\end{aligned}$$

where the last step comes from equation (2.19). Let us now compute the second term in the lower bound to the trace distance, that is: $\left|\mathrm{Tr}\left[\mathsf{A}_1\mathcal{E}(\tau_0')\right] - \mathrm{Tr}(\mathsf{A}_1\mathcal{E}(\rho'))\right|$.

$$\begin{aligned}
\left|\mathrm{Tr}\left[\mathsf{A}_1\mathcal{E}(\tau_0')\right] - \mathrm{Tr}(\mathsf{A}_1\mathcal{E}(\rho'))\right| &= \left|\Big(1 - \mathrm{Tr}\left[\mathsf{A}_0\mathcal{E}(\tau_0')\right]\Big) - \Big(1 - \mathrm{Tr}(\mathsf{A}_0\mathcal{E}(\rho'))\Big)\right| \\
&= \left|1 - \mathrm{Tr}\left[\mathsf{A}_0\mathcal{E}(\tau_0')\right] - 1 + \mathrm{Tr}(\mathsf{A}_0\mathcal{E}(\rho'))\right| \\
&= \left|\mathrm{Tr}\left[\mathsf{A}_0\mathcal{E}(\tau_0')\right] - \mathrm{Tr}(\mathsf{A}_0\mathcal{E}(\rho'))\right|.
\end{aligned} \tag{2.21}$$

We conclude, using Theorem 4, that

$$\|\mathcal{E}(\tau_0') - \mathcal{E}(\rho')\|_1 \geqslant \sum_{i=0,1}\left|\mathrm{Tr}\left[A_i(\tau_0' - \rho')\right]\right| > \epsilon/4 + \epsilon/4 = \epsilon/2.$$

Hence τ_0' and ρ' constitute a violation of $(t-1, \epsilon/4)$-weak-indistinguishability, which, using Lemma 1, in turns implies a violation of the $(t-1, \epsilon/2)$-indistinguishability. QED.

We have now established that entropic-indistinguishability and entropic-security are equivalent. We shall now use entropic-indistinguishability to prove that two different encryption schemes are in fact secure according to entropic security.

2.2 Ciphers

We shall use the following trick in the proof of security of both ciphers, a trick which is mentioned, with hints on how to proof it, in [4]. We do a full demonstration here for the sake of completeness.

Lemma 7 *For any density operator imbedded in a space of dimension d, if* $\mathrm{Tr}\left[\rho^2\right] \leqslant \frac{1}{d}(1+\epsilon^2)$, *then we have that* $\left\|\rho - \frac{\mathbb{I}}{d}\right\|_1 \leqslant \epsilon$.

Proof:
We shall start by proving the following fact for Hermitian operator of rank d:

$$\mathrm{Tr}\left[|\Delta|\right]^2 \leqslant d\mathrm{Tr}\left[\Delta^2\right] \tag{2.22}$$

The left hand side is equal to $\left(\sum_i |\lambda_i|\right)^2$, where $\Delta = \sum_i \lambda_i |\psi_i\rangle\langle\psi_i|$. Multiplying by one, we get: $d^2\left(\frac{1}{d}\sum_i |\lambda_i|\right)^2$. Squaring is a convex function, we can therefore apply Jensen's inequality and obtain that

$$d^2\left(\frac{1}{d}\sum_i |\lambda_i|\right)^2 \leqslant d^2\frac{\left(\sum_i |\lambda_i|^2\right)}{d}. \tag{2.23}$$

We can simplify this to: $\left(\sum_i |\lambda_i|\right)^2 \leqslant d\left(\sum_i \lambda_i^2\right) = d\mathrm{Tr}\left[\Delta^2\right]$, which is what we wanted. Let us now apply (2.22) to the Hermitian operator $\rho - \mathbb{I}/d$.

$$\begin{aligned} \mathrm{Tr}\left[\left|\rho - \frac{\mathbb{I}}{d}\right|\right]^2 &\leqslant d\mathrm{Tr}\left[\rho^2 - 2\frac{\rho}{d} + \frac{\mathbb{I}}{d^2}\right] && (2.24) \\ &= d\mathrm{Tr}\left[\rho^2\right] - 2 + 1, && (2.25) \end{aligned}$$

since ρ and $\mathbb{I}/d$ are density operators. Adding one to both sides and dividing by d we get that

$$\frac{\mathrm{Tr}\left[\left|\rho - \frac{\mathbb{I}}{d}\right|\right]^2}{d} + \frac{1}{d} \leqslant \mathrm{Tr}\left[\rho^2\right]. \qquad (2.26)$$

From the statement of the Lemma, we know that $\mathrm{Tr}\left[\rho^2\right] \leqslant \frac{1}{d}(1+\epsilon^2)$. Therefore

$$\frac{\mathrm{Tr}\left[\left|\rho - \frac{\mathbb{I}}{d}\right|\right]^2}{d} + \frac{1}{d} \leqslant \frac{1}{d}(1+\epsilon^2). \qquad (2.27)$$

Multiplying by d and subtracting 1, we get $\mathrm{Tr}\left[\left|\rho - \frac{\mathbb{I}}{d}\right|\right]^2 \leqslant \epsilon^2$ from which we conclude that $\mathrm{Tr}\left[\left|\rho - \frac{\mathbb{I}}{d}\right|\right] \leqslant \epsilon$. QED

Scheme based on δ-biased sets

Let A be random variable over $\{0,1\}^n$. The bias of A with respect to a string α is the distance from uniform of the bit $\alpha \odot A$. More formally:

$$\mathsf{bias}(A) = \Big|\Pr[\alpha \odot A = 0] - \Pr[\alpha \odot A = 1]\Big| = \mathbb{E}_A[(-1)^{\alpha\odot A}]. \qquad (2.28)$$

If E is a set of n-bit strings, $E \subseteq \{0,1\}^n$, then we call the bias of E with respect to α the bias of the uniform random variable over E with respect to α. If that bias is inferior to δ for all possible strings α, excluding the zero string, we say the set is δ-biased.

The Ambainis-Smith scheme uses a construction by Alon, Goldreich, Håstad and Peralta [2], which requires polynomial time to construct and has size $\mathcal{O}(n^2/\delta^2)$. Hence it requires $2\log(n) + 2\log(1/\delta)$ bits to index the set.

We can write any Pauli operator over a 2^n dimension space this way:

$$X^u Z^v = X^{u_1} Z^{v_1} \otimes \cdots \otimes X^{u_n} Z^{v_n},$$

where u and v are two n-bit strings. Let B be a δ-biased set over strings of length $2n$, and interpret every string in B as $a\|b$, where both a and b are n-bit strings. Then the following is an approximate quantum encryption scheme:

$$\mathcal{E}(\rho) = \frac{1}{|B|} \sum_{a\|b \in B} X^a Z^b \rho Z^b X^a. \tag{2.29}$$

It is proven in [4] that whenever this scheme uses $n + 2\log(n) + 2\log(1/\epsilon)$ bits of key to index a δ-biased set, where $\delta = \epsilon 2^{-n/2}$, then for all ρ_0

$$\left\| \mathcal{E}(\rho_0) - \frac{\mathbb{I}}{2^n} \right\|_1 \leqslant \epsilon. \tag{2.30}$$

The only remaining thing to prove is that we can cut on the key length if we use the (t, ϵ)-indistinguishability security criterion instead of the approximate encryption criterion. So let $\rho = \sum_k \gamma_k |k\rangle\langle k| = \sum_i p_i \sigma_i$, where $H_\infty(\rho) \geqslant t$. Observe that an approximate encryption scheme requires that for all σ_i

$$\left\| \mathcal{E}(\sigma_i) - \frac{\mathbb{I}}{2^n} \right\|_1 \leqslant \epsilon,$$

whilst (t, ϵ)-indistinguishability requires equation (2.30) to hold for $\rho_0 = \rho = \sum_i p_i \sigma_i$.

I the min-entropy of the adversary on the message space is high enough, higher than $2\log(n) + 2\log(1/\epsilon) + \mathcal{O}(1)$, then this scheme requires less than n bits of key for n qubits.

Theorem 5 *Let B be a δ-biased set over strings of length $2n$, and interpret every string in B as $a\|b$, where both a and b are n-bit strings. Then the following scheme*

$$\mathcal{E}(\rho) = \frac{1}{|B|} \sum_{a\|b \in B} X^a Z^b \rho Z^b X^a, \tag{2.31}$$

where the private key is used to index the elements of B, is (t, ε)-indistinguishable.

Proof:
We shall use Lemma 7. If ρ is embedded in a d-dimensional space and $\mathrm{Tr}\,[\mathcal{E}(\rho)^2] \leqslant 1/d(1+\epsilon^2)$, then $\|\mathcal{E}(\rho) - \mathbb{I}/d\|_{\mathrm{tr}} \leqslant \epsilon$, which implies the desired (t, ϵ)-indistinguishability. The next equation is already proven in [4]:

$$\mathrm{Tr}\left[\mathcal{E}(\rho)^2\right] \leqslant \frac{1}{2^n}(1 + \delta^2 2^n \mathrm{Tr}\left[\rho^2\right]). \tag{2.32}$$

Now, knowing that $H_\infty(\rho) \geqslant t$, we can evaluate $\mathrm{Tr}\,[\rho^2]$ more precisely than saying it is inferior to one. We know that $\mathrm{Tr}\,[\rho^2] = \sum_k \gamma_k^2 \leqslant \sum_k 2^{-t}\gamma_k = 2^{-t}$. We simply use it in equation (2.32) and we get:

$$\mathrm{Tr}\left[\mathcal{E}(\rho)^2\right] \leqslant \frac{1}{2^n}(1 + \underbrace{\delta^2 2^{n-t}}_{\epsilon^2}). \tag{2.33}$$

So if we pose $\epsilon^2 = \delta^2 2^{n-t}$, then by using Lemma 7 we can compute how large B needs to be for this scheme to work. We conclude that the size of the key belongs to $\log(\mathcal{O}(\frac{n^2 2^{n-t}}{\epsilon^2}))$, which is equal to $n - t + 2\log(n) + 2\log(1/\epsilon) + \mathcal{O}(1)$. QED

Scheme based on XOR-Universal functions

Definition 13 *Let $\mathsf{H}_n = \{h_i\}_{i \in I}$ be a 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*

$$\mathrm{Pr}_i[h_i(x) \oplus h_i(y) = a] = \frac{1}{2^n}.$$

Take the Field of size 2^n, $F = GF(2^n)$. Let $h_i(x)$ be ix where $i \in F$ and $x \in F$ and we use the Field operation for multiplication between the two elements. For this field, addition is simply the xor of the strings that represent the elements. Hence, $h_i(x) \oplus h_i(y) = a$ if and only if $ix + iy = a$ or if $i(x + y) = a$. And this obviously has a unique solution for every pair (x, y). Hence, the probability that this happens for

$x \neq y$ is exactly $1/2^n$, since there are 2^n different i possible. Note that this property does not depend at all on the distribution of the x and y, as long as they are not equal.

Theorem 6 *Let H_{2n} be a strongly-XOR-universal family of functions. Consider the super-operator $\mathcal{E}_k(\rho) = \frac{1}{|I|}\sum_{i \in I} |i\rangle\langle i|^{S'} \otimes X^a Z^b \rho Z^b X^a$, where S' is an ancillary system, $a\|b = h_i(k)$, $|a| = |b| = n$, $h_i \in \mathsf{H}_{2n}$ and k is the secret key selected uniformly at random from a set $K \subseteq \{0,1\}^{2n}$. Then, if $H_\infty(K) + H_\infty(\rho) \geqslant n + 2\log(1/\epsilon)$, $\mathcal{E}$ is (t,ϵ)-indistinguishable. This scheme is not length preserving since the ancillary system S' is part of the cipher text.*

Proof :

We use Lemma 7 again. If ρ is embedded in a d-dimensional space and $\mathrm{Tr}\left[\mathcal{E}(\rho)^2\right] \leqslant 1/d(1+\epsilon^2)$, then $\|\mathcal{E}(\rho) - \mathbb{I}/d\|_{\mathrm{tr}} \leqslant \epsilon$, which implies the desired (t,ϵ)-indistinguishability. Observe that $\mathcal{E}(\rho)^2 = \mathcal{E}(\rho)\mathcal{E}(\rho)$, two independent instances of $\mathcal{E}(\rho)$ which are using independent key and coins. The adversary's view can be written this way: $\rho' = \mathcal{E}(\rho) = \mathbb{E}_{k,i}[|i\rangle\langle i| \otimes X^a Z^b \rho Z^b X^a]$, where the $|i\rangle\langle i|$ are equiprobable. We are interested in the following quantity:

$$\begin{aligned}
\mathrm{Tr}\left[\mathcal{E}(\rho)^2\right] &\overset{(a)}{=} \mathrm{Tr}\left[\mathbb{E}_{k,k',i,j}[(|i\rangle\langle i| \otimes X^a Z^b \rho Z^b X^a)(|j\rangle\langle j| \otimes X^c Z^d \rho Z^d X^c)]\right] \\
&= \mathrm{Tr}\left[\mathbb{E}_{k,k',i,j}[|i\rangle\langle i|\,|j\rangle\langle j| \otimes X^a Z^b \rho Z^b X^a X^c Z^d \rho Z^d X^c]\right] \\
&\overset{(b)}{=} \frac{1}{|I|}\mathrm{Tr}\left[\mathbb{E}_{k,k',i}[|i\rangle\langle i| \otimes X^a Z^b \rho Z^b X^a X^c Z^d \rho Z^d X^c]\right] \\
&= \frac{1}{|I|}\mathrm{Tr}\left[\mathbb{E}_{k,k',i}[|i\rangle\langle i| \otimes Z^d X^c X^a Z^b \rho Z^b X^a X^c Z^d \rho]\right] \\
&= \frac{1}{|I|}\mathrm{Tr}\left[\mathbb{E}_{k,k',i}[|i\rangle\langle i| \otimes (-1)^{d\odot c}(-1)^{d\odot a} X^c X^a Z^d Z^b \rho Z^b X^a X^c Z^d \rho]\right] \\
&= \frac{1}{|I|}\mathrm{Tr}\left[\mathbb{E}_{k,k',i}[|i\rangle\langle i| \otimes ((-1)^{d\odot c})^2((-1)^{d\odot a})^2 X^c X^a Z^d Z^b \rho Z^b Z^d X^a X^c \rho]\right] \\
&\overset{(c)}{=} \frac{1}{|I|}\mathrm{Tr}\left[\mathbb{E}_{k,k',i}[|i\rangle\langle i| \otimes X^e Z^f \rho Z^f X^e \rho]\right] \qquad (2.34)
\end{aligned}$$

where at step (a) $a\|b = h_i(k)$ and $c\|d = h_j(k')$ and where k and k' are independent instances of the key. Step (b) follows since $|i\rangle\langle i|\,|j\rangle\langle j| = \delta_{ij}$ and both terms have a $1/|I|$ probability associated with them. In step (c) $e\|f = (a \oplus c)\|(b \oplus d) = (a\|b) \oplus (c\|d)$.

Let us divide Equation (2.34) into two terms, one term for $k = k'$ and the other for $k \neq k'$. Let us introduce the following notation: ρ_{ef} instead of $X^e Z^f \rho Z^f X^e$ and p_{ef} for the probability that $e\|f$ is observed. Thus, after taking the partial trace on the ancillary system, we can rewrite everything like this:

$$\mathrm{Tr}\left[\mathcal{E}(\rho)^2\right] = \frac{1}{|I|}\mathrm{Tr}\left[\frac{\rho^2}{|K|} + \left(1 - \frac{1}{|K|}\right)\sum_{\substack{e,f \\ \text{where } k\neq k'}} p_{ef}\rho_{ef}\rho\right]. \tag{2.35}$$

We know that when $k = k'$ then for every i we have $e\|f = 0$ whilst for $k \neq k'$ by Definition 13, we know that the probability over all i of seeing any string $e\|f$ is equal to $1/2^{2n}$. Of course $\sum_{e,f} 1/2^n \rho_{ef} = \mathbb{I}/2^n$ [3]. Hence the second term reduces to $\mathrm{Tr}\left[\mathbb{I}/2^n\rho\right] = 1/2^n\mathrm{Tr}\left[\rho\right] = 1/2^n$.

$$\mathrm{Tr}\left[\mathcal{E}(\rho)^2\right] \leqslant \frac{1}{|I|}\left(\mathrm{Tr}\left[\frac{\rho^2}{|K|}\right] + \frac{1}{2^n}\right). \tag{2.36}$$

Let us denote $\mathrm{H}_\infty(K)$ by $t_K = \log|K|$ and $\mathrm{H}_\infty(\rho)$ by t_ρ. By hypothesis, we have $\mathrm{H}_\infty(K) + \mathrm{H}_\infty(\rho) \geqslant n + 2\log(1/\epsilon)$, hence $2^{n-t_k-t_\rho} \leqslant \epsilon^2$. We can thus rewrite (2.36) this way:

$$\mathrm{Tr}\left[\mathcal{E}(\rho)^2\right] \leqslant \frac{1}{|I|}\frac{1}{2^n}\left(2^{n-t_k-t_\rho} + 1\right) \leqslant \frac{1}{|I|}\frac{1}{2^n}\left(\epsilon^2 + 1\right), \tag{2.37}$$

since $\mathrm{Tr}\left[\rho^2\right] \leqslant 1/2^{t_\rho}$. This, in turn, implies that $\left\|\mathcal{E}(\rho) - \frac{\mathbb{I}}{d}\right\|_1 \leqslant \epsilon$ for $t_k = \log|K| \geqslant n - t + 2\log(1/\epsilon)$. QED.

The reader should note that the previous scheme is proven to be (t,ϵ)-indistinguishable using $n-t+2\log(1/\epsilon)$ bits of key in this model, whilst the same scheme was proven in [18] to be (t,ϵ)-indistinguishable in the classical model using $n-t+2\log(1/\epsilon)+2$ bits of key. A very slight improvement which is a gift of the better proof technique. But the most interesting thing to notice, is that in a stronger model than [18], we can now send quantum messages and the adversary can now be any POVM, we do not require more key in order to achieve security. This is, as far as we know, the only relaxation on perfect security which has this property: that is, both classical and quantum key size requirements are the same.

Furthermore, the reader should notice that the entropy on the key is not necessary maximum. The statement says that the scheme is secure if $H_\infty(K) + H_\infty(\rho) \geqslant n + 2\log(1/\epsilon)$. This is not new as Dodis and Smith already had stated their theorem this way, but they did not attracted the attention of the reader to the fact that the key did not need to be perfectly secret. We do believe that it is a very interesting feature of this second scheme.

But there is a small problem with what was proven. There is a tiny probability that the message is not encrypted and that the adversary is told that it is so. If $i = 0$, then we have the trivial identity function and since the sender puts i on the wire with the cipher text, he just told the adversary the message was in clear. This is not a very prudent thing to do, even though this can only happen with negligible probability. Fortunately, we can slightly modify the previous scheme and prove security in all cases.

Consider the event $Z = h_i(x) \oplus h_i(y)$. Now consider the same xor-function discussed earlier but modify it such that the probability that $i = 0$ is zero, and all other values for i happen with uniform probability $\frac{1}{2^n-1}$. Then, using this new family of xor-function, there is two different probabilities that a given value z that Z could take. Either Z is zero with probability $1/|K|$ or for any other value $Z = z$, this value has probability

$$p_z = \left(1 - \frac{1}{|K|}\right) \cdot \frac{1}{2^n - 1}, \qquad (2.38)$$

that is, once $x \neq y$ (the left term) the probability is uniform since i is chosen uniformly over $2^n - 1$ strings (right term). We want to prove that p_z is in fact inferior to $1/2^n$. High school arithmetic can convince us that if $|K| \leqslant 2^n \iff p_z \leqslant 1/2^n$.

Using this variation on XOR-universal functions, we can modify the proof of Theorem 6 to show the scheme is still (t, ϵ)-indistinguishable. We start with equation (2.34) which we parse exactly the same way. Let us divide it into two terms: one term for $e\|f = 0$ and one term for $e\|f \neq 0$ (it used to be $k = k'$ and $k \neq k'$). Thus, after taking the partial trace on the ancillary system, we can rewrite everything like this:

$$\operatorname{Tr}\left[\mathcal{E}(\rho)^2\right] = \frac{1}{|I|}\operatorname{Tr}\left[\frac{\rho^2}{|K|} + \sum_{\substack{e,f \\ \text{where } e\|f\neq 0}} p_{ef}\rho_{ef}\rho\right]. \tag{2.39}$$

Observe two things: for all $e\|f \neq 0$ we know that $p_{ef} \leqslant 1/2^{2n}$ and $\sum_{ef} \frac{1}{2^{2n}}\rho_{ef} = \mathbb{I}/2^n$, the perfectly mixed state. Quantum mechanic also tells us that $\operatorname{Tr}[\rho\sigma]$ is the expectation of the observed eigenvalue if one measures the observable ρ on the state σ. A specific case is $\operatorname{Tr}\left[\frac{\mathbb{I}}{2^n}\rho\right] = 1/2^n$, since all eigenvalues of the perfectly mixed state are equal to $1/2^n$, the average can not be different from this number.

Let A be the positive operator $\sum_{\substack{e,f \\ e\|f\neq 0}} p_{ef}\rho_{ef}$. From the previous observations, we can conclude that there exists a positive operator B such that $A + B = \mathbb{I}/2^n$. More specifically $B = \sum_{e,f}(\frac{1}{2^n} - p_{ef})\rho_{ef}$ and $p_{0\|0} = 0$. Therefore $\operatorname{Tr}[(A+B)\rho] \leqslant \frac{1}{2^n}$, thus $\operatorname{Tr}[A\rho] + \operatorname{Tr}[B\rho] \leqslant \frac{1}{2^n}$ and finally $\operatorname{Tr}[A\rho] \leqslant \frac{1}{2^n}$.

So we can rewrite Equation (2.39) this way:

$$\operatorname{Tr}\left[\mathcal{E}(\rho)^2\right] \leqslant \frac{1}{|I|}\left(\operatorname{Tr}\left[\frac{\rho^2}{|K|}\right] + \frac{1}{2^n}\right) \tag{2.40}$$

which is exactly the same as equation (2.36), hence we can conclude for this modify scheme the same thing concluded in Theorem 6.

This completes our study of the model excluding any kind of correlation or entanglement. We provided different proofs of security, mainly entropic-security and entropic-indistinguishability, and we proved that they are in fact, up to small parameter adjustment , equivalent. Very importantly, we showed that these definitions are indeed achievable and do provide improvement on the state of the art cryptography by presenting two different efficient ciphers which are indeed entropically-secure,

We shall now generalize all these results to a model where any correlation or entanglement between the sender and the adversary is be permitted.

Chapter 3

Correlated Cryptography

In this section, we discuss security definitions and ciphers in a model where the adversary could be correlated and/or entangled with the sender. From the adversary's point of view, the sender chooses (receives) a message σ_i^{SA} with probability p_i where σ_i^{SA} is a state shared by both the sender and the adversary. They each receive a register $\mathfrak{R}$ that holds their part of the shared state: $\mathfrak{R}^S$ for the sender and $\mathfrak{R}^A$ for the adversary. Hence the adversary's view (a priori knowledge) of the Sender-Adversary space is $\rho^{SA} = \sum_i p_i \sigma_i^{SA}$ and $H_\infty(\rho^{SA}|\rho^A) \geqslant t$ (*defined below*) where $\rho^A = \mathrm{Tr}_S(\rho^{SA})$. We call the set $\{(p_i, \sigma_i^{SA})\}_i$ an **interpretation** for ρ^{SA}. Then the sender encrypts his half, $\mathfrak{R}^S$, and gives it to the adversary.

Here, the adversary can see the entire encrypted system as the following source $(\mathcal{E}^S \otimes \mathbb{I}^A)(\rho^{SA}) = \sum_i p_i(\mathcal{E}^S \otimes \mathbb{I}^A)(\sigma_i^{SA})$, and he tries to predict i, or $f(i)$, or $f(\sigma_i^{SA})$ from what he is given, that is the two registers. We shall use the notation $f(i)$ to lighten an already very heavy notation from now on. Note that the encryption scheme is now a tensor of operators, that is the sender encrypts the $\mathfrak{R}^S$ register and sends its content to the receiver and nothing is done to the adversary's register: thus the encryption operator is $(\mathcal{E}^S \otimes \mathbb{I}^A)$, but we shall write $\mathcal{E}$ for simplicity.

$$\begin{tikzcd}
\boxed{\rho^{SA} = \sum_i p_i \sigma_i^{SA}} \arrow[r, "\sigma_i^{SA}"] & {} \arrow[r, "\mathfrak{R}^S"] \arrow[rr, bend right, "\mathfrak{R}^A"'] & \mathsf{S} \arrow[r, "\mathcal{E}(\mathfrak{R}^S)"] & \mathsf{A} \arrow[r] & f(i)
\end{tikzcd}$$

Figure 3.1: The generalized Model of the sender-adversary interaction

Definition 14 (Quantum conditional min-entropy) *For any quantum state ρ^{SA} shared between the sender and the adversary, we define the conditional min-entropy of ρ^{SA} given ρ^A as*

$$H_\infty(\rho^{SA}|\rho^A) = -\log \lambda,$$

where λ is the minimum real number such that the Hermitian operator $\lambda \mathbb{I}^S \otimes \rho^A - \rho^{SA}$ is positive semi-definite.

Observe that the last operator is defined using the identity matrix on the S space and not the perfectly mixed state. The following notation is occasionally used in the literature for quantum conditional min-entropy $H_\infty(S|A)_\rho \triangleq H_\infty(\rho^{SA}|\rho^A)$; the subscript indicates the state with respect to which the min-entropy is calculated. Observe also that we can obtain an equivalent definition for λ using the following:

$$\begin{aligned}
H_\infty(\rho^{SA}|\rho^A) &= -\log \min\{\lambda : \lambda \mathbb{I}^S \otimes \rho^A - \rho^{SA} \geqslant 0\} \\
&= -\log \min \left\{\lambda : \forall |\psi\rangle, \langle\psi|\lambda \mathbb{I}^S \otimes \rho^A|\psi\rangle \geqslant \langle\psi|\rho^{SA}|\psi\rangle\right\} \\
&= -\log \min \left\{\lambda : \forall |\psi\rangle,\ \lambda \geqslant \frac{\langle\psi|\rho^{SA}|\psi\rangle}{\langle\psi|\mathbb{I}^S \otimes \rho^A|\psi\rangle}\right\} \\
&= -\log \max_{|\psi\rangle} \left\{\frac{\langle\psi|\rho^{SA}|\psi\rangle}{\langle\psi|\mathbb{I}^S \otimes \rho^A|\psi\rangle}\right\}.
\end{aligned}$$

This last expression is reminiscent of the definition of classical conditional min-entropy, which we reproduce here:

$$H_\infty(X|Y) = -\log \max_{x,y} \left\{\frac{p(x,y)}{p(y)}\right\} \tag{3.1}$$

Some properties about the quantum conditional min-entropy can be proven which will be handy later on. First, this lemma:

Lemma 8 *Let the joint state of the sender and the adversary be a tensor product state,* $\rho^{SA} = \rho^S \otimes \rho^A$*, then* $H_\infty(\rho^{SA}|\rho^A) = H_\infty(\rho^S)$*.*

Proof:

The structure of ρ^{SA} lets us write this equality: $\lambda \mathbb{I}^S \otimes \rho^A - \rho^{SA} = (\lambda \mathbb{I}^S - \rho^S) \otimes \rho^A$. We know that ρ^A is positive, since it is a valid density operator, hence if we want this expression to be positive semi-definite, we need $\lambda \mathbb{I}^S - \rho^S$ to be positive semi-definite. This implies, since $\mathbb{I}$ commutes with everything, that $\lambda = \gamma_{\max}$, where $\gamma_{\max}$ is the largest eigenvalue of ρ^S. QED

But there are states which are still more general than tensor product states and yet imply no quantum correlation (i.e. entanglement). We say a state ρ^{AB} is separable if it can be written as $\rho^{AB} = \sum_z p_z \sigma_z^A \otimes \tau_z^B$, where $\sum_z p_z = 1$ and the p_z's are positive real numbers.

In this case, Lemma 3.1.8 of Renner's Ph.D thesis [37] allows us to conclude something interesting. Using Renner's notation, we say that a state ρ^{ABZ} is classical with respect to the space Z if there exists an orthonormal basis $\{|z\rangle\}$ for Z such that $\rho^{ABZ} = \sum_z p_z \rho_z^{AB} \otimes |z\rangle\langle z|$. Therefore, for any separable state ρ^{AB} there exist a space Z and a state ρ^{ABZ} such that $\mathrm{Tr}_Z[\rho^{ABZ}] = \rho^{AB}$, that is $\rho^{ABZ} = \sum_z p_z \sigma_z^A \otimes \tau_z^B \otimes |z\rangle\langle z|$. Lemma 3.1.8 in [37] states that

$$H_\infty(\rho^{ABZ}|\rho^{BZ}) = \inf_z H_\infty(\rho_z^{AB}|\rho_z^B). \tag{3.2}$$

Note that this quantity for separable states is very classical and contains no perverse quantum effects: by Lemma 8 we can conclude $H_\infty(\rho_z^{AB}|\rho_z^B) = H_\infty(\sigma_z^A \otimes \tau_z^B|\tau_z^B) = H_\infty(\sigma_z^A)$.

Lemma 3.1.7 of the same thesis also tells us that for any system C, $H_\infty(\rho^{ABC}|\rho^{BC}) \leqslant H_\infty(\rho^{AB}|\rho^B)$. Hence, putting all this together, we get for separable states that

$$H_\infty(\rho^{AB}|\rho^B) \geqslant \inf_z H_\infty(\sigma_z) \geqslant 0. \tag{3.3}$$

Sadly, as far as we know, no better expression is known for the min-entropy of separable states. Note that this also implies that using the definition of quantum conditional min-entropy will enable us to subtract more key bit than pure paranoia, quantified by $\inf_z H_\infty(\sigma_z)$, would allow us.

Note also that if the S and A spaces are maximally entangled, for example the state $\sum_{i=1}^{d} \frac{1}{\sqrt{d}} |i\rangle^S |i\rangle^A$, where $n = \log d$, then

$$H_\infty(\rho^{SA}|\rho^A) = -n. \tag{3.4}$$

The reader should also take note that all proofs in this work are compatible with a generalization of the conditional min-entropy known as smooth-entropy as defined in section 3 of [37]. Readers interested by the operational meaning of conditional min-entropy should consult [32].

Definition 15 (Entropic Security) *An encryption system $\mathcal{E}$ is (t,ε)-entropically secure if for all states ρ^{SA} such that $H_\infty(\rho^{SA}|\rho^A) \geqslant t$, all interpretations $\{(p_i, \sigma_i^{SA})\}_i$ and all adversaries A, there exists an A' such that for all functions f, we have* [1]

$$\left|\Pr_i[\mathsf{A}(\mathcal{E}(\sigma_i^{SA})) = f(i)] - \Pr_i[\mathsf{A}'(\sigma_i^{A}) = f(i)]\right| \leqslant \varepsilon. \tag{3.5}$$

We have to give σ_i to A' otherwise even a perfect scheme would not be able to achieve this definition. Take for example the following state: $\rho = \sum_{i\in I} 1/|I| \left|i^S \otimes i^A\middle\rangle\!\middle\langle i^S \otimes i^A\right|$. That is, when S gets i, then A also gets i; a perfectly correlated classical variable and let $f(\left|i^S \otimes i^A\middle\rangle\!\middle\langle i^S \otimes i^A\right|) = i$. Then $\Pr_i[\mathsf{A}(\mathcal{E}(\left|i^S \otimes i^A\middle\rangle\!\middle\langle i^S \otimes i^A\right|)) = f(i)] = 1$ whilst $\Pr_i[\mathsf{A}'(\cdot) = f(i)] = 1/|I|$. Which is obviously a bad definition, since even a perfect scheme would not achieve it for $\epsilon \leqslant 1/2$.

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

Definition 16 (Strong entropic security)
An encryption system $\mathcal{E}$ is strongly (t, ε)-entropically secure if for all states ρ^{SA} such that $H_\infty(\rho^{SA}|\rho^A) \geqslant t$, all interpretations $\{(p_i, \sigma_i^{SA})\}_i$, all adversaries A, and all functions f, we have

$$\left|\Pr_i[\mathsf{A}(\mathcal{E}(\sigma_i^{SA})) = f(i)] - \Pr_i[\mathsf{A}(\mathcal{E}(\rho^S) \otimes \sigma_i^A) = f(i)]\right| \leqslant \varepsilon, \tag{3.6}$$

where $\rho^S = \mathrm{Tr}_A(\rho^{SA})$.

Definition 17 (Entropic Indistinguishability)
An encryption system $\mathcal{E}$ is (t, ε)-indistinguishable if there exists a state $\Omega^{S'}$ such that for all states ρ^{SA} for which $H_\infty(\rho^{SA}|\rho^A) \geqslant t$ we have

$$\left\|\mathcal{E}(\rho^{SA}) - \Omega^{S'} \otimes \rho^A\right\|_1 < \varepsilon, \tag{3.7}$$

where, $\mathcal{E}$ sends the sender space S to the cipher space S'.

It is also easy to see, using the triangle inequality, that Definition 17 implies:

Definition 18 (Weak Entropic Indistinguishability) *An encryption scheme $\mathcal{E}$ is said to be weakly (t, ϵ)-indistinguishable if for all operators ρ^{SA} and γ^{SA}, where $\mathrm{Tr}_S\left[\gamma_{SA}\right] = \rho^A$, such that $H_\infty(\rho^{SA}|\rho^A) \geqslant t$ and $H_\infty(\gamma^{SA}|\gamma^A) \geqslant t$ we have*

$$\left\|\mathcal{E}(\rho^{SA}) - \mathcal{E}(\gamma^{SA})\right\|_1 < 2\epsilon. \tag{3.8}$$

Note that in the previous definition, we could have use all state γ_{SA} and not just separable ones, but the definition would then be even weaker.

3.1 Equivalence of the definitions

In this section, we shall prove that all four definitions of security in the general model are all equivalent. We use the same abbreviation as in §2 that is entropic security (ES), strong-entropic security (SES), Indistinguishability (I) and Weak-Indistinguishability (WI). Note that we have one more implication than in the uncorrelated model.

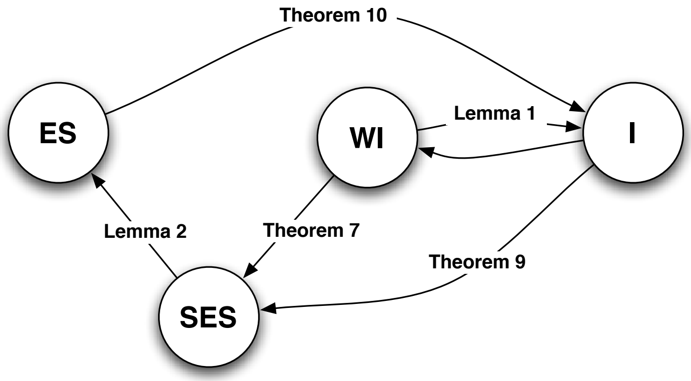

Figure 3.2: Graph of implications in the general Model

Theorem 7 *If $t \leqslant n-1$, then $(t-1, \varepsilon/4)$-weak entropic indistinguishability implies strong (t, ε)-entropic security.*

We shall prove a few intermediate results which will be useful.

Lemma 9 *Let A be a binary physical adversary in the general strong-entropic setting, i.e. a POVM with two elements, that has advantage ϵ at guessing h on a state $\rho = p_0\tau_0^{SA} + p_1\tau_1^{SA}$, where $h(i) = i$. Then for any sub-interpretation of τ_0^{SA} and τ_1^{SA} and a predicate g that partitions the output space as in the original interpretation, A's advantage is still ϵ at guessing $g(i)$ in the new interpretation.*

Proof:

We shall omit, as in Lemmas 3 and 4, to write the encryption $\mathcal{E}$ in order to lighten the notation. Let us develop the lemma's statement. We know that $\rho = p_0\tau_0^{SA} + p_1\tau_1^{SA}$ and that

$$\left|\mathrm{Pr}_k[\mathsf{A}(\tau_k^{SA}) = h(k)] - \mathrm{Pr}_k[\mathsf{A}(\rho^S \otimes \tau_k^A) = h(k)]\right| = \epsilon, \tag{3.9}$$

where h is a predicate, $\mathsf{A} = \{\mathsf{A}_0, \mathsf{A}_1\}$ and $\mathrm{Pr}[\mathsf{A}(\tau_k^{SA}) = h(k)] = \mathrm{Tr}\left[\mathsf{A}_{h(k)}\tau_k^{SA}\right]$. The statement also mentions a second interpretation, and predicate, $\rho = \sum_i q_i\sigma_i^{SA}$ and of a partition of the indices, $F_0 \triangleq \{i|g(i) = 0\}_i$ and $F_1 \triangleq \{i|g(i) = 1\}_i$, such that $p_0\tau_0^{SA} = \sum_{i\in F_0} q_i\sigma_i^{SA}$ and $p_1\tau_1^{SA} = \sum_{i\in F_1} q_i\sigma_i^{SA}$. We shall assume for simplicity that $h(k) = k$. We wish to show that

$$\begin{aligned}
&\left|\mathrm{Pr}_i[\mathsf{A}(\sigma_i^{SA}) = g(i)] - \mathrm{Pr}_{i,j}[\mathsf{A}(\sigma_j^S \otimes \sigma_i^A) = g(i)]\right| \\
&\qquad = \left|\mathrm{Pr}_k[\mathsf{A}(\tau_k^{SA}) = h(k)] - \mathrm{Pr}_{k,l}[\mathsf{A}(\tau_l^S \otimes \tau_k^A) = h(k)]\right| \\
&\qquad = \epsilon.
\end{aligned} \tag{3.10}$$

Let us first start by proving that the first terms of both sides are the same.

$$\begin{aligned}
\mathrm{Pr}_i[\mathsf{A}(\sigma_i^{SA}) = g(i)] &= \sum_i q_i \mathrm{Pr}[\mathsf{A}(\sigma_i^{SA}) = g(i)] \\
&= \sum_{i\in F_0} q_i \mathrm{Pr}[\mathsf{A}(\sigma_i^{SA}) = 0] + \sum_{i\in F_1} q_i \mathrm{Pr}[\mathsf{A}(\sigma_i^{SA}) = 1] \\
&= \sum_{i\in F_0} q_i \mathrm{Tr}\left[\mathsf{A}_0\sigma_i^{SA}\right] + \sum_{i\in F_1} q_i \mathrm{Tr}\left[\mathsf{A}_1\sigma_i^{SA}\right] \\
&= p_0 \mathrm{Tr}\left[\mathsf{A}_0\tau_0^{SA}\right] + p_1 \mathrm{Tr}\left[\mathsf{A}_1\tau_1^{SA}\right] \\
&= p_0 \mathrm{Pr}[\mathsf{A}(\tau_0^{SA}) = 0] + p_1 \mathrm{Pr}[\mathsf{A}(\tau_1^{SA}) = 1] \\
&= \mathrm{Pr}_k[\mathsf{A}(\tau_k^{SA}) = k].
\end{aligned}$$

Now for the second terms:

$$\begin{aligned}
\mathrm{Pr}_{i,j}&[\mathsf{A}(\sigma_j^S \otimes \sigma_i^A) = g(i)] \\
&= \sum_i q_i \mathrm{Pr}_j[\mathsf{A}(\sigma_j^S \otimes \sigma_i^A) = g(i)] \\
&= \sum_{i \in F_0} q_i \mathrm{Pr}_j[\mathsf{A}(\sigma_j^S \otimes \sigma_i^A) = 0] + \sum_{i \in F_1} q_i \mathrm{Pr}_j[\mathsf{A}(\sigma_j^S \otimes \sigma_i^A) = 1] \\
&\overset{(a)}{=} \sum_{i \in F_0} q_i \left(\sum_{j \in F_0} q_j \mathrm{Pr}[\mathsf{A}(\sigma_j^S \otimes \sigma_i^A) = 0] + \sum_{j \in F_1} q_j \mathrm{Pr}[\mathsf{A}(\sigma_j^S \otimes \sigma_i^A) = 0] \right) + \ldots \\
&= \sum_{i \in F_0} q_i \left(\sum_{j \in F_0} q_j \mathrm{Tr}\left[\mathsf{A}_0(\sigma_j^S \otimes \sigma_i^A)\right] + \sum_{j \in F_1} q_j \mathrm{Tr}\left[\mathsf{A}_0(\sigma_j^S \otimes \sigma_i^A)\right] \right) + \ldots \\
&= \sum_{i \in F_0} q_i \left(p_0 \mathrm{Tr}\left[\mathsf{A}_0(\tau_0^S \otimes \sigma_i^A)\right] + p_1 \mathrm{Tr}\left[\mathsf{A}_0(\tau_1^S \otimes \sigma_i^A)\right] \right) + \ldots \\
&= \sum_{i \in F_0} q_i \left(\mathrm{Pr}_l[\mathsf{A}(\tau_l^S \otimes \sigma_i^A) = 0] \right) + \ldots
\end{aligned}$$

where (a) follows by simply replacing the second term in the sum by dots for the meanwhile. Bringing back the long forgotten second term lost in (a) we can continue

$$\begin{aligned}
\mathrm{Pr}_{i,j}&[\mathsf{A}(\sigma_j^S \otimes \sigma_i^A) = g(i)] \\
&= \sum_{i \in F_0} q_i \left(\mathrm{Pr}_l[\mathsf{A}(\tau_l^S \otimes \sigma_i^A) = 0] \right) + \sum_{i \in F_1} q_i \mathrm{Pr}_j[\mathsf{A}(\sigma_j^S \otimes \sigma_i^A) = 1] \\
&= \sum_{i \in F_0} q_i \left(\mathrm{Pr}_l[\mathsf{A}(\tau_l^S \otimes \sigma_i^A) = 0] \right) + \sum_{i \in F_1} q_i \left(\mathrm{Pr}_l[\mathsf{A}(\tau_l^S \otimes \sigma_i^A) = 1] \right) \\
&= p_0 \mathrm{Pr}_l[\mathsf{A}(\tau_l^S \otimes \tau_0^A) = 0] + p_1 \mathrm{Pr}_l[\mathsf{A}(\tau_l^S \otimes \sigma_i^A) = 1] \\
&= \mathrm{Pr}_{l,k}[\mathsf{A}(\tau_l^S \otimes \tau_k^A) = k].
\end{aligned}$$

Both term being equal, it must be that the difference has not changed in the new interpretation. QED

Theorem 8 *Let ρ^{SA} be a state, $\{(p_i, \sigma_i^{SA})\}_i$ be an interpretation, $\mathcal{E}$ be a cipher, f be a function and A be an adversary such that*

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

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

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

Proof:
Let our predicate be a Goldreich-Levin predicate [21], that is $h_r(x) = r \odot f(x)$. Let $p = \Pr[\mathsf{A}(\mathcal{E}(\sigma_i^{SA})) = f(i)]$ and $q = \Pr[\mathsf{A}(\mathcal{E}(\rho^S) \otimes \sigma_i^A) = f(i)]$. Then we know that $|p - q| > \epsilon$. Let us compute

$$E = \left|\mathbb{E}_r\Big[\Pr[r \odot \mathsf{A}(\mathcal{E}(\sigma_i^{SA})) = h_r(i)] - \Pr[r \odot \mathsf{A}(\mathcal{E}(\rho^S) \otimes \sigma_i^A) = h_r(i)]\Big]\right|, \tag{3.11}$$

where the expectation is taken over all r of adequate size. We need two observations. First, when A predicts correctly, then for every r we have $r \odot \mathsf{A}(\mathcal{E}(\sigma_i^{SA})) = h_r(i)$. Second, when A does not predict correctly, the probability that $r \odot \mathsf{A}(\mathcal{E}(\sigma_i^{SA})) = h_r(i)$ is exactly one half. These two observations also hold for $r \odot \mathsf{A}(\mathcal{E}(\rho^S) \otimes \sigma_i^A)$. Hence Equation (3.11) reduces to

$$\begin{aligned} E &= \left|1 \cdot p + \frac{1}{2} \cdot (1 - p) - \Big(1 \cdot q + \frac{1}{2} \cdot (1 - q)\Big)\right| \\ &= \left|\frac{p - q}{2}\right| > \frac{\varepsilon}{2}. \end{aligned} \tag{3.12}$$

Thus there exists at least one value r such that the following is true:

$$\left|\Pr[r \odot \mathsf{A}(\mathcal{E}(\sigma_i^{SA})) = h_r(i)] - \Pr[r \odot \mathsf{A}(\mathcal{E}(\rho^S) \otimes \sigma_i^A) = h_r(i)]\right| > \frac{\varepsilon}{2}. \tag{3.13}$$

The lemma is proven if adversary B is defined, using this appropriate r, as $r \odot \mathsf{A}$.
QED

Not surprisingly, one cannot immediately generalize Lemma 5 to the correlated model of security. Inspection of the proof of Lemma 5 reveals that the probability of correctly predicting the predicate is not the same between A and $\mathsf{A}(\cdot)$ (where here $\mathsf{A}(\cdot)$ means that A is called with a forged input), hence simplification will not occur. This reveals something interesting about the correlated model: there might be predicates for which, if $\mathcal{E}$ is not good enough, then the predicting capabilities of A and $\mathsf{A}(\cdot)$ are not the same on a constant predicate.

Here is an example of this phenomenon. Let the message space have two states in it: $\Phi^{+SA} = 1/\sqrt{2}(|00\rangle + |11\rangle)$ and $\Phi^{-SA} = 1/\sqrt{2}(|00\rangle - |11\rangle)$. Let the adversary A be the POVM Π, constituted of the two following measurement operators: Π_Φ, which is a projector on the space spanned by Φ^{+SA} and Φ^{-SA}, and Π_ψ which is a projector on the space spanned by $\Psi^{+SA} = 1/\sqrt{2}(|01\rangle + |10\rangle)$ and $\Psi^{-SA} = 1/\sqrt{2}(|01\rangle - |10\rangle)$. Note that Π is a complete binary measurement of the space and that Π is in fact a constant predicate on the message space. So the advantage of A over $\mathsf{A}(\cdot)$ is

$$\left|\Pr_i[\mathsf{A}(\mathcal{E}(\Phi^{\pm SA})) = f(i)] - \Pr_i[\mathsf{A}(\mathcal{E}(\rho^S) \otimes \Phi^{\pm A}) = f(i)]\right|$$

If we choose the really bad encryption scheme which is the identity — Lemma 5 does not even mention encryption in order to get it's result, hence its result holds even using $\mathbb{I}$ as an encryption scheme — clearly we get

$$\left|\underbrace{\Pr_i[\mathsf{A}(\Phi^{\pm SA}) = f(i)]}_{=1} - \underbrace{\Pr_i[\mathsf{A}(\mathbb{I}^S \otimes \mathbb{I}^A) = f(i)]}_{=1/2}\right| = \frac{1}{2}.$$

This is once more a strange effect of correlation and entanglement. We need to be more creative.

Lemma 10 *For any function f if there exits an adversary A that has advantage ϵ at guessing its value, then there is another adversary A' and a non-constant predicate h'_r such that A' has advantage $\epsilon/2$ at guessing h'_r in the generalized strong-entropic security.*

Proof:

We start from the adversary constructed in Theorem 8. We shall construct a new function f' and use it instead of f in constructing the predicate h'_r which will use the same r as h_r. Let us start with equation (3.13) and again choose a r such that

$$E = \left|\Pr[r \odot \mathsf{A}(\mathcal{E}(\sigma_i^{SA})) = h_r(i)] - \Pr[r \odot \mathsf{A}(\mathcal{E}(\rho^S) \otimes \sigma_i^A) = h_r(i)]\right| > \frac{\varepsilon}{2}. \qquad (3.14)$$

Assume h_r is constant. Let us now assume that the range of f is over m-bit strings: $\forall i, f(i) \in \{0,1\}^m$. Let $F \triangleq \{f(i)\}_i$, $F_0 = \{j \in \{0,1\}^m | j \odot r = 0\}_i$ and $F_1 = \{j \in \{0,1\}^m | j \odot r = 1\}_i$. Since $h_r(i)$ is constant, it must be that $|F| \leqslant 2^{m-1}$. The value r partitions the input space into two sets: the one whose element have their image in F_0 and the one whose element have their image in F_1. Since $h_r(i)$ is constant, then it must be that all i belong to one of those two sets.

Let us construct a new function f'. This function will simply remap part of the output of f to lie in the other set. Let us assume without loss of generality that for all i, $f(i) \in F_0$. Since f is a function, it has at least 3 different outputs with non-zero measure (otherwise, we would consider it to be a predicate, and we would not need this Lemma). Let the set $Z = \{z | \exists i \text{ s.t. } z = f(i)\}_z$ be the set of possible outputs for f and consider the sets $E_z = \{i | f(i) = z\}_i$. The sets E_z partition the input to f. To construct f', choose a totally arbitrary number of set E_z (at least one and not all of them) and reassign all the points $i \in E_z$ to some $z' \in F_1$. That is, for part of the input, $f'(E_z) = f(E_z) = z$ and for the other part $f'(E_z) \neq f(E_z)$ and $f(E_z) \odot r = 1$. This remapping is unitary, it is in fact simply a permutation of the output of f. Let us call this remap U, where U is the unitary operator that remaps the output of f. Then, obviously $\mathsf{A}' = U\mathsf{A}U^\dagger$ will be as good at predicting f' as A is good at predicting f. Hence we can conclude

$$E = \left| \Pr[r \odot U\mathsf{A}(\mathcal{E}(\sigma_i^{SA}))U^\dagger = h'_r(i)] - \Pr[r \odot U\mathsf{A}(\mathcal{E}(\rho^S) \otimes \sigma_i^A)U^\dagger = h'_r(i)] \right| > \frac{\varepsilon}{2},$$

where $h'_r(i) = r \odot f'(i)$ and h_r is not constant. QED

Proof of Theorem 7:

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

$$\left| \Pr_i[\mathsf{B}(\mathcal{E}(\sigma_i^{SA})) = f(i)] - \Pr_i[\mathsf{B}(\mathcal{E}(\rho^S) \otimes \sigma_i^A) = f(i)] \right| > \epsilon. \tag{3.15}$$

Then we know, see Theorem 8, that there exists another adversary and a predicate h such that $(t, \varepsilon/2)$-strong-entropic security is violated. Let's call this adversary A and let us define the sets E_0 and E_1 as follows:

$$E_0 = \{i | h(i) = 0\}_i \tag{3.16}$$

$$E_1 = \{i | h(i) = 1\}_i \,. \tag{3.17}$$

Define the following:

$$r_0 = \sum_{i \in E_0} p_i, \tag{3.18}$$

$$r_1 = \sum_{i \in E_1} p_i, \tag{3.19}$$

$$\tau_0^{SA} = \frac{1}{r_0}\left(\sum_{i \in E_0} p_i \sigma_i^{SA}\right) \tag{3.20}$$

$$\tau_1^{SA} = \frac{1}{r_1}\left(\sum_{i \in E_1} p_i \sigma_i^{SA}\right). \tag{3.21}$$

Note that $\rho^{SA} = r_0\tau_0^{SA} + r_1\tau_1^{SA}$. Lemma 9 tells us that A's advantage is still larger than $\epsilon/2$ when used as a black box to predict h on $\mathcal{E}(\rho^{SA})$ when ρ^{SA} is interpreted as $\rho^{SA} = r_0\tau_0^{SA} + r_1\tau_1^{SA}$. Our violation over the τ_i^{SA} is now:

$$\left|\sum_{i=0,1} p_i \Big(\Pr[\mathsf{A}(\mathcal{E}(\tau_i^{SA})) = i] - \Pr[\mathsf{A}(\mathcal{E}(\rho^S) \otimes \tau_i^A) = i]\Big)\right| > \frac{\epsilon}{2}. \tag{3.22}$$

So there exist i such that

$$\Big|p_i\Big(\Pr[\mathsf{A}(\mathcal{E}(\tau_i^{SA})) = i] - \Pr[\mathsf{A}(\mathcal{E}(\rho^S) \otimes \tau_i^A) = i]\Big)\Big| > \epsilon/4 \tag{3.23}$$

Now, Theorem 4 tells us that if this last equation is true then the trace distance between $\mathcal{E}(\tau_i^{SA})$ and $\mathcal{E}(\rho^S \otimes \tau_i^A)$ is at least $(\epsilon/4)/p_i$. We are not done yet since we have no guaranty on the quantities $H_\infty(\tau_i^{SA}|\tau_i^A)$ and $H_\infty(\rho^S \otimes \tau_i^A|\tau_i^A)$. We need to construct new states. Let us define the following two states:

$$\tilde{\tau}_i^{SA} = r_i\tau_i^{SA} + r_j\frac{\mathbb{I}^S}{d_S} \otimes \tau_j^A \tag{3.24}$$

$$\tilde{\rho}_i^{SA} = r_i\rho^S \otimes \tau_i^A + r_j\frac{\mathbb{I}^S}{d_S} \otimes \tau_j^A, \tag{3.25}$$

where $i \in \{0,1\}$ and $j = 1-i$. Note that $\mathrm{Tr}_S\left[\tilde{\tau}_i^{SA}\right] = \mathrm{Tr}_S\left[\tilde{\rho}_i^{SA}\right] = \rho^A$. Now as Lemma 11 proves, both these new states have at least $t-1$ conditional min-entropy. And we can now evaluate the following equation, which is one element of the trace distance:

$$\left|\Pr[\mathsf{A}(\mathcal{E}(\tilde{\tau}_i^{SA})) = i] - \Pr[\mathsf{A}(\mathcal{E}(\tilde{\rho}_i^{SA})) = i]\right|. \tag{3.26}$$

So, assuming without loss of generality, that $i = 0$, we have:

$$\begin{aligned}
&\left|\Pr[\mathsf{A}(\mathcal{E}(\tilde{\tau}_0^{SA})) = 0] - \Pr[\mathsf{A}(\mathcal{E}(\tilde{\rho}_0^{SA})) = 0]\right| \\
&\quad= \left|\mathrm{Tr}\left[\mathsf{A}_0\mathcal{E}(\tilde{\tau}_0^{SA})\right] - \mathrm{Tr}\left[\mathsf{A}_0\mathcal{E}(\tilde{\rho}_0^{SA})\right]\right| \\
&\quad= \left|\mathrm{Tr}\left[\mathsf{A}_0\mathcal{E}(r_0\tau_0^{SA} + r_1\frac{\mathbb{I}^S}{d_S} \otimes \tau_1^A)\right] - \mathrm{Tr}\left[\mathsf{A}_0\mathcal{E}(r_0\rho^S \otimes \tau_0^A + r_1\frac{\mathbb{I}^S}{d_S} \otimes \tau_1^A)\right]\right| \\
&\quad= \left|\mathrm{Tr}\left[\mathsf{A}_0\mathcal{E}(r_0\tau_0^{SA})\right] + \mathrm{Tr}\left[\mathsf{A}_0\mathcal{E}(r_1\frac{\mathbb{I}^S}{d_S} \otimes \tau_1^A)\right]\right. \\
&\qquad\qquad \left. - \mathrm{Tr}\left[\mathsf{A}_0\mathcal{E}(r_0\rho^S \otimes \tau_0^A)\right] - \mathrm{Tr}\left[\mathsf{A}_0\mathcal{E}(r_1\frac{\mathbb{I}^S}{d_S} \otimes \tau_1^A)\right]\right| \\
&\quad= \left|r_0\mathrm{Tr}\left[\mathsf{A}_0\mathcal{E}(\tau_0^{SA})\right] - r_0\mathrm{Tr}\left[\mathsf{A}_0\mathcal{E}(\rho^S \otimes \tau_0^A)\right]\right| \\
&\quad= \left|r_0\Big(\Pr[\mathsf{A}(\mathcal{E}(\tau_0^{SA})) = 0] - \Pr[\mathsf{A}(\mathcal{E}(\rho^S \otimes \tau_0^A)) = 0]\Big)\right| \\
&\quad> \frac{\epsilon}{4}
\end{aligned} \tag{3.27}$$

where the last step uses (3.23). Using the same trick as in equation (2.21) and Theorem 4, we conclude that $\left\|\mathcal{E}(\tilde{\tau}_0^{SA}) - \mathcal{E}(\tilde{\rho}_0^{SA})\right\|_1$ is larger than $\epsilon/2$.

Hence $\tilde{\tau}_0^{SA}$ and $\tilde{\rho}_0^{SA}$ constitute a violation of $(t-1, \epsilon/4)$-weak-indistinguishability, which, by Lemma 1, in turns implies a violation of the $(t-1, \epsilon/2)$-indistinguishability. QED

Lemma 11 *Let $\rho^{SA} = r_0\tau_0^{SA} + r_1\tau_1^{SA}$ be a state such that $H_\infty(\rho^{SA}|\rho^A) > t$ and $t \leqslant n-1$. Then the four states $\tilde{\tau}_i^{SA} = r_i\tau_i^{SA} + r_j\frac{\mathbb{I}^S}{d_S} \otimes \tau_j^A$ and $\tilde{\rho}_i^{SA} = r_i\rho^S \otimes \tau_i^A + r_j\frac{\mathbb{I}^S}{d_S} \otimes \tau_j^A$ where $i \in \{0,1\}$ and $j = 1-i$, all have high conditional min-entropy, that is $H_\infty(\tilde{\tau}_i^{SA}|\tilde{\tau}_i^A) > t-1$ and $H_\infty(\tilde{\rho}_i^{SA}|\tilde{\rho}_i^A) > t-1$.*

Proof:

Let us first deal with the first two states. Observe that $\mathrm{Tr}_S\left[\tilde{\rho}_i^{SA}\right] = \mathrm{Tr}_S\left[\tilde{\tau}_i^{SA}\right] = \rho^A$ since the partial trace is linear — $\mathrm{Tr}_S\left[\sum_i p_i \sigma_i^{SA}\right] = \sum_i p_i \mathrm{Tr}_S\left[\sigma_i^{SA}\right]$. By definition, we know that

$$H_\infty(\tilde{\tau}_i^{SA}|\tilde{\tau}_i^A) = -\log \max_{|\psi\rangle} \frac{\langle\psi|\tilde{\tau}_i^{SA}|\psi\rangle}{\langle\psi|\mathbb{I}^S \otimes \tilde{\tau}_i^A|\psi\rangle}.$$

We can develop the right hand side into

$$\max_{|\psi\rangle} \frac{\langle\psi|\tilde{\tau}_i^{SA}|\psi\rangle}{\langle\psi|\mathbb{I}^S \otimes \tilde{\tau}_i^A|\psi\rangle} \leqslant r_i \max_{|\psi\rangle} \frac{\langle\psi|\tau_i^{SA}|\psi\rangle}{\langle\psi|\mathbb{I}^S \otimes \rho^A|\psi\rangle} + r_j \max \psi \frac{\langle\psi|\frac{\mathbb{I}^S}{d_S} \otimes \rho^A|\psi\rangle}{\langle\psi|\mathbb{I}^S \otimes \rho^A|\psi\rangle}.$$

Let us develop the first term:

$$\begin{aligned} r_i \max_{|\psi\rangle} \frac{\langle\psi|\tau_i^{SA}|\psi\rangle}{\langle\psi|\mathbb{I}^S \otimes \rho^A|\psi\rangle} &\overset{(a)}{\leqslant} r_i \max_{|\psi\rangle} \frac{\langle\psi|\tau_i^{SA} + \frac{r_j}{r_i}\tau_j^{SA}|\psi\rangle}{\langle\psi|\mathbb{I}^S \otimes \rho^A|\psi\rangle} \\ &\leqslant \max_{|\psi\rangle} \frac{\langle\psi|r_i\tau_i^{SA} + r_j\tau_j^{SA}|\psi\rangle}{\langle\psi|\mathbb{I}^S \otimes \rho^A|\psi\rangle} \\ &\leqslant \max_{|\psi\rangle} \frac{\langle\psi|\rho^{SA}|\psi\rangle}{\langle\psi|\mathbb{I}^S \otimes \rho^A|\psi\rangle} \\ &\leqslant 2^{-t}, \end{aligned}$$

where $j = 1 - i$ and (a) follows since adding a non-negative term, $\langle\psi|r_j/r_i\tau_j^{SA}|\psi\rangle \geqslant 0$, to the numerator cannot decrease the expression. Now for the second term:

$$\begin{aligned} r_j \max_{\psi} \frac{\langle\psi|\frac{\mathbb{I}^S}{d_S} \otimes \rho^A|\psi\rangle}{\langle\psi|\mathbb{I}^S \otimes \rho^A|\psi\rangle} &\leqslant r_j 2^{-t} \\ &\leqslant 2^{-t} < 2^{-n}, \end{aligned}$$

since $H_\infty(\frac{\mathbb{I}^S}{d_S} \otimes \rho^A|\rho^A) = -\log \max_{|\psi\rangle} \frac{\langle\psi|\frac{\mathbb{I}^S}{d_S}\otimes\rho^A|\psi\rangle}{\langle\psi|\mathbb{I}^S\otimes\rho^A|\psi\rangle}$ and, by Lemma 8, $H_\infty(\frac{\mathbb{I}^S}{d_S} \otimes \rho^A|\rho^A)$ is maximum, that is larger than $t \leqslant n - 1$.

Putting all this together we get

$$\begin{aligned}\max_{|\psi\rangle} \frac{\langle\psi|\tilde{\tau}_i^{SA}|\psi\rangle}{\langle\psi|\mathbb{I}^S \otimes \tilde{\tau}_i^A|\psi\rangle} &\leqslant 2^{-t} + 2^{-t} \\ &= 2^{-(t-1)}.\end{aligned}$$

Now for the last two states:

$$\begin{aligned}\max_{|\psi\rangle} \frac{\langle\psi|\tilde{\rho}_i^{SA}|\psi\rangle}{\langle\psi|\mathbb{I}^S \otimes \tilde{\rho}_i^A|\psi\rangle} &= \max_{|\psi\rangle} \frac{\langle\psi|r_i\rho^S \otimes \tau_i^A + r_j\frac{\mathbb{I}^S}{d_S} \otimes \tau_j^A|\psi\rangle}{\langle\psi|\mathbb{I}^S \otimes (r_i\tau_i^A + r_j\tau_j^A)|\psi\rangle} \\ &\leqslant r_i \max_{|\psi\rangle} \frac{\langle\psi|\rho^S \otimes \tau_i^A|\psi\rangle}{\langle\psi|\mathbb{I}^S \otimes (r_i\tau_i^A + r_j\tau_j^A)|\psi\rangle} \\ &\qquad + r_j \max_{|\psi\rangle} \frac{\langle\psi|\frac{\mathbb{I}^S}{d_S} \otimes \tau_j^A|\psi\rangle}{\langle\psi|\mathbb{I}^S \otimes (r_i\tau_i^A + r_j\tau_j^A)|\psi\rangle}\end{aligned}$$

We can develop the second term this way:

$$\begin{aligned}r_j \max_{|\psi\rangle} \frac{\langle\psi|\frac{\mathbb{I}^S}{d_S} \otimes \tau_j^A|\psi\rangle}{\langle\psi|\mathbb{I}^S \otimes (r_i\tau_i^A + r_j\tau_j^A)|\psi\rangle} &\overset{(a)}{\leqslant} r_j \max_{|\psi\rangle} \frac{\langle\psi|\frac{\mathbb{I}^S}{d_S} \otimes \tau_j^A|\psi\rangle}{\langle\psi|\mathbb{I}^S \otimes r_j\tau_j^A|\psi\rangle} \\ &= \max_{|\psi\rangle} \frac{\langle\psi|\frac{\mathbb{I}^S}{d_S} \otimes \tau_j^A|\psi\rangle}{\langle\psi|\mathbb{I}^S \otimes \tau_j^A|\psi\rangle} \\ &\overset{(b)}{\leqslant} 2^{-n} \\ &\leqslant 2^{-t},\end{aligned}$$

where (a) follows since removing a non-negative term in the denominator cannot decrease the expression and (b) follows by Lemma 8. We can bound the first term as follows:

$$\begin{aligned}r_i \max_{|\psi\rangle} \frac{\langle\psi|\rho^S \otimes \tau_i^A|\psi\rangle}{\langle\psi|\mathbb{I}^S \otimes (r_i\tau_i^A + r_j\tau_j^A)|\psi\rangle} &\overset{(a)}{\leqslant} r_i \max_{|\psi\rangle} \frac{\langle\psi|\rho^S \otimes \tau_i^A + \frac{r_j}{r_i}\rho^S \otimes \tau_j^A|\psi\rangle}{\langle\psi|\mathbb{I}^S \otimes \rho^A|\psi\rangle} \\ &= \max_{|\psi\rangle} \frac{\langle\psi|r_i\rho^S \otimes \tau_i^A + r_j\rho^S \otimes \tau_j^A|\psi\rangle}{\langle\psi|\mathbb{I}^S \otimes \rho^A|\psi\rangle} \\ &= \max_{|\psi\rangle} \frac{\langle\psi|\rho^S \otimes \rho^A|\psi\rangle}{\langle\psi|\mathbb{I}^S \otimes \rho^A|\psi\rangle} \\ &\overset{b}{\leqslant} \max_{|\psi\rangle} \frac{\langle\psi|\rho^{SA}|\psi\rangle}{\langle\psi|\mathbb{I}^S \otimes \rho^A|\psi\rangle} \\ &\leqslant 2^{-t},\end{aligned}$$

where (a) follows since adding a non-negative term to the numerator cannot decrease the expressions and (b) is justified by the following chain of implications that uses the first definition of λ in the conditional min-entropy: $\lambda\mathbb{I}^S \otimes \rho^A - \rho^{SA} \geqslant 0 \implies \mathrm{Tr}_A\left(\lambda\mathbb{I}^S \otimes \rho^A - \rho^{SA}\right) \geqslant 0 \implies \lambda\mathbb{I}^S \otimes \rho^A - \rho^S \otimes \rho^A \geqslant 0$, hence the conditional min-entropy cannot decrease along that chain of implication.

Putting all this together, we get :

$$\max_{|\psi\rangle} \frac{\langle\psi|\tilde{\rho}_i^{SA}|\psi\rangle}{\langle\psi|\mathbb{I}^S \otimes \tilde{\rho}_i^A|\psi\rangle} \leqslant 2_{-t} + 2^{-t} = 2^{-(t-1)}.$$

QED

At the cost of being a little more obscure, we can eliminate the need to use weak-indistinguishability in the proof and prove directly that indistinguishability and strong entropic security are equivalent.

Theorem 9 *$(t-1, \varepsilon/2)$-entropic indistinguishability implies strong (t, ε)-entropic security for all functions.*

Proof:

We can follow the proof of Theorem 7 until equation (3.21). We shall construct two different states in order to get a contradiction with indistinguishability:

$$\begin{aligned} \tilde{\tau}_0^{SA} &= r_0\tau_0^{SA} + r_1\rho^S \otimes \tau_1^A && (3.28) \\ \tilde{\tau}_1^{SA} &= r_1\tau_1^{SA} + r_0\rho^S \otimes \tau_0^A, && (3.29) \end{aligned}$$

where, as usual, $\tau_i^A = \mathrm{Tr}_S[\tau_i^{SA}]$. Lemma 12 tells us that both states have conditional min-entropy no less than $t-1$. We want to show that A can distinguish $\mathcal{E}(\tilde{\tau}_0^{SA})$ from $\mathcal{E}(\tilde{\tau}_1^{SA})$ with probability strictly better than $1/2 + \varepsilon/4$. Let's denote by η the probability that A will correctly distinguish $\mathcal{E}(\tau_0^{SA})$ from $\mathcal{E}(\tau_1^{SA})$ 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 $\mathcal{E}(\tilde{\tau}_0^{SA})$ with probability 1/2 and $\mathcal{E}(\tilde{\tau}_1^{SA})$ with probability 1/2. Observe that this is exactly as if we gave it an r_0, r_1 mixture of $\mathcal{E}(\tau_0^{SA})$ and $\mathcal{E}(\tau_1^{SA})$ 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 $\mathcal{E}(\tilde{\tau}_0^{SA})$ from $\mathcal{E}(\tilde{\tau}_1^{SA})$ 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 Lemma 9 and the assumption that A violates entropic security, we know that

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

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

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

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

Lemma 12 *Assuming $H_\infty(\rho^{SA}|\rho^A) \geqslant t$, we then have that both $H_\infty(\tilde{\tau}_0^{SA}|\tilde{\tau}_0^A)$ and $H_\infty(\tilde{\tau}_1^{SA}|\tilde{\tau}_1^A)$ are at least $t-1$ for $\tilde{\tau}_i^{SA}$ as define in 9.*

Proof:

First, since the partial trace is linear, it is clear that $\tilde{\tau}_0^A = \tilde{\tau}_1^A = \rho^A$. We then have

$$\max_{|\psi\rangle} \frac{\langle\psi|\tilde{\tau}_0^{SA}|\psi\rangle}{\langle\psi|\mathbb{I}^S \otimes \rho^A|\psi\rangle} \leqslant r_0 \max_{|\psi\rangle} \frac{\langle\psi|\tau_0^{SA}|\psi\rangle}{\langle\psi|\mathbb{I}^S \otimes \rho^A|\psi\rangle} + r_1 \max_{|\psi\rangle} \frac{\langle\psi|\rho^A \otimes \tau_1^A|\psi\rangle}{\langle\psi|\mathbb{I}^S \otimes \rho^A|\psi\rangle}.$$

We already bounded both terms in Lemma 11 by 2^{-t}.

Combining these two results, we obtain

$$\max_{|\psi\rangle} \frac{\langle\psi|\tilde{\tau}_0^{SA}|\psi\rangle}{\langle\psi|\mathbb{I}^S \otimes \rho^A|\psi\rangle} \leqslant 2 \times 2^{-t} = 2^{-(t-1)}.$$

Of course, an identical calculation yields the same result for $\tilde{\tau}_1^{SA}$. QED

Theorem 10 *If $t \leqslant n-1$ and one defines $\Omega^{S'}$ to be $\mathcal{E}(\mathbb{I}^S/d)$, then (t,ε)-entropic-security implies $(t-1, 6\varepsilon)$-indistinguishability.*

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

$$\tilde{\rho}^{SA} = \frac{1}{3}\rho^{SA} + \frac{2}{3}\frac{\mathbb{I}}{d_S} \otimes \rho^A.$$

.

We show that $H_\infty(\tilde{\rho}^{SA}|\tilde{\rho}^A) = H_\infty(\tilde{\rho}^{SA}|\rho^A) \geqslant t$:

$$\begin{aligned}
\frac{\langle\psi|\tilde{\rho}^{SA}|\psi\rangle}{\langle\psi|\mathbb{I}^S \otimes \rho^A|\psi\rangle} &= \frac{1}{3}\frac{\langle\psi|\rho^{SA}|\psi\rangle}{\langle\psi|\mathbb{I}^S \otimes \rho^A|\psi\rangle} + \frac{2}{3}\frac{\langle\psi|\frac{\mathbb{I}^S}{d_S} \otimes \rho^A|\psi\rangle}{\langle\psi|\mathbb{I}^S \otimes \rho^A|\psi\rangle} \\
&\leqslant \frac{1}{3}2^{-(t-1)} + \frac{2}{3}\frac{1}{2^n} \\
&= \frac{2}{3}\left(2^{-t} + \frac{1}{2^n}\right) \\
&\leqslant \frac{2}{3}\left(2^{-t} + \frac{2^{-t}}{2}\right) \\
&= 2^{-t}.
\end{aligned}$$

Since $\left\|\mathcal{E}(\rho^{SA}) - \Omega^{S'} \otimes \rho^A\right\|_1 > 6\varepsilon$, we know that there exists an adversary that can distinguish $\mathcal{E}(\rho^{SA})$ from $\Omega^{S'} \otimes \rho^A$ 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 $\mathcal{E}(\rho^{SA})$ and with probability η_2 when it is given $\Omega^{S'} \otimes \rho^A$. We then have $\frac{1}{2}(\eta_1 + \eta_2) > \frac{1}{2} + \frac{3}{2}\varepsilon$.

Now, consider the following interpretation of $\tilde{\rho}^{SA}$:

$$\tilde{\rho}^{SA} = \frac{1}{3}\sigma_1^{SA} + \frac{1}{3}\sigma_2^{SA} + \frac{1}{3}\sigma_3^{SA} \tag{3.30}$$

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

First of all, it is clear that by having access only to the adversary'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 $\tilde{\rho}^{SA}$. It is clear that A's best strategy is to try to distinguish between $\mathcal{E}(\rho^{SA})$ and $\Omega^{S'} \otimes \rho^A$ and return 1 when it gets $\mathcal{E}(\rho^{SA})$ and randomly return either 2 or 3 when it gets $\Omega^{S'} \otimes \rho^A$. We then have:

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

Finally we get

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

a violation of entropic security. QED

We have now generalized the definitions of §2 and have established that entropic-indistinguishability and entropic-security are also equivalent in the generalized model. We shall now use entropic-indistinguishability to prove that two different encryption schemes are in fact secure according to entropic security in the generalized model.

3.2 ciphers

Both encryption schemes from Section 2.2 are still secure in this generalized framework.

We shall first show three technical lemmas which will be useful as intermediate steps for both encryption schemes security proofs.

Lemma 13 *For any operator A, B, C and D, the following is true:* $\mathrm{Tr}\left[AB \otimes CD\right] = \mathrm{Tr}\left[BA \otimes CD\right]$

Proof:
We start from $\mathrm{Tr}\left[AB \otimes CD\right]$ and massage it until we get the result

$$\mathrm{Tr}\left[AB \otimes CD\mathbb{I}\right] = \mathrm{Tr}\left[(A \otimes CD)(B \otimes \mathbb{I})\right] = \mathrm{Tr}\left[(B \otimes \mathbb{I})(A \otimes CD)\right] = \mathrm{Tr}\left[BA \otimes CD\right].$$

QED

Lemma 14 *The partial trace operator commutes with operators on the space not being traced out, or*

$$\mathrm{Tr}_S\left[(E^S \otimes F^A)\sigma^{SA}\right] = F^A \mathrm{Tr}_S\left[(E^S \otimes \mathbb{I}^A)\sigma^{SA}\right].$$

Proof:

$$\begin{aligned}
\mathrm{Tr}_S\left[(E^S \otimes F^A)\sigma^{SA}\right] &= \sum_i \langle i|^S \otimes \mathbb{I}^A (E^S \otimes F^A)\sigma^{SA}|i\rangle^S \otimes \mathbb{I}^A \\
&= \sum_i \langle i|^S \otimes \mathbb{I}^A (\mathbb{I}^S \otimes F^A)(E^S \otimes \mathbb{I}^A)\sigma^{SA}|i\rangle^S \otimes \mathbb{I}^A \\
&= \sum_i \langle i|^S \otimes F^A (E^S \otimes \mathbb{I}^A)\sigma^{SA}|i\rangle^S \otimes \mathbb{I}^A \\
&= \sum_i F^A (\langle i|^S \otimes \mathbb{I}^A (E^S \otimes \mathbb{I}^A)\sigma^{SA}|i\rangle^S \otimes \mathbb{I}^A) \\
&= F^A \mathrm{Tr}_S\left[(E^S \otimes \mathbb{I}^A)\sigma^{SA}\right].
\end{aligned}$$

QED

Note that in this last Lemma, E and F can be any kind of operator. It is well known that the Pauli operators $X^u Z^v$ form a basis for the linear space of complex matrices. We can furthermore say that the operators $X^u Z^v/\sqrt{d}$, where d is the dimension of the operators, form an orthonormal basis according to the Hilbert-Schmidt inner product given by $\langle A, B\rangle = \mathrm{Tr}\left[A^\dagger B\right]$. Therefore any operator can be decomposed in this basis. For any operator ρ, we can write

$$\rho = \sum_{u,v} \alpha_{u,v} \frac{X^u Z^v}{\sqrt{d}}. \tag{3.31}$$

We can also compute the $\alpha_{u,v}$ using the following formula

$$\alpha_{u,v} = \mathrm{Tr}\left[\frac{Z^v X^u}{\sqrt{d}} \rho\right]. \tag{3.32}$$

Note that the last two equations are true for any orthonormal basis $\{E_i\}_i$. Then we can write that

$$\rho = \sum_i \alpha_i E_i \tag{3.33}$$

where

$$\alpha_i = \mathrm{Tr}\left[E_i^\dagger \rho\right]. \tag{3.34}$$

Lemma 15 *For every bi-partite state σ^{SA}, we have*

$$\sigma^{SA} = \sum_{uv} \frac{X^u Z^v}{\sqrt{d_S}} \otimes \mathrm{Tr}_S\left[\left(\frac{Z^v X^u}{\sqrt{d_S}} \otimes \mathbb{I}\right) \sigma^{SA}\right].$$

Proof:

Let $\{E_j\}_j$ be any orthonormal basis for the space $\mathcal{L}(\mathcal{H}_A)$. Then we can write

$$\begin{aligned}
\sigma^{SA} &\overset{(a)}{=} \sum_{uvj} \frac{X^u Z^v}{\sqrt{d_S}} \otimes E_j \operatorname{Tr}\left[\left(\frac{Z^v X^u}{\sqrt{d_S}} \otimes E_j^\dagger\right) \sigma^{SA}\right] \\
&\overset{(b)}{=} \sum_{uvj} \frac{X^u Z^v}{\sqrt{d_S}} \otimes E_j \operatorname{Tr}\left[E_j^\dagger \operatorname{Tr}_S\left[\left(\frac{Z^v X^u}{\sqrt{d_S}} \otimes \mathbb{I}\right) \sigma^{SA}\right]\right] \\
&= \sum_{uv} \frac{X^u Z^v}{\sqrt{d_S}} \otimes \left\{\sum_j E_j \operatorname{Tr}\left[E_j^\dagger \operatorname{Tr}_S\left[\left(\frac{Z^v X^u}{\sqrt{d_S}} \otimes \mathbb{I}\right) \sigma^{SA}\right]\right]\right\} \\
&\overset{(c)}{=} \sum_{uv} \frac{X^u Z^v}{\sqrt{d_S}} \otimes \operatorname{Tr}_S\left[\left(\frac{Z^v X^u}{\sqrt{d_S}} \otimes \mathbb{I}\right) \sigma^{SA}\right],
\end{aligned}$$

where (a) follows by equations (3.31) to (3.34), (b) follows by Lemma 14 and remembering that $\operatorname{Tr}\left[\rho^{SA}\right] = \operatorname{Tr}\left[\operatorname{Tr}_S\left[\rho^{SA}\right]\right]$ and finally (c) is justified by equations (3.33) and (3.34). QED

The proofs of security for both encryption schemes will use Lemma 5.1.3 of Renner's Thesis [37]. We reproduce the Lemma here:

Lemma 16 *Let S be a Hermitian operator and let σ be any positive definite operator. Then*

$$\|S\|_1 \leqslant \sqrt{\operatorname{Tr}[\sigma] \operatorname{Tr}[S\sigma^{-1/2} S\sigma^{-1/2}]}.$$

Let us define the operator $\tilde{\rho}^{SA} \triangleq \rho^{SA} - \frac{\mathbb{I}^S}{d_S} \otimes \rho^A$ and observe that for any encryption schemes that maps the identity to the identity, albeit not necessarily in the same space, we can write $\mathcal{E}(\tilde{\rho}^{SA}) = \mathcal{E}(\rho^{SA}) - \frac{\mathbb{I}^{S'}}{d_{S'}} \otimes \rho^A$. Using Lemma 16, and fixing σ in that Lemma to be $\mathbb{I}^{S'} \otimes \rho^A$, then we can write:

$$\begin{aligned}
\left\|\mathcal{E}(\rho^{SA}) - \frac{\mathbb{I}^{S'}}{d_{S'}} \otimes \rho^A\right\|_1 &= \left\|\mathcal{E}(\rho^{\tilde{S}A})\right\|_1 \qquad (3.35) \\
&\leqslant \sqrt{d_{S'} \operatorname{Tr}\left[\mathcal{E}(\tilde{\rho}^{SA})(\mathbb{I}^{S'} \otimes \rho^{A^{-1/2}})\mathcal{E}(\tilde{\rho}^{SA})(\mathbb{I}^{S'} \otimes \rho^{A^{-1/2}})\right]}.
\end{aligned}$$

Scheme based on δ-biased set

Theorem 11 *If $H_\infty(\rho^{SA}|\rho^A) \geqslant t$, then the Ambainis-Smith scheme*

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

where B is a δ-biased set, is (t,ε)-entropically indistinguishable using $n - t + 2\log n + 2\log(\frac{1}{\varepsilon}) + 2$ bits of key to index the set B, where $n = \log d_S$.

Proof:

Let us assume for now that ρ^A is full rank, that is ρ^A is invertible (we shall fix this later on for all states). We start from Lemma 15 and write

$$\tilde{\rho}^{SA} = \sum_{uv} \frac{X^u Z^v}{\sqrt{d_S}} \otimes \tilde{M}_{uv}, \tag{3.36}$$

where $\tilde{M}_{uv}$ is a shortcut notation for $\mathrm{Tr}_S\left[\left(\frac{Z^v X^u}{\sqrt{d_S}} \otimes \mathbb{I}^A\right)\tilde{\rho}^{SA}\right]$. We shall also write M_{uv} instead of $\mathrm{Tr}_S\left[\left(\frac{Z^v X^u}{\sqrt{d_S}} \otimes \mathbb{I}^A\right)\rho^{SA}\right]$. We can now apply a δ-biased scheme, defined by the δ-biased set B, to this operator and get

$$\begin{aligned}
\mathcal{E}(\tilde{\rho}^{SA}) &= \sum_{uv} \mathcal{E}\left(\frac{X^u Z^v}{\sqrt{d_S}}\right) \otimes \tilde{M}_{uv} \\
&= \sum_{uvab} \frac{1}{|B|}\left(X^a Z^b \frac{X^u Z^v}{\sqrt{d_S}} Z^b X^a\right) \otimes \tilde{M}_{uv} \\
&\overset{(a)}{=} \sum_{uvab} \frac{1}{|B|}\left(X^a Z^b Z^b X^a (-1)^{a\odot v}(-1)^{b\odot u}\frac{X^u Z^v}{\sqrt{d_S}}\right) \otimes \tilde{M}_{uv} \\
&= \sum_{uv} \alpha_{uv} \frac{X^u Z^v}{\sqrt{d_S}} \otimes \tilde{M}_{uv},
\end{aligned} \tag{3.37}$$

where $\alpha_{uv} = \frac{1}{|B|}\sum_{a||b\in B}(-1)^{a||b\odot v||u}$ and where (a) follows by the anti-commuting property of Pauli operators (i.e $XZ = -ZX$, or $X^a Z^b = (-1)^{a\odot b} Z^b X^a$). Since B is δ-biased, we can conclude that for all $v||u \neq 0$ we have that $|\alpha_{uv}| \leqslant \delta$. For $uv = 0$, observe that

$$\tilde{M}_{00} = \frac{1}{\sqrt{d_S}} \mathrm{Tr}_S\left[\rho^{SA} - \frac{\mathbb{I}^S}{d_S} \otimes \rho^A\right] = 0^A, \tag{3.38}$$

the zero matrix.

Now, continuing with (3.35) we can write

$$\begin{aligned}
&\mathrm{Tr}\Big[\Big(\mathcal{E}(\tilde{\rho}^{SA})(\mathbb{I}^S\otimes\sqrt[-2]{\rho^A})\Big)^2\Big] \\
&\qquad = \mathrm{Tr}\left[\left(\sum_{uv}\alpha_{uv}\frac{X^uZ^v}{\sqrt{d_S}}\otimes\tilde{M}_{uv}\right)\left(\sum_{rs}\alpha_{rs}\frac{X^rZ^s}{\sqrt{d_S}}\otimes\sqrt[-2]{\rho^A}\tilde{M}_{rs}\ \sqrt[-2]{\rho^A}\right)\right] \\
&\qquad \overset{(a)}{=} \mathrm{Tr}\left[\left(\sum_{uv}\alpha_{uv}\frac{X^uZ^v}{\sqrt{d_S}}\otimes\tilde{M}_{uv}\right)\left(\sum_{rs}\alpha_{rs}\frac{Z^sX^r}{\sqrt{d_S}}\otimes\sqrt[-2]{\rho^A}\tilde{M}^\dagger_{rs}\ \sqrt[-2]{\rho^A}\right)\right] \\
&\qquad \overset{(b)}{=} \mathrm{Tr}\left[\sum_{uv}\alpha^2_{uv}\frac{\mathbb{I}^S}{d_S}\otimes\tilde{M}_{uv}\rho^{A^{-1/2}}\tilde{M}^\dagger_{uv}\rho^{A^{-1/2}}\right] \\
&\qquad \overset{(c)}{\leqslant} \delta^2\mathrm{Tr}\left[\sum_{uv}\frac{\mathbb{I}^S}{d_S}\otimes\tilde{M}_{uv}\rho^{A^{-1/2}}\tilde{M}^\dagger_{uv}\rho^{A^{-1/2}}\right] \\
&\qquad \overset{(d)}{\leqslant} \delta^2\mathrm{Tr}\left[\sum_{uv}\frac{\mathbb{I}^S}{d_S}\otimes M_{uv}\rho^{A^{-1/2}}M^\dagger_{uv}\rho^{A^{-1/2}}\right] \\
&\qquad =\delta^2\mathrm{Tr}\left[\left(\sum_{uv}\frac{X^uZ^v}{\sqrt{d_S}}\otimes M_{uv}\right)\left(\sum_{rs}\frac{Z^sX^r}{\sqrt{d_S}}\otimes\sqrt[-2]{\rho^A}M^\dagger_{rs}\ \sqrt[-2]{\rho^A}\right)\right] \\
&\qquad \overset{(e)}{=} \delta^2\mathrm{Tr}\left[\rho^{SA}\left(\left[\mathbb{I}^S\otimes\ \sqrt[-2]{\rho^A}\right]\rho^{SA}\left[\mathbb{I}^S\otimes\ \sqrt[-2]{\rho^A}\right]\right)^\dagger\right] \\
&\qquad \overset{(f)}{=} \delta^2\mathrm{Tr}\left[\rho^{SA}\left(\left[\mathbb{I}^S\otimes\ \sqrt[-2]{\rho^A}\right]\rho^{SA}\left[\mathbb{I}^S\otimes\ \sqrt[-2]{\rho^A}\right]\right)\right] \\
&\qquad \overset{(g)}{\leqslant} \delta^2\mathrm{Tr}\left[\rho^{SA}2^{-t}\mathbb{I}^{SA}\right] \\
&\qquad =\delta^2 2^{-t}.
\end{aligned}$$

We can justify step (a) since for any Hermitian operator S and any operator R we have $R^\dagger SR$ is Hermitian; this is obvious by checking that $(R^\dagger SR)^\dagger = (R^\dagger S^\dagger R^{\dagger\dagger}) = (R^\dagger SR)$. Here $R = (\mathbb{I}^S\otimes\sqrt[-2]{\rho^A})$ and $S = \mathcal{E}(\tilde{\rho}^{SA})$. Step (b) follows since $(A\otimes B)(C\otimes D) = (AC\otimes BD)$ and that pauli operators are orthonormal according to $\mathrm{Tr}\left[(X^uZ^v)(Z^sX^r)\right] = d_S\delta_{vs}\delta_{ur}$, where δ_{ab} is the dirac δ-function. Step (c) follows from the comments after (3.37) and from the fact that every term in the sum is positive. This is easy to see by observing that

$$\mathrm{Tr}\left[\sum_{uv}\frac{\mathbb{I}^S}{d_S}\otimes\tilde{M}_{uv}\rho^{A^{-1/2}}\tilde{M}^\dagger_{uv}\rho^{A^{-1/2}}\right] = \mathrm{Tr}\left[\sum_{uv}\frac{\mathbb{I}^S}{d_S}\otimes\rho^{A^{-1/4}}\tilde{M}_{uv}\rho^{A^{-1/2}}\tilde{M}^\dagger_{uv}\rho^{A^{-1/4}}{}^\dagger\right],$$

where we used Lemma 13. Since every operator in this equation is Hermitian, it follows that on the right hand side we simply have the conjugation of $\rho^{A^{-1/2}}$, which is positive, by $\rho^{A^{-1/4}}\tilde{M}_{uv}$ and as noted in the comment justifying (a), this is Hermitian. It is also positive, since for any $|x\rangle$ we have that $\langle x|\rho^{A^{-1/4}}\tilde{M}_{uv}\rho^{A^{-1/2}}\tilde{M}_{uv}^{\dagger}\rho^{A^{-1/4^{\dagger}}}|x\rangle = \langle y|\rho^{A^{-1/2}}|y\rangle$, where $|y\rangle = \tilde{M}_{uv}^{\dagger}\rho^{A^{-1/4^{\dagger}}}|x\rangle$, which is positive.

Step (d) needs a more complex justification. Essentially by removing the tilde, we are only adding a tiny number to the right hand side.

Let $N_{uv} = \mathrm{Tr}_S\left[\left(\frac{Z^v X^u}{\sqrt{d_S}} \otimes \mathbb{I}^A\right)\frac{\mathbb{I}^S}{d_S} \otimes \rho^A\right]$. Therefore, by definition we can write that $\tilde{M}_{uv} = (M_{uv} - N_{uv})$. Hence we have that

$$
\begin{aligned}
\mathrm{Tr}\Bigg[\sum_{uv}\frac{\mathbb{I}^S}{d_S} &\otimes \tilde{M}_{uv}\ \sqrt[-2]{\rho^A}\tilde{M}_{uv}^{\dagger}\ \sqrt[-2]{\rho^A}\Bigg] \\
&= \mathrm{Tr}\left[\mathrm{Tr}_S\left[\sum_{uv}\frac{\mathbb{I}^S}{d_S} \otimes \tilde{M}_{uv}\ \sqrt[-2]{\rho^A}\tilde{M}_{uv}^{\dagger}\ \sqrt[-2]{\rho^A}\right]\right] \\
&= \mathrm{Tr}\left[\mathrm{Tr}_S\left[\sum_{uv}\frac{\mathbb{I}^S}{d_S} \otimes (M_{uv}- N_{uv})\ \sqrt[-2]{\rho^A}(M_{uv}- N_{uv})\ \sqrt[-2]{\rho^A}\right]\right] \\
&= \sum_{uv}\mathrm{Tr}\left[(M_{uv} - N_{uv})\ \sqrt[-2]{\rho^A}(M_{uv} - N_{uv})\ \sqrt[-2]{\rho^A}\right],
\end{aligned}
\tag{3.39}
$$

where the last expression is simply equal to

$$
\begin{aligned}
\mathrm{Tr}&\left[M_{uv}\ \sqrt[-2]{\rho^A}M_{uv}\ \sqrt[-2]{\rho^A}\right] \\
&+ \mathrm{Tr}\left[-M_{uv}\ \sqrt[-2]{\rho^A}N_{uv}\ \sqrt[-2]{\rho^A} - N_{uv}\ \sqrt[-2]{\rho^A}M_{uv}\ \sqrt[-2]{\rho^A} + N_{uv}\ \sqrt[-2]{\rho^A}N_{uv}\ \sqrt[-2]{\rho^A}\right].
\end{aligned}
\tag{3.40}
$$

Since the Trace operator allows rotation we can rewrite the previous equation this way

$$
\begin{aligned}
\mathrm{Tr}&\left[M_{uv}\ \sqrt[-2]{\rho^A}M_{uv}\ \sqrt[-2]{\rho^A}\right] \\
&+ \mathrm{Tr}\left[-2M_{uv}\ \sqrt[-2]{\rho^A}N_{uv}\ \sqrt[-2]{\rho^A} + N_{uv}\ \sqrt[-2]{\rho^A}N_{uv}\ \sqrt[-2]{\rho^A}\right].
\end{aligned}
\tag{3.41}
$$

Note that $M_{00} = N_{00} = \rho^A/\sqrt{d_S}$. For any other $uv \neq 00$, we use the fact that a Pauli operator is an observable with two projectors having eigen-values $+1$ and -1. Fix any u and v and rewrite $\frac{Z^v X^u}{\sqrt{d_S}} = \mathsf{P}_+ - \mathsf{P}_-$, where the P_- and P_+ are the eigen-spaces of the Pauli operator and $\operatorname{rank}(\mathsf{P}_+) = \operatorname{rank}(\mathsf{P}_-) = d_S/2$. Just ignore the $\sqrt{d_S}$ as it will not matter. Hence there exists a basis $\{|p_i\rangle\}_i$ such that $\sum_i |p_i\rangle\langle p_i| = \mathbb{I}$ and two sets of indices, E_+ and E_- (of equal size), partitioning the indices i such that $\mathsf{P}_+ = \sum_{i\in E_+} |p_i\rangle\langle p_i|$ and $\mathsf{P}_- = \sum_{i\in E_-} |p_i\rangle\langle p_i|$. Let us compute N_{uv}.

$$
\begin{aligned}
&\mathrm{Tr}_S\Big[(\mathsf{P}_+ - \mathsf{P}_-) \otimes \mathbb{I}^A(\frac{\mathbb{I}^S}{d_S} \otimes \rho^A)\Big] \\
&\qquad =\mathrm{Tr}_S\left[\left(\sum_{i\in E_+} |p_i\rangle\langle p_i| \frac{\mathbb{I}^S}{d_S} - \sum_{j\in E_-} |p_j\rangle\langle p_j| \frac{\mathbb{I}^S}{d_S}\right) \otimes \rho^A\right] \\
&\qquad =\sum_{k\in E_-\cup E_+} \langle p_k| \otimes \mathbb{I}^A \left[\left(\sum_{i\in E_+} |p_i\rangle\langle p_i| \frac{\mathbb{I}^S}{d_S} - \sum_{j\in E_-} |p_j\rangle\langle p_j| \frac{\mathbb{I}^S}{d_S}\right) \otimes \rho^A\right] |p_k\rangle \otimes \mathbb{I}^A \\
&\qquad =\sum_{\substack{k\in E_-\cup E_+ \\ i\in E_+, j\in E_-}} \left(\langle p_k|\, |p_i\rangle\langle p_i| \frac{\mathbb{I}^S}{d_S} |p_k\rangle - \langle p_k|\, |p_j\rangle\langle p_j| \frac{\mathbb{I}^S}{d_S} |p_k\rangle\right) \otimes \mathbb{I}^A \rho^A \mathbb{I}^A \\
&\qquad =\left(\frac{d_S}{2} - \frac{d_S}{2}\right) \otimes \rho^A \\
&\qquad =0 \otimes \rho^A \\
&\qquad =0^A,
\end{aligned}
$$

the zero matrix. Hence

$$
\begin{aligned}
\mathrm{Tr}\left[\sum_{uv} \frac{\mathbb{I}^S}{d_S} \otimes \tilde{M}_{uv} \rho^{A^{-1/2}} \tilde{M}^\dagger_{uv} \rho^{A^{-1/2}}\right] &= \mathrm{Tr}\left[\sum_{uv} \frac{\mathbb{I}^S}{d_S} \otimes M_{uv} \rho^{A^{-1/2}} M^\dagger_{uv} \rho^{A^{-1/2}}\right] - \frac{\rho^A}{d_S} \\
&\leqslant \mathrm{Tr}\left[\sum_{uv} \frac{\mathbb{I}^S}{d_S} \otimes M_{uv} \rho^{A^{-1/2}} M^\dagger_{uv} \rho^{A^{-1/2}}\right],
\end{aligned}
$$

since, obviously, ρ^A is positive and only the $uv = 00$ terms of N_{uv} survive.

Step (e) follows by applying Lemma 15 backwards. Step (f) follows from the same reason as step (a). Step (g) follows by applying the conditional min-entropy bound, that is: $\rho^{SA} \leqslant 2^{-t}\mathbb{I}^S \otimes \rho^A \implies (\mathbb{I}^S \otimes \sqrt[-2]{\rho^A})\rho^{SA}(\mathbb{I}^S \otimes \sqrt[-2]{\rho^A}) \leqslant 2^{-t}\mathbb{I}^{SA}$ since if $B \leqslant C$ then $\sqrt{A}B\sqrt{A} \leqslant \sqrt{A}C\sqrt{A}$, see §5 in [9], therefore $\mathrm{Tr}[AB] \leqslant \mathrm{Tr}[AC]$.

Recapitulating, we just computed the following:

$$\left\|\mathcal{E}(\rho^{SA}) - \frac{\mathbb{I}^{S'}}{d_{S'}} \otimes \rho^A\right\|_1 \leqslant \sqrt{d_S\delta^2 2^{-t}} \leqslant \epsilon, \tag{3.42}$$

and from the proof of Theorem 5, we already know that setting $\delta = \sqrt{2^t\epsilon^2/d_S}$ we can construct a δ-biased set of size $\mathcal{O}(\frac{n^2 2^{n-t}}{\epsilon^2})$ that requires $n-t+2\log(n)+2\log(1/\epsilon)+\mathcal{O}(1)$ bits of key to index.

We still need to show that this proof technique also works for operators ρ^A which are not invertible. We will use the fact that invertible matrices are dense in the space of all matrices. Let us define

$$\rho_\gamma^{SA} = (1-\gamma)\rho^{SA} + \gamma\frac{\mathbb{I}^{SA}}{d_{SA}},$$

where γ takes values between 0 and 1.The operator ρ_γ^{SA} is thus only ρ^{SA} to which we added some noise. The first thing to observe is that

$$\left\|\rho^{SA} - \rho_\gamma^{SA}\right\|_1 \leqslant 2\gamma,$$

hence, for small γ's ρ_γ^{SA} is a good approximation to ρ^{SA}. And of course, since trace preserving POVM cannot increase distance, we have that

$$\left\|\mathcal{E}(\rho^{SA}) - \mathcal{E}(\rho_\gamma^{SA})\right\|_1 \leqslant 2\gamma,$$

which intuitively tells us that for small γ no adversary should do the difference between the two with good probability. Hence if $\mathcal{E}$ is secure for ρ_γ^{SA} for small γ's, it should be secure for ρ^{SA}.

The next thing to observe is that ρ_γ^{SA} has full rank. This is easy to see since ρ^{SA} and the perfectly mixed state commute. Thus no eigen-value of ρ_γ^{SA} can be zero, they are all at least γ/d_{SA}. Remembering the fact that the partial trace is a linear operator and applying the same reasoning, we conclude that $\rho_\gamma^A = \mathrm{Tr}_S\left[\rho_\gamma^{SA}\right]$ is also an invertible operator.

Finally, we can write the following:

$$\lim_{\gamma\to 0}\left\|\mathcal{E}(\rho_\gamma^{SA}) - \frac{\mathbb{I}^S}{d_S}\otimes\rho_\gamma^A\right\|_1 = \left\|\mathcal{E}(\rho^{SA}) - \frac{\mathbb{I}^S}{d_S}\otimes\rho^A\right\|_1. \tag{3.43}$$

Hence, since (3.42) is true for all γ, we can conclude that $\mathcal{E}$ is (t,ϵ)-indistinguishable. Therefore using Theorem 9 we conclude that the Ambainis-Smith scheme is $(t+1, 2\epsilon)$-entropically secure using $n - t + 2\log(n) + 2\log(1/\epsilon) + \mathcal{O}(1)$ bits of key.

QED

Scheme based on XOR-Universal functions

We need to observe a few things first. Let us start by denoting the perfect encryption scheme by $\mathcal{E}^p$ and note that

$$\mathcal{E}^p(\rho) = \sum_{e,f}\frac{1}{d^2}Z^fX^e\rho X^eZ^f = \frac{\mathbb{I}}{d}.$$

For such a scheme we can write

$$\begin{aligned}\mathcal{E}^p(\tilde{\rho}^{SA}) &= \sum_{uv}\mathcal{E}^p\left(\frac{X^uZ^v}{\sqrt{d_S}}\right)\otimes\tilde{M}_{uv} &(3.44)\\ &= \sum_{uvef}\frac{1}{d_S^2}Z^fX^e\frac{X^uZ^v}{\sqrt{d_S}}X^eZ^f\otimes\tilde{M}_{uv}. &(3.45)\end{aligned}$$

independently, we can also write

$$\begin{aligned}\mathcal{E}^p(\tilde{\rho}^{SA}) &= \frac{\mathbb{I}^S}{d_S}\otimes\rho^A - \frac{\mathbb{I}^S}{d_S}\otimes\rho^A &(3.46)\\ &= 0, &(3.47)\end{aligned}$$

which we know since the scheme is perfect, see [3]. We also need to rethink equation (3.35). In the case of the XOR-universal scheme, $\mathcal{E}$ does not preserve length. We shall consider that $\mathcal{E}$ takes two inputs and has two outputs. Hence $\mathcal{E}$ takes two states for inputs: $\mathbb{I}^{S'}/d_{S'}$ and ρ^{SA}. Here $\rho^{\tilde{S}A} = \mathbb{I}^{S'}/d_{S'} \otimes \rho^{SA} - \mathbb{I}^{S'S}/d_{S'S} \otimes \rho^{A}$ and we use $\sigma = \mathbb{I}^{S} \otimes \mathbb{I}^{S'}/d_{S'} \otimes \rho^{A}$ instead of $\sigma = \mathbb{I}^{S} \otimes \rho^{A}$ in Lemma 16. So we can write:

$$\begin{aligned} \left\| \mathcal{E}(\mathbb{I}^{S'} \otimes \rho^{SA}) - \frac{\mathbb{I}^{S'S}}{d_{S'S}} \otimes \rho^{A} \right\|_1 &= \left\| \mathcal{E}(\rho^{\tilde{S}A}) \right\|_1 \\ &= \sqrt{d_S \mathrm{Tr}\left[\left(\mathcal{E}(\tilde{\rho}^{SA})(\sqrt[-2]{\frac{\mathbb{I}^{S'}}{d_{S'}}} \otimes \mathbb{I}^{S} \otimes \sqrt[-2]{\rho^{A}}) \right)^2 \right]}. \end{aligned} \tag{3.48}$$

Finally, we can, in this setup, rewrite Lemma 15 this way:

$$\frac{\mathbb{I}^{S'}}{d_{S'}} \otimes \sigma^{SA} = \sum_{uv} \frac{\mathbb{I}^{S'}}{d_{S'}} \otimes \frac{X^u Z^v}{\sqrt{d_S}} \otimes M_{uv}. \tag{3.49}$$

We shall also introduce another notation for the sake of compactness. We shall write Π_v^u instead of $X^u Z^v$. Observe that the anti-commutation law for Pauly operator takes the form:

$$\Pi_d^c \Pi_v^u = (-1)^{a\|b \odot c\|d} \Pi_v^u \Pi_d^c. \tag{3.50}$$

Theorem 12 *Let H_{2n} be a strongly-XOR-universal family of functions. Consider the super-operator $\mathcal{E}_k(\rho) = \frac{1}{|I|} \sum_{i \in I} |i\rangle\langle i|^{S'} \otimes (X^a Z^b \otimes \mathbb{I}^S) \rho^{SA} (Z^b X^a \otimes \mathbb{I}^S)$, where S' is an ancillary system, $a\|b = h_i(k)$, $|a| = |b| = n$, $h_i \in \mathsf{H}_{2n}$ and k is the secret key selected uniformly at random from a set $K \subseteq \{0,1\}^{2n}$. Then $\mathcal{E}$ is (t, ϵ)-indistinguishable if $\log |K| \geqslant n - t + 1 + 2\log(1/\epsilon)$. This scheme is not length preserving since the ancillary system S' is part of the cipher text.*

Proof:

We start, as in the δ-biased case with (3.48).

$$\begin{aligned}
&\operatorname{Tr}\left[\mathcal{E}(\tilde{\rho}^{SA})(\sqrt{d_{S'}}\mathbb{I}^{SS'} \otimes \sqrt[-2]{\rho^A})\mathcal{E}(\tilde{\rho}^{SA})(\sqrt{d_{S'}}\mathbb{I}^{SS'} \otimes \sqrt[-2]{\rho^A})\right] \\
&\quad \overset{(a)}{=} \operatorname{Tr}\Bigg[\left(\sum_{iuvk} \frac{1}{|K|}\frac{F_i^{S'}}{d_{S'}} \otimes \Pi_b^a \frac{\Pi_v^u}{\sqrt{d_S}}\Pi_b^{a\dagger} \otimes \tilde{M}_{uv}\right) \\
&\qquad\qquad \cdot \left(\sum_{jrsk'} \frac{d_{S'}}{|K|}\frac{F_j^{S'}}{d_{S'}} \otimes \Pi_d^c \frac{\Pi_s^r}{\sqrt{d_S}}\Pi_d^{c\dagger} \otimes \sqrt[-2]{\rho^A}\tilde{M}_{rs} \sqrt[-2]{\rho^A}\right)\Bigg] \\
&\quad \overset{(b)}{=} \operatorname{Tr}\Bigg[\left(\sum_{iuvk} \frac{1}{|K|}\frac{F_i^{S'}}{d_{S'}} \otimes \Pi_b^a \frac{\Pi_v^u}{\sqrt{d_S}}\Pi_b^{a\dagger} \otimes \tilde{M}_{uv}\right) \\
&\qquad\qquad \cdot \left(\sum_{jrsk'} \frac{1}{|K|}\frac{F_j^{S'}}{d_{S'}} \otimes \Pi_d^c \frac{\Pi_s^r}{\sqrt{d_S}}\Pi_d^{c\dagger} \otimes \sqrt[-2]{\rho^A}\tilde{M}_{rs}^\dagger \sqrt[-2]{\rho^A}\right)\Bigg] \\
&\quad \overset{(c)}{=} \operatorname{Tr}\left[\left(\sum_{iuvrskk'} \frac{1}{|K|^2}\frac{F_i^{S'}}{d_{S'}} \otimes \Pi_b^a \frac{\Pi_v^u}{\sqrt{d_S}}\Pi_b^{a\dagger}\Pi_d^c \frac{\Pi_s^r}{\sqrt{d_S}}\Pi_d^{c\dagger} \otimes \tilde{M}_{uv} \sqrt[-2]{\rho^A}\tilde{M}_{rs}^\dagger \sqrt[-2]{\rho^A}\right)\right] \\
&\quad \overset{(d)}{=} \operatorname{Tr}\left[\left(\sum_{iuvrskk'} \frac{1}{|K|^2}\frac{F_i^{S'}}{d_{S'}} \otimes \Pi_d^{c\dagger}\Pi_b^a \frac{\Pi_v^u}{\sqrt{d_S}}\Pi_b^{a\dagger}\Pi_d^c \frac{\Pi_s^r}{\sqrt{d_S}} \otimes \tilde{M}_{uv} \sqrt[-2]{\rho^A}\tilde{M}_{rs}^\dagger \sqrt[-2]{\rho^A}\right)\right] \\
&\quad \overset{(e)}{=} \operatorname{Tr}\left[\left(\sum_{iuvrskk'} \frac{1}{|K|^2}\frac{F_i^{S'}}{d_{S'}} \otimes \Pi_f^e \frac{\Pi_v^u}{\sqrt{d_S}}\Pi_f^{e\dagger} \frac{\Pi_s^r}{\sqrt{d_S}} \otimes \tilde{M}_{uv} \sqrt[-2]{\rho^A}\tilde{M}_{rs}^\dagger \sqrt[-2]{\rho^A}\right)\right],
\end{aligned} \tag{3.51}$$

where in (a) the symbol F_i is a shortcut for $|i\rangle\langle i|$ and $a\|b = h_i(k)$ and $c\|d = h_j(k')$. Step (b) follows since, if A is Hermitian, then for any operator B we know that $C = BAB^\dagger$ is Hermitian. Step (c) follows since $|i\rangle\langle i|\,|j\rangle\langle j| = \delta_{ij}$ and the fact that $(A \otimes B)(C \otimes D) = (AC \otimes BD)$. Step (d) follows by Lemma 13. Step (e) follows since $\Pi_d^{c\dagger}\Pi_b^a = Z^dX^cX^aZ^b = (-1)^{d\odot c}(-1)^{d\odot a}X^cX^aZ^dZ^b = (-1)^{d\odot c}(-1)^{d\odot a}\Pi_f^e$, where $e\|f = (a \oplus c)\|(b \oplus d)$. Since this operation is done twice, the phase $(-1)^{d\odot c}(-1)^{d\odot a}$ is applied twice and thus cancels out.

We shall now split the last term into two according to $k = k'$ or $k \neq k'$.

$$\operatorname{Tr}\left[\left(\sum_{iuvrsk=k'} \frac{1}{|K|^2}\frac{F_i^{S'}}{d_{S'}} \otimes \Pi_f^e \frac{\Pi_v^u}{\sqrt{d_S}} \Pi_f^{e\,\dagger} \frac{\Pi_s^r}{\sqrt{d_S}} \otimes \tilde{M}_{uv} \sqrt[-2]{\rho^A} \tilde{M}_{rs}^\dagger \sqrt[-2]{\rho^A}\right)\right] \\ + \operatorname{Tr}\left[\left(\sum_{iuvrsk\neq k'} \frac{1}{|K|^2}\frac{F_i^{S'}}{d_{S'}} \otimes \Pi_f^e \frac{\Pi_v^u}{\sqrt{d_S}} \Pi_f^{e\,\dagger} \frac{\Pi_s^r}{\sqrt{d_S}} \otimes \tilde{M}_{uv} \sqrt[-2]{\rho^A} \tilde{M}_{rs}^\dagger \sqrt[-2]{\rho^A}\right)\right]. \tag{3.52}$$

We know by the definition of the XOR-universal-function, Definition 13, that when $k = k'$, then for all i we have that $e\|f = 0$. On the other hand, we know that, when $k \neq k$, the probability that $h_i(k) \oplus h_i(k') = e\|f$ is exactly $1/d_S^2$. We can thus write, after taking the partial trace on the S' system for both terms and remembering that $\sum_i F_i/d_{S'} = \mathbb{I}^{S'}/d_{S'}$:

$$\frac{1}{|K|}\operatorname{Tr}\left[\left(\sum_{uvrs} \frac{\Pi_v^u}{\sqrt{d_S}} \frac{\Pi_s^r}{\sqrt{d_S}} \otimes \tilde{M}_{uv} \sqrt[-2]{\rho^A} \tilde{M}_{rs}^\dagger \sqrt[-2]{\rho^A}\right)\right] \\ + \left(1 - \frac{1}{|K|}\right)\operatorname{Tr}\left[\left(\sum_{uvrsef} \frac{1}{d_S^2}\Pi_f^e \frac{\Pi_v^u}{\sqrt{d_S}} \Pi_f^{e\,\dagger} \frac{\Pi_s^r}{\sqrt{d_S}} \otimes \tilde{M}_{uv} \sqrt[-2]{\rho^A} \tilde{M}_{rs}^\dagger \sqrt[-2]{\rho^A}\right)\right]. \tag{3.53}$$

Now the first term goes to

$$\frac{1}{|K|}\operatorname{Tr}\left[\left(\sum_{uv} \frac{\mathbb{I}^S}{d_S} \otimes \tilde{M}_{uv} \sqrt[-2]{\rho^A} \tilde{M}_{uv}^\dagger \sqrt[-2]{\rho^A}\right)\right], \tag{3.54}$$

since Pauly operators are orthonormal according to the inner product $\operatorname{Tr}\left[\Pi_v^u \Pi_s^r\right] = d_S \delta_{ur} \delta_{vs}$. Now, just as in step (d) of equation (3.39) in the proof of Theorem 11, we can remove the $\sim$ on the M_{uv} and follow the proof of Theorem 11 from there to conclude that the first term is in fact inferior to $\frac{2^{-t}}{|K|}$.

What about the second term of equation 3.53? We can rewrite the term like this

$$\left(1 - \frac{1}{|K|}\right)\operatorname{Tr}\left[\left(\sum_{uvef} \frac{1}{d_S^2}\Pi_f^e \frac{\Pi_v^u}{\sqrt{d_S}} \Pi_f^{e\,\dagger} \otimes \tilde{M}_{uv}\right)\left(\sum_{rs} \frac{\Pi_s^r}{\sqrt{d_S}} \otimes \sqrt[-2]{\rho^A} \tilde{M}_{rs}^\dagger \sqrt[-2]{\rho^A}\right)\right]. \tag{3.55}$$

Now from equations (3.44) and (3.45) we can immediately see that the left term in the trace of the last equation is really $\mathcal{E}^p(\rho^{\tilde{S}A})$ and we know that this term, by definition, can only be zero. Hence the entire term (3.55) is zero.

From this we conclude that

$$\operatorname{Tr}\left[\mathcal{E}(\tilde{\rho}^{SA})(\sqrt[-2]{\frac{\mathbb{I}^{SS'}}{d_{S'}}} \otimes \sqrt[-2]{\rho^A})\mathcal{E}(\tilde{\rho}^{SA})(\sqrt[-2]{\frac{\mathbb{I}^{SS'}}{d_{S'}}} \otimes \sqrt[-2]{\rho^A})\right] \leqslant \frac{2^{-t}}{|K|} + 0 \tag{3.56}$$

and that

$$\left\|\mathcal{E}(\mathbb{I}^{S'} \otimes \rho^{SA}) - \frac{\mathbb{I}^{S'S}}{d_{S'S}} \otimes \rho^A\right\|_1 \leqslant \sqrt{d_S \frac{2^{-t}}{|K|}}. \tag{3.57}$$

The Theorem assumes that $\lg|k| \geqslant n - t + 2\lg(1/\epsilon)$ and taking exponentials $|K| \geqslant 2^n 2^{-t}/\epsilon^2$. Which means that, using the same limiting process, as in Theorem 11, from ρ_γ^{SA} to ρ^{SA} we can say

$$\left\|\mathcal{E}(\mathbb{I}^{S'} \otimes \rho^{SA}) - \frac{\mathbb{I}^{S'S}}{d_{S'S}} \otimes \rho^A\right\|_1 \leqslant \epsilon, \tag{3.58}$$

which is what we wanted. Hence $\mathcal{E}$ is (t, ϵ)-indistinguishable, therefore, using Theorem 9, it is $(t+1, 2\epsilon)$-entropically secure. QED

We have the same problem here that we had at the end of chapter §2, that is, if $i = 0$ in the XOR-universal function, not only is ρ^{SA} not encrypted, but we actually told so to the adversary. We shall use a different trick than in §2. Let $\mathcal{E}'$ be the XOR-universal encryption scheme where the function will never use $i = 0$ and let $\mathcal{E}$ be the scheme from Theorem 12. Let us compute

$$\Delta = \left\|\mathcal{E}(\rho^{SA}) - \mathcal{E}'(\rho^{SA})\right\|_1. \tag{3.59}$$

The only thing that changes between the two schemes is the probability with which a given value i is chosen in the XOR-universal-function. Thus,

$$\Delta = \frac{1}{2^{2n}} \cdot 1 + 2^{2n} - 1\left(\frac{1}{2^{2n} - 1} - \frac{1}{2^{2n}}\right), \tag{3.60}$$

where the first term of the right hand side is the probability difference for $i = 0$ and the right most term is the probability difference for all other values. One can convince himself using high school algebra that

$$2^{2n} - 1\left(\frac{1}{2^{2n}-1} - \frac{1}{2^{2n}}\right) \leqslant 2^{2n} - 1\left(\frac{2^{2n}}{2^{2n}(2^{2n}-1)} - \frac{2^{2n}-1}{2^{2n}(2^{2n}-1)}\right) = \frac{1}{2^{2n}}. \tag{3.61}$$

Thus $\Delta \leqslant 1/2^{2n} + 1/2^{2n} \leqslant 1/2^{2n-1}$ for sufficiently large n.

Hence, using equation (3.58), the definition of Δ and the triangle inequality we can conclude that:

$$\left\|\mathcal{E}'(\rho^{SA}) - \frac{\mathbb{I}}{d_{S'S}}\rho^{A}\right\|_1 \leqslant \Delta + \epsilon, \tag{3.62}$$

Since Δ is exponentially small, we can forget it or just smudge ϵ. We can therefore have a more reasonable scheme that always encrypts the message and most importantly never tells the adversary that the message is not encrypted.

This completes our study of the model including any kind of correlation or entanglement. We provided different proofs of security, mainly entropic-security and entropic-indistinguishability, and we proved that they are in fact, up to small parameter adjustments, equivalent. Very importantly, we showed that these definitions are indeed achievable and do provide improvement on the state of the art cryptography by presenting two different efficient ciphers which are indeed entropically-secure in the general model. Furthermore, the formulae expressing key-length for both ciphers are exactly the same

Chapter 4

Conclusion

4.1 Recapitulation

We proposed generalizations of the classical security definitions of entropic indistinguishability and entropic security. These definitions were proposed in a framework that allows to model the most general situation possible. The adversary is allowed to get more information on the message after the message was sent, even after he received the encrypted message. We base security on a measure of how much uncertainty he has before the sampling of the side-channel (sampling which could be coherent with the encrypted system). That is, we fix what all situations could be and then quantify from this the adversary's uncertainty. Yes, the adversary will learn something more about the message, but the definition of entropic security is reminiscent of classical perfect security: what ever the adversary knows and will learn, the cipher-text will not help him learn more (with high probability).

This bound allows us to devise security definitions that are achievable and that guarantee security in an information theoretic way. Of course, in any given situation, calculating this bound is a problem in itself. It is more akin to computer security than cryptography. How much min-entropy is there in mp3 or jpg files? How much radiation does a computer screen emit? How much does one's wife know about something and then tell her lover? But in highly secure environments, it is hopefully feasible to estimate such side-channels and ensure that leakage of information does no get out of control.

In our new model, messages are now quantum states, which if restricted to classical messages, could be generalized to distribution on bit-strings. One interesting effect of this model, is that security does not depend solely on the probability of a given message, but really on the eigen-values of the mixture of all messages. For example, one might want to protect the provenance of data collected from a few sites, this data could be classical data from the environment of the apparatuses. That data could have different distributions depending from which site it came. Now, even though there might be just a few sites, hence low entropy on the origin of the data, the mixture could have high min-entropy. Hence entropic-encryption would lower the key requirement in order hide the provenance (and any other function on the data).

We also generalized existing cipher schemes to our framework and showed that they could reduce the key length compared with the same schemes used in previous security models. For schemes that previously used roughly n bits of classical key to encrypt n qubits, we showed that they can, if used with the quantum conditional min-entropy assumption, use roughly $n-t$ bits of key. This model also allows more latitude when one wants to choose a security definition (it is actually, in many cases the best security definition to use). It allows to go from $n-t$ bits of key to 2n bits of key for non-entangled n-qubit states having t bits of min-entropy or maximally entangled n-qubit state respectively, with all kinds of possibilities between the two. This possibility of encrypting quantum states which are entangled with the adversary with less than $2n$ bits of key (if entanglement is not too large) is new to this model.

4.2 Future directions

Authentication is another cryptographic primitive that lets a receiving party verify the provenance of a given message. That is, the sender and the receiver share a secret key which lets the sender tag messages in a way that ensures that with high probability, any tempering of the message will be detected by the receiver [20].

Authentication of Quantum Messages was introduced in 2002 in [5]. In that work, a protocol to authenticate quantum messages is given. The protocol works essentially as follows: the sender and receiver agree on a purity testing code $\{Q_k\}_k$, and private keys k, x and y. To authenticate a specific ρ, S encrypts ρ (in a perfect fashion) using the key x. Then $\mathcal{E}(\rho)$ is encoded using the code Q_k and the syndrome y is added to the resulting codeword. The result is sent to the receiver.

The receiver R measures the syndrome according to $\{Q_k\}_k$ and verifies that it is equal to y. If so, R simply decodes according $\{Q_k\}_k$ and then decrypts using key x. Simple enough. We must emphasize that the encryption scheme is a perfect one.

Could we apply the technique developed in this thesis and replace the encryption scheme with an entropic one? Let us develop that idea.

Borrowing their definition and notation, let us define the following projectors for any given pure $|\psi\rangle$ that one wishes to authenticate:

$$\begin{aligned} P_1^{|\psi\rangle} &= |\psi\rangle\langle\psi| \otimes \mathbb{I}_V + \mathbb{I}_M \otimes |REJ\rangle\langle REJ| - |\psi\rangle\langle\psi| \otimes |REJ\rangle\langle REJ| \\ P_0^{|\psi\rangle} &= (\mathbb{I}_M - |\psi\rangle\langle\psi|) \otimes (|ACC\rangle\langle ACC|), \end{aligned}$$

where M and V stand for message and verdict respectively, and the V register takes two values: *REJect* and *ACCept*.

The following defines security for quantum authentication, where S_k and R_k are the behavior of the sender and receiver when they are using global key k.

Definition 19 *A QAS is secure with error ϵ for a state $|\psi\rangle$ if it satisfies*

Completeness*: For all keys $k \in K$:* $\mathsf{R}_k(\mathsf{S}_k(|\psi\rangle\langle\psi|)) = |\psi\rangle\langle\psi| \otimes |ACC\rangle\langle ACC|$.

Soundness*: For all super-operators $\mathcal{O}$, let ρ_{R} be the state output by the receiver when the adversary's intervention is characterized by $\mathcal{O}$, that is*

$$\rho_{\mathsf{R}} = \frac{1}{|K|}\sum_k \mathsf{R}_k(\mathcal{O}(\mathsf{S}_k(|\psi\rangle\langle\psi|))).$$

The QAS has soundness error ϵ for $|\psi\rangle$ if

$$\mathrm{Tr}\left[P_1^{|\psi\rangle}\rho_{\mathsf{R}}\right] \geqslant 1-\epsilon.$$

A QAS is secure with error ϵ if it is secure with error ϵ for all states $|\psi\rangle$.

The most different property of quantum authentication, compared to classical authentication, is that it must also be an encryption scheme. Classically, these task are orthogonal. You do not have to encrypt to authenticate. It is our belief that if one replaces the encryption scheme used by an approximate encryption scheme or an entropic encryption scheme, one still obtains a secure quantum authentication protocol (maybe will we get a *non-malleable* encryption scheme), albeit with a security parameter ϵ that depends on the security parameter of the encryption scheme used.

This notion of authentication was reused by one of the authors, Daniel Gottesman in [25], to devise what he called an *uncloneable encryption*. If one restricts the input states in the QAS to be classical, one in fact can prove that the QAS becomes a quantum encryption of a classical state and that if the authentication succeeds, then with overwhelming probability, the adversary knows nothing on the message, even if given the encryption key which was used (hence the non-cloneable label); note that this is an impossible task classically: the adversary can always copy the authentication packet, wait for the key and compute what he wants with the key and the authenticated message. If we succeed in proving that QAS is still, in some fashion, secure with an entropic encryption schemes, of course the natural resolution is to prove that entropic non-cloneable encryptions are also feasible.

Bibliography

[1] Noga Alon, Oded Goldreich, Johan Håstad, and Ren é Peralta. Simple constructions of almost k-wise independent random variables. *Random Structures and Algorithms*, 3(3):289–304, 1992.

[2] Noga Alon, Oded Goldreich, Johan Håstad, and Rene Peralta. Simple constructions of almost k-wise independent random variables. In *IEEE Symposium on Foundations of Computer Science*, pages 544–553, 1990.

[3] Andris Ambainis, Michele Mosca, Alain Tapp, and Ronald de Wolf. Private quantum channels. In *IEEE Symposium on Foundations of Computer Science*, pages 547–553, 2000.

[4] Andris Ambainis and Adam Smith. Small pseudo-random families of matrices: Derandomizing approximate quantum encryption. In Klaus Jansen, Sanjeev Khanna, José D. P. Rolim, and Dana Ron, editors, *APPROX-RANDOM*, volume 3122 of *Lecture Notes in Computer Science*, pages 249–260. Springer, 2004.

[5] Howard Barnum, Claude Crépeau, Daniel Gottesman, Adam Smith, and Alain Tapp. Authentication of quantum messages. *PROC.43RD ANNUAL IEEE SYMPOSIUM ON THE FOUNDATIONS OF COMPUTER S*, 02:449, 2002.

[6] Mihir Bellare, Alexandra Boldyreva, and Adam O'Neill. Deterministic and efficiently searchable encryption. In *Advances in Cryptology - Crypto 2007*, Lecture Notes in Computer Science. Springer-Verlag, 2007.

[7] Avraham Ben-Aroya and Amnon Ta-Shma. Quantum expanders and the quantum entropy difference problem, 2007. quant-ph/0702129.

[8] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing*, pages 175–179. IEEE, 1984.

[9] Rajendra Bhatia. *Matrix Analysis*. Springer-Verlag, 1996.

[10] Alexandra Boldyreva, Serge Fehr, and Adam O'Neill. On notions of security for deterministic encryption, and efficient constructions without random oracles. Cryptology ePrint Archive, Report 2008/352, 2008. http://eprint.iacr.org/.

[11] Ran Canetti. Towards realizing random oracles: Hash functions that hide all partial information. *Lecture Notes in Computer Science*, 1294:455–469, 1997.

[12] Ran Canetti, Daniele Micciancio, and Omer Reingold. Perfectly one-way probabilistic hash functions (preliminary version). In *Proc 30th ACM Sump. on Theory of Computing*, pages 131–140, 1998.

[13] Claude Cohen-Tannoudji, Bernard Diu, and Frank Laloë. *Mécanique quantique*. Hermann, éditeurs des sciences et des arts, 293 rue Lecourbe, 75015 Paris, 1973.

[14] Martin Courchesne. De la sphère de poincaré au chiffrement d'information quantique. Master's thesis, McGill University, 2005.

[15] Simon Pierre Desrosiers. Entropic security in quantum cryptography. *Quantum Information Processing*, 2007. To appear.

[16] Simon Pierre Desrosiers and Frédéric Dupuis. Quantum entropic security and approximate quantum encryption. *IEEE Transactions on Information Theory*. To appear.

[17] Paul A. Dickinson and Ashwin Nayak. Approximate randomization of quantum states with fewer bits of key, 2006. quant-ph/0611033.

[18] Yevgeniy Dodis and Adam Smith. Entropic security and the encryption of high entropy messages. Cryptology ePrint Archive, Report 2004/219, 2004. http://citeseer.ist.psu.edu/705634.html.

[19] Serge Fehr and Christian Schaffner. Randomness extraction via delta-biased masking in the presence of a quantum attacker, 2007. http://lanl.arxiv.org/abs/0706.2606.

[20] E. N. Gilbert, F. J. MacWilliams, and N. J. A. Sloane. Codes which detect deception. *Bell System Tech. J.*, 53:405–424, 1974.

[21] O. Goldreich and L. A. Levin. A hard-core predicate for all one-way functions. In *STOC '89: Proceedings of the twenty-first annual ACM symposium on Theory of computing*, pages 25–32, New York, NY, USA, 1989. ACM.

[22] Oded Goldreich. *Foundations of Cryptography*, volume II Basic Applications. Cambridge University Press, 2004.

[23] Shafi Goldwasser and Silvio Micali. Probabilistic encryption & how to play mental poker keeping secret all partial information. In *STOC '82: Proceedings of the fourteenth annual ACM Symposium on Theory of computing*, pages 365–377, New York, NY, USA, 1982. ACM Press.

[24] Shafi Goldwasser and Silvio Micali. Probabilistic encryption. *J. Comput. Syst. Sci.*, 28(2):270–299, 1984.

[25] Daniel Gottesman. Uncloneable encryption. *Quantum information and Computation*, 3:581, 2003.

[26] D. Gross and J. Eisert. Quantum margulis expanders. *Quantum information and Computation*, 8:722, 2008.

[27] Aram W. Harrow. Quantum expanders from any classical cayley graph expander. *Quantum information and Computation*, 8:715, 2008.

[28] Patrick Hayden, Debbie Leung, Peter W. Shor, and Andreas Winter. Randomizing quantum states: Constructions and applications. *Communications in Mathematical Physics*, 250:371–391, Sep 2004.

[29] Carl W. Helstrom. Quantum detection and estimation theory. *Journal of Statistical Physics*, 1(2):231–252, 1969.

[30] R. A. Horn and C. A. Johnson. *Matrix analysis.* Cambridge University Press, Cambridge, UK, 1985.

[31] Roger A Horn. *Topics in matrix analysis.* Cambridge University Press, New York, NY, USA, 1986.

[32] Robert Koenig, Renato Renner, and Christian Schaffner. The operational meaning of min- and max-entropy, 2008. http://lanl.arxiv.org/abs/0807.1338.

[33] R. König, R. Renner, A. Bariska, and U. Maurer. Small Accessible Quantum Information Does Not Imply Security. *Physical Review Letters*, 98(14):140502–+, April 2007.

[34] R. J. McEliece. *A Public-Key System Based on Algebraic Coding Theory*, pages 114–116. Jet Propulsion Lab, 1978. DSN Progress Report 44.

[35] Ashwin Nayak and Pranab Sen. Invertible quantum operations and perfect encryption of quantum states. *Quantum Information and Computation*, jan. 2007.

[36] M. A. Nielsen and Isaac L. Chuang. *Quantum computation and quantum information.* Cambridge University Press, New York, NY, USA, 2000.

[37] Renato Renner. *Security of Quantum Key Distribution.* PhD thesis, Swiss Federal Institute of Technology, 2005.

[38] R. L. Rivest, A. Shamir, and L. M. Adelman. A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM*, 21:120–126, 1978.

[39] Alexander Russell and Hong Wang. How to fool an unbounded adversary with a short key. In *EUROCRYPT '02: Proceedings of the International Conference on the Theory and Applications of Cryptographic Techniques*, pages 133–148, London, UK, 2002. Springer-Verlag.

[40] C.E. Shannon. Communications theory of secrecy systems. *Bell System Technical Journal*, 28(4):656–715, October 1949.

[41] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM J.SCI.STATIST.COMPUT.*, 26:1484, 1997.

[42] Douglas R. Stinson. *Cryptography: Theory and Practice (Discrete Mathematics and Its Applications)*. CRC Press, March 1995.

[43] Gilbert S. Vernam. Cipher printing telegraph systems for secret wire and radio telegraphic communications. *Journal of the IEEE*, 55:109–115, 1926.