Distributed Keyless Security for Correlated Data with Applications in Visual Sensor Networks

William Luh
Department of Electrical and Computer Engineering
Texas A&M University
College Station, Texas 77843
luh@ece.tamu.edu

Deepa Kundur
Department of Electrical and Computer Engineering
Texas A&M University
College Station, Texas 77843
deepa@ece.tamu.edu

ABSTRACT

This paper examines the problem in which several nodes sharing highly correlated data, such as visual data, wish to compress and encrypt their data to provide confidentiality. The nodes however perform these tasks separately, without communicating with one another and without the use of cryptographic keys. The base station (BS) receiving all such encrypted data, can reconstruct each of the nodes' data, whereas a passive eavesdropper who is only allowed a subset of the encrypted data gleans as little information as possible about the nodes' data.

We build on previous results with the goal of increasing secrecy (measured by Shannon equivocation) by: (1) relaxing the BS's perfect reconstruction criterion thus permitting non-zero distortion reconstruction; (2) permitting communication (feedback) from the BS to the nodes. We show that permitting non-zero distortion reconstruction does increase secrecy, however unconditional secrecy is still not achievable unless the distortion is maximal. We also prove that feedback from the BS usually (under most practical scenarios) does not improve secrecy, unless the BS has certain knowledge concerning the eavesdropper.

Finally this paper proposes ideas for applying the results to images by analyzing the ideal image model to demonstrate the practical difficulties in achieving provable security for images.

Categories and Subject Descriptors

H.1.1 [**Models and Principles**]: Systems and Information Theory—*Information Theory*; I.4.2 [**Image Processing and Computer Vision**]: Compression (Coding)

General Terms

Security, Theory

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, to republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.

MM&Sec'07, September 20–21, 2007, Dallas, Texas, USA.
Copyright 2007 ACM 978-1-59593-857-2/07/0009 ...$5.00.

Keywords

Distributed secrecy, Shannon equivocation, multiterminal source coding

1. INTRODUCTION AND MOTIVATION

Distributed systems have gained popularity over the years as CMOS technology nears its limits, thus bounding the power of individual computing platforms. New paradigms are being developed for distributed platforms to harness their full, integral power. One particular type of distributed network is the sensor network, whose individual nodes lack the basic computing abilities available on personal computers a decade ago, but which make up for this deficiency through node ubiquity.

As sensor nodes are often deployed in a manner that cluster several of them within close physical proximity of one another, the data they collect are likely to be highly correlated. We consider the scenario in which nodes within such a cluster *cannot* communicate with one another, either because of energy constraints, or perhaps there is some other reason (either incidental or malicious) preventing them from communicating with one another. Although *explicit* collaboration does not exist under this scenario, since each node is aware that other nodes are processing data highly correlated with its own, this *implicit* knowledge can be used by a node to not only effectively compress that node's data [27], but also to encrypt the data for some level of confidentiality.[1]

The security assumption employed in this paper is similar to the secret sharing problem [24, 11, 31] in that the eavesdropper is permitted to eavesdrop on only a small subset of the nodes. The goal is a scheme whereby this small subset of encrypted data is not enough to reconstruct the nodes' data; on the other hand the base station (BS) receives *all* the nodes transmissions, and thus can reconstruct the data. The novelty in this problem is that the nodes cannot communicate (and must process their own data instead of forwarding data to an aggregator) and do not share any secret cryptographic keys unknown to the eavesdropper. The second keyless assumption accounts for the worst-case scenario in which physically unprotected may be accessed, and their keys revealed.

[1] Our notion of *distributed* is different from the conventional peer-to-peer systems encountered in network engineering, and we really mean *multiuser* when referring to the term distributed.

We distinguish between two related subproblems. The first subproblem is when all nodes have identical data or messages. We call this problem the *distributed secret sharing* (DSS) problem, since the original secret sharing problem also deals with a single message being shared by several entities. The second subproblem is more general, and concerns the case when all nodes have different but correlated data. We call this problem the *distributed encryption* (DE) problem after [6] who initially introduced the problem. The analyses of these two subproblems are different and thus treated separately.

We point out that although no cryptographic keys are employed in our system, the design may be complemented with more traditional ciphers/cryptosystems at the cost of higher complexity, as well as the need for a key distribution and management system.

1.1 Contribution of Paper

This paper presents novel theoretical models and analyses for the subproblems stated above. The main novel contribution in this paper is the analysis of the compression-secrecy tradeoff when the base station is permitted a non-zero distortion reconstruction of the nodes' data; this extends our previous work in which we required perfect reconstruction at the base station [16, 17]. The extension involves the application of rate-distortion and multiterminal source coding theory. We show that by permitting non-zero distortion, secrecy as measured by Shannon equivocation, can be increased from the case when perfect reconstruction is required.[2] We also prove that BS feedback usually does not increase secrecy, in contrast with many multiuser information theory results.

In addition to our novel analysis, we also outline some fundamental ideas in applying the theoretical results to image data. Specifically, we look at how our coding theorems fit the more conventional image encryption algorithms designed to date. We outline how to encrypt an ideal image model using the codes presented in our previous papers [16, 17].

The reason for our current focus on the coding aspects stems from the following observation. Theoretically, optimal compression can be achieved using coding alone. In practice, signal processing (a transform) is applied as a preprocessor to alleviate the complexities of coding [21]. Hence in practice, both signal processing and coding are employed to achieve goals such as image compression and watermarking. However since standard transforms are now a common technology, we focus on the coding aspects of our problem.

2. PRELIMINARIES

To make the analysis tractable, we consider a distributed system consisting of two nodes (referred to as Alice and Bob) and one base station. With minimal effort, the results presented in this paper can be generalized to multiple nodes.

2.1 Notation

Let upper-case letters denote random variables (RVs), e.g. X, caligraphic upper-case letters denote finite sets, e.g. $\mathcal{X}$, $|\mathcal{X}|$ denotes the finite cardinality of $\mathcal{X}$, lower-case letters denote realizations, e.g. x is a realization of RV X, and superscripted letters denote (column, unless otherwise stated) vectors, e.g. x^n, where the superscript n gives the dimension of the vector (or number of components in the vector). The probability mass function (pmf) of X is denoted using P_X. A Markov chain X, Y, Z in that order is denoted $X \leftrightarrow Y \leftrightarrow Z$ if and only if the joint pmf can be factored as $P_{X,Y,Z} = P_{X|Y} P_{Z|Y}$. $H(X)$ is the entropy of X, $H(X|Y)$ is the conditional entropy of X given Y, and $I(X;Y)$ is the mutual information between X and Y [5]. Matrices are given by upper-case bold letters, e.g. $\mathbf{A}$.

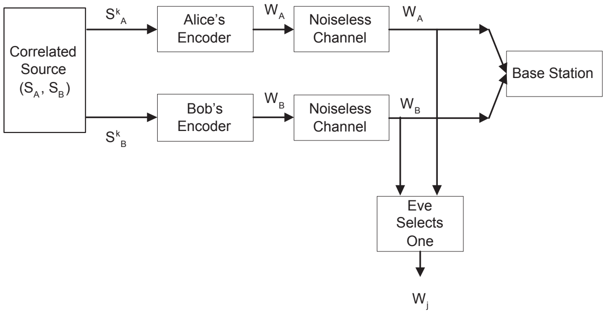

Figure 1: Separate Enciphering by Alice and Bob with Eavesdropping by Eve

2.2 Problem Formulation

Let $S^k_A \in \mathcal{S}^k_A$ and $S^k_B \in \mathcal{S}^k_B$ denote Alice and Bob's messages resp.; in the distributed secret sharing (DSS) problem, we would have $S^k_A = S^k_B \triangleq S^k \in \mathcal{S}^k$. Alice and Bob's messages are generated by a joint discrete memoryless source (DMS) given by Eq. 1.

$$P^k_{S_A,S_B}(s^k_A, s^k_B) = \prod_{i=1}^{k} P_{S_A,S_B}(s_{A,i}, s_{B,i}) \qquad (1)$$

Our problem is summarized in Fig. 1. Alice and Bob are to encipher their S^k_A, S^k_B *separately without cooperation* creating $W_A \in \mathcal{W}_A$ and $W_B \in \mathcal{W}_B$ resp.

The base station (BS) receives both W_A and W_B, and its goal is to reconstruct S^k_A and S^k_B within some fidelity criterion to be discussed below. Let the quadruple

$$(f_A, f_B, \varphi_A, \varphi_B)$$

denote Alice's (possibly stochastic) encoder, Bob's (possibly stochastic) encoder, and the BS's decoders to reconstruct Alice and Bob's messages resp. Here $f_A : \mathcal{S}^k_A \to \mathcal{W}_A$, $f_B : \mathcal{S}^k_B \to \mathcal{W}_B$, $\varphi_A : \mathcal{W}_A \times \mathcal{W}_B \to \hat{\mathcal{S}}^k_A$, and $\varphi_B : \mathcal{W}_A \times \mathcal{W}_B \to \hat{\mathcal{S}}^k_B$, where $\hat{\mathcal{S}}^k_A$ and $\hat{\mathcal{S}}^k_B$ are the reconstruction alphabets for Alice and Bob resp.

If the encoders f_A, f_B are stochastic, they can be defined without loss of generality by deterministic encoders f'_A, f'_B, where the randomness comes from locally generated RVs T_A, T_B resp. as shown below.

$$W_A = f_A(S^k_A) = f'_A(S^k_A, T_A) \qquad (2)$$

$$W_B = f_B(S^k_B) = f'_B(S^k_B, T_B) \qquad (3)$$

The random variables T_A, T_B simulate choosing a codeword randomly from the subsets of $\mathcal{W}_A, \mathcal{W}_B$ resp.

[2] Our choice to use Shannon equivocation as the measure of security opposed to security based on computational and complexity theory [8] is because the problem can be solved using public-key cryptography (see Section 3.3).

Let $\rho_A^k : \mathcal{S}_A^k \times \hat{\mathcal{S}}_A^k \to \mathbb{R}^+$ be the *block* distortion measure between Alice's original message block s_A^k and the BS's reconstruction $\hat{s}_A^k$; similarly $\rho_B^k : \mathcal{S}_B^k \times \hat{\mathcal{S}}_B^k \to \mathbb{R}^+$ is the block distortion measure for Bob's message. Following Shannon theory, the block distortion measures are defined by *single-letter* distortion measures $\rho_j : \mathcal{S}_j \times \hat{\mathcal{S}}_j$ for $j = A, B$ so that the block distortion measure is an average of the single-letter distortion measures as in Eq. 4.

$$\rho_j^k(s_j^k, \hat{s}_j^k) = \frac{1}{k}\sum_{i=1}^{k} \rho_j(s_{j,i}, \hat{s}_{j,i}), \quad j = A, B \tag{4}$$

Hence the BS's reconstruction distortion criteria can be specified by two real numbers representing Alice and Bob's messages, $D_A > 0$ and $D_B > 0$ resp., such that the expected distortion is bounded by these two numbers as in Eqs. 5 and 6 for $\epsilon > 0$ arbitrarily small. The expectation is taken over all random quantities, such as the original message blocks S_A^k, S_B^k, as well as the possibly stochastic encoders f_A, f_B via T_A, T_B resp.

$$E[\rho_A^k(S_A^k, \hat{S}_A^k)] \leq D_A + \epsilon \tag{5}$$

$$E[\rho_B^k(S_B^k, \hat{S}_B^k)] \leq D_B + \epsilon \tag{6}$$

In other words, for a distortion pair (D_A, D_B), the encoders and decoders $(f_A, f_B, \varphi_A, \varphi_B)$ satisfying Eqs. 5 and 6 are said to satisfy the distortion criteria (D_A, D_B).

The (source coding) rates of Alice and Bob's enciphered messages are defined as

$$R_A \triangleq \frac{\log_2 |\mathcal{W}_A|}{k} \tag{7}$$

$$R_B \triangleq \frac{\log_2 |\mathcal{W}_B|}{k}. \tag{8}$$

Note that although the definitions of rate do not include reference to the RVs T_A, T_B, rate may still be affected by stochastic encoding. For example, the set $\mathcal{W}_j$ may be partitioned into non-overlapping subsets (cosets), such that each coset is associated with a unique message s_j^k, and the RV T_j randomly chooses a codeword from the coset associated with the input message [30]. In this case, the encoding maps one message to many codewords (in which one codeword is selected randomly by T_j), and thus in this example $|\mathcal{W}_j|$ is affected by T_j.

In Fig. 1, the eavesdropper, referred to as Eve, is allowed to select either W_A or W_B, but not both. Depending on which enciphered message Eve selects, the equivocation rates of Eve w.r.t. Alice and Bob are defined as

$$\Delta_A \triangleq \frac{H(S_A^k|W_A)}{k} \tag{9}$$

$$\Delta_B \triangleq \frac{H(S_B^k|W_B)}{k}. \tag{10}$$

Equivocation rates of $\Delta_A = H(S_A)$ for Alice and $\Delta_B = H(S_B)$ for Bob are desired as this implies $H(S_j^k|W_j) = kH(S_j) = H(S_j^k)$ for $j = A, B$, which means Eve is no better off with W_j than she was without it. Our definitions of equivocation rate also require $H(S_A) = H(S_B)$. This requirement implies that if Eve interecepts W_A, then $\Delta_B \geq \Delta_A$, and if she intercepts W_B, then $\Delta_A \geq \Delta_B$. In other words, if Eve intercepts Alice's stream, then she would learn more about Alice's message than Bob's message.

We say a quadruple (d_A, d_B, r_A, r_B) corresponding to

$$(\Delta_A, \Delta_B, R_A, R_B)$$

is *achievable* w.r.t (D_A, D_B) if there exists a $(f_A, f_B, \varphi_A, \varphi_B)$ such that for all $\epsilon > 0$ (arbitrarily small) and k sufficiently large the following are satisfied:

$$R_A \leq r_A + \epsilon \tag{11}$$

$$R_B \leq r_B + \epsilon \tag{12}$$

$$d_A - \epsilon \leq \Delta_A \leq d_A \tag{13}$$

$$d_B - \epsilon \leq \Delta_B \leq d_B \tag{14}$$

where

$$W_A = f_A(S_A^k) \tag{15}$$

$$W_B = f_B(S_B^k) \tag{16}$$

$$\hat{S}_A^k = \varphi_A(W_A, W_B) \tag{17}$$

$$\hat{S}_B^k = \varphi_B(W_A, W_B) \tag{18}$$

and Eqs. 5 and 6 are also satisfied. In addition, all parties, Alice, Bob, and Eve, have complete knowledge of f_A, f_B (except for the possibly locally generated RVs T_A, T_B), and any cryptographic keys used.

The DSS problem is a special case of the above formulation of the DE problem, and is formulated similarly by replacing S_A, S_B with just S. We make the distinction between these two problems since their analysis and coding solutions may be different.

3. ENLARGING THE CAPACITY REGIONS

In this section we show that permitting non-zero distortion for the BS reconstruction increases the capacity region, while feedback from the BS generally does not increase the capacity region, and may in fact hurt secrecy.

The capacity regions for the distributed secret sharing (DSS) and distributed encryption (DE) cases are different. The former is based on single-user rate-distortion theory, while the latter does not have a complete capacity region characterized. This incompleteness is due to the unresolved capacity region (inner region not equal to outer region) for the general multiterminal source coding (MSC) problem [29, 9, 2].

3.1 Capacity Region for DSS

The capacity region $\mathcal{R}_{DSS}(D)$ for the DSS problem is defined to be the set of quadruples (d_A, d_B, r_A, r_B) that are achievable w.r.t to D, the distortion criterion between original message and BS reconstruction.

THEOREM 1. *For a given distortion criterion D, the capacity region is given by*

$$\begin{aligned} \mathcal{R}_{DSS}(D) = \{(d_A, d_B, r_A, r_B) :& \\ & r_A \geq 0, \\ & r_B \geq 0, \\ & 0 \leq d_A \leq H(S), \\ & 0 \leq d_B \leq H(S), \\ & 0 \leq d_A + d_B \leq 2H(S) - R(D), \\ & r_A + r_B \geq R(D), \\ & r_A + d_A \geq H(S), \\ & r_B + d_B \geq H(S)\}. \end{aligned} \tag{19}$$

In Theorem 1 (proved in Appendix A.1), the rate-distortion function is given by

$$R(D) = \min_{p(\hat{s}|s):E[\rho(S,\hat{S})]\leq D} I(S;\hat{S}). \tag{20}$$

Informally, $R(D)$ is the minimum number of bits per symbol (from $\hat{\mathcal{S}}$) such that the reconstruction distortion is (no greater than) D. This means that $\hat{s}^k$ would be approximately $kR(D)$ bits long given k is sufficiently large.

Theorem 1 also confirms what we intuitively expect: if Alice and Bob send nothing to the base station, i.e. $R(D) = 0$, then unconditional secrecy can be achieved (since it is possible for $\Delta_A = H(S)$ and $\Delta_B = H(S)$ while satisfying $\Delta_A + \Delta_B = 2H(S)$). In addition, $R(D) = 0$ is necessary for unconditional secrecy, and so although allowing non-zero distortion does increase secrecy from the distortionless case (when $R(D) = H(S)$), it is not for free. Finally Theorem 1 can also be shown to match our previous distortionless result when $D = 0$ in [16].

3.2 Outer and Inner Regions for DE

The capacity region $\mathcal{R}_{DE}(D_A, D_B)$ for the DE problem is defined to be the set of quadruples (d_A, d_B, r_A, r_B) that are achievable w.r.t to (D_A, D_B), the distortion criteria between original messages and BS reconstruction. Outer and inner regions, $\mathcal{R}_{DE-out}(D_A, D_B)$ and $\mathcal{R}_{DE-in}(D_A, D_B)$ are defined to be sets such that

$$\mathcal{R}_{DE-in}(D_A, D_B) \subseteq \mathcal{R}_{DE}(D_A, D_B) \subseteq \mathcal{R}_{DE-out}(D_A, D_B).$$

Due to the existing gap between the outer and inner regions for the MSC problem [2],

$$\mathcal{R}_{DE-in}(D_A, D_B) \neq \mathcal{R}_{DE-out}(D_A, D_B),$$

and thus a complete capacity region has not been derived, although it is conjectured that the outer region in the MSC problem [29, 9, 2] is the capacity region for MSC.

Definition 1. *Define $\mathcal{P}(D_A, D_B)$ as the set of auxiliary RVs (Y_A, Y_B) jointly distributed with (S_A, S_B) such that:*

(i) $Y_A \leftrightarrow S_A \leftrightarrow S_B$ and $S_A \leftrightarrow S_B \leftrightarrow Y_B$;

(ii) there exist functions $F_A : \mathcal{Y}_A \times \mathcal{Y}_B \to \hat{\mathcal{S}}_A$ and $F_B : \mathcal{Y}_A \times \mathcal{Y}_B \to \hat{\mathcal{S}}_B$ such that

$$\begin{aligned} E[\rho_A(S_A, \hat{S}_A)] &\leq D_A && (21)\\ E[\rho_B(S_B, \hat{S}_B)] &\leq D_B && (22)\end{aligned}$$

where

$$\begin{aligned} \hat{S}_A &= F_A(Y_A, Y_B) && (23)\\ \hat{S}_B &= F_B(Y_A, Y_B). && (24)\end{aligned}$$

Theorem 2 (Outer Region). *$\mathcal{R}_{DE-out}(D_A, D_B)$ is the set of all (d_A, d_B, r_A, r_B) that satisfy*

$$\begin{aligned} 0 \leq d_A &\leq H(S_A) && (25)\\ 0 \leq d_B &\leq H(S_B) && (26)\\ d_A + d_B &\leq H(S_A) + H(S_B) - I(S_A, S_B; Y_A, Y_B) && (27)\\ r_A &\geq I(Y_A; S_A, S_B|Y_B) && (28)\\ r_B &\geq I(Y_B; S_A, S_B|Y_A) && (29)\\ r_A + r_B &\geq I(S_A, S_B; Y_A, Y_B) && (30)\\ r_A + d_A &\geq H(S_A) && (31)\\ r_B + d_B &\geq H(S_A) && (32)\end{aligned}$$

for all $(Y_A, Y_B) \in \mathcal{P}(D_A, D_B)$.

Theorem 2 is proved in Appendix A.2.

Theorem 3 (Inner Region). *$\mathcal{R}_{DE-in}(D_A, D_B)$ is the set of all (d_A, d_B, r_A, r_B) that satisfy*

$$\begin{aligned} 0 \leq d_A &\leq H(S_A) && (33)\\ 0 \leq d_B &\leq H(S_B) && (34)\\ d_A + d_B &\leq I(S_A; S_B) + H(S_A|S_B, Y_A) \\ &\quad + H(S_B|S_A, Y_B) && (35)\\ r_A &\geq I(S_A; S_B, Y_A|Y_B) && (36)\\ r_B &\geq I(S_B; S_A, Y_B|Y_A) && (37)\\ r_A + r_B &\geq H(S_A, S_B) - H(S_A|S_B, Y_A) \\ &\quad - H(S_B|S_A, Y_B) && (38)\\ r_A + d_A &\geq H(S_A) && (39)\\ r_B + d_B &\geq H(S_A) && (40)\end{aligned}$$

for all $(Y_A, Y_B) \in \mathcal{P}(D_A, D_B)$.

Theorem 3 is proved in Appendix A.3.

The informal interpretation of the auxiliary RVs Y_A, Y_B found in both Theorems 2 and 3, is that they represent not only W_A, W_B resp., but also capture the distortion between original messages and decoded messages. Therefore if the auxiliary RVs are chosen $Y_A = S_A$, $Y_B = S_B$, then this corresponds to the distortionless case [29] and one can verify that the inequalities in both Theorems 2 and 3 match under this setting, and in addition also match our previous distortionless result in [17]. In [2], it is shown that the new inner region for the MSC problem is contained in the outer region, and thus for our problem, we necessarily have

$$\mathcal{R}_{DE-in}(D_A, D_B) \subset \mathcal{R}_{DE-out}(D_A, D_B)$$

since Eqs. 36 to 38 are directly from [2].

In order to achieve unconditional secrecy, Theorem 1 shows that it is necessary for $I(S_A, S_B; Y_A, Y_B) = 0$. However, this corresponds to (S_A, S_B) independent from (Y_A, Y_B), and thus we can expect the distortion to be at least

$$\max_{(s_j, \hat{s}_j)\in \mathcal{S}_j \times \hat{\mathcal{S}}_j} \rho(s_j, \hat{s}_j)$$

for $j = A, B$, i.e. Alice and Bob send nothing to the BS as in Section 3.1.

3.3 Feedback from the BS

In both the DSS and DE problems, Alice and Bob are not permitted to communicate with one another. However since they can send to the BS, the BS can also send to both parties. We show that BS feedback to the parties generally does not increase secrecy if all channels including Eve's channel are noiseless, even if Eve is permitted to eavesdrop on *only* one of the streams from the BS. This is in contrast to the wiretap channel with feedback results in [14, 10, 18, 1, 3, 13] in which public feedback does increase secrecy.

There are two types of BS feedback: the BS can send information to Alice and Bob, Z_A and Z_B resp., based on the $\hat{s}^k$ reconstructed from W_A and W_B (true feedback), or the BS can send arbitrary information independent from what

Table 1: Different Types of BS Feedback

	Yes	No
True Feedback?	1	0
Knowledge of Previous Eavesdrop?	1	0
Knowledge of Future Feedback Eavesdrop?	1	0

it received from Alice and Bob (artificial feedback). The BS may either have knowledge of which W_j, for $j = A$ or $j = B$, Eve *previously* intercepted, or have no such knowledge. The BS may have knowledge of which Z_j, $j = A$ or $j = B$ Eve *will* intercept, or have no such knowledge. Therefore there are eight feedback scenarios summarized in Table 1. We can systematically analyze all the different feedback cases succinctly since we are only interested in whether secrecy capacity may be increased or not. Using Table 1, the case 101 corresponds to: true feedback, no knowledge of previous eavesdrop, and knowledge of future feedback eavesdrop. The case *00 corresponds to either true or artificial feedback, no knowledge of previous eavesdrop, and knowledge of future feedback eavesdrop.

- Case **1: If the BS knows Eve will not be eavesdropping on Z_B say, then the BS can add a tag to Z_B informing Bob that Z_B may be used as a one-time pad for Bob's future transmission to the BS, thus secrecy for Bob is increased via the one-time pad cipher.
- Case 110: Feedback either does not help or can actually decrease secrecy. The proof is given in Appendix A.4.
- Case 100: Without knowledge of what Eve possess, this case performs worst than the case 110.
- Case 0*0: Artificial feedback does not improve secrecy, nor does it decrease secrecy. The proof is given in Appendix A.4.

Note that although feedback does not improve secrecy in the Shannon equivocation sense, feedback can improve computational secrecy, e.g. BS sends the parties its public-key for asymmetric ciphers [28].

4. SUMMARY OF PRACTICAL CODES

In this section we briefly review some of the coding schemes that can either achieve or come close to achieving the capacity regions for distortionless distributed secret sharing (DSS) [16] and distributed encryption (DE) [17] problems. The interpretation of the proofs in Appendix A allow us to easily apply these codes to some of the non-zero distortion cases.

In Section 3 we showed unconditional secrecy is not possible, unless the allowable distortion is excessively high such that Alice and Bob send nothing to the BS. Therefore the codes reviewed in this section relevant to our problem also cannot have unconditional secrecy. However one assumption that can hinder Eve's attempts at recovering the original messages is the assumption that the RVs S_A and S_B are uniformly distributed. When this is the case, Eve may reduce her uncertainty of the message given Alice's W_A or Bob's W_B to a smaller message space. However within this smaller message space, since all the messages are equally likely, she can only guess at which message is the original one (similar to the proof in Appendix A.1). Thus we assume that S_A^k and S_B^k (or just S^k for the DSS problem) are uniformly distributed.

4.1 DSS Codes

A scheme for the DSS problem based on the table construction given in Appendix A.1 is presented. This scheme was not previously mentioned in [16] due to limited space.

Suppose S^k is a binary string, uniformly distributed over $\{0,1\}^k$. In order to avoid large lookup tables, one can create a table whose entries are the indices 0 to approximately $2^k - 1$, sorted in ascending order row-by-row. Each binary string s^k can also be represented by its equivalent decimal number, which is in one-to-one correspondence with one of the entries in the table. Alice and Bob's w_A, w_B can then be computed without a lookup table. Suppose the table has a rows and b columns as in Fig. 4, then encoding is simply

$$w_A = \left\lfloor \frac{decimal(s^k)}{b} \right\rfloor \quad (41)$$

$$w_B = decimal(s^k) \bmod a \quad (42)$$

where $\lfloor x \rfloor$ is the floor operation (largest integer less than x), and $decimal(x)$ is the equivalent decimal representation of x. The BS can reconstruct s^k via

$$decimal(s^k) = w_A \cdot b + w_b. \quad (43)$$

This scheme may be satisfactory for some applications. The drawback is that if Eve intercepts W_A, Eve only needs to guess from a list of sorted numbers (i.e. from one row of the table). Most of these numbers in binary form will have the same most significant bits, and thus although her guess may not be exact, it could be a good approximation. Any transformation of this sorted table for the purposes of "unsorting it" does not increase the secrecy for Alice, since Eve can always apply the inverse transformation (the keyless assumption signifies that the transformation is known to Eve).

In [16] we derived a better code that thwarts Eve's attempts to obtain a good guess of s^k. Let S^k be uniformly distributed over $(GF(q))^k$ Let $\mathbf{C}$ be the matrix containing elements from $GF(q)$

$$\mathbf{C} = \left(\begin{array}{cccccccc} a_1 & a_2 & \cdots & a_r & 0 & \cdots & \cdots & 0 \\ 0 & a_1 & a_2 & \cdots & a_r & 0 & \cdots & 0 \\ \vdots & & \ddots & & & & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & a_1 & a_2 & \cdots & a_r \\ \hline b_1 & b_2 & \cdots & b_l & 0 & \cdots & \cdots & 0 \\ 0 & b_1 & b_2 & \cdots & b_l & 0 & \cdots & 0 \\ \vdots & & \ddots & & & & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & b_1 & b_2 & \cdots & b_l \end{array}\right) = \left(\begin{array}{c} \mathbf{C}_1 \\ \hline \mathbf{C}_2 \end{array}\right) \quad (44)$$

such that $\mathbf{C}_1$ has αk rows and $\mathbf{C}_2$ has $(1-\alpha)k$ rows so that $r = k - \alpha k + 1$ and $l = k - (1-\alpha)k + 1$. The encoding is defined as

$$w_A = \mathbf{C}_1 s^k \quad (45)$$

$$w_B = \mathbf{C}_2 s^k \quad (46)$$

where the operations are over $GF(q)$. A simple shift-register implementation can be used to perform the matrix multiplications, since each row is shifted one to the right. Decoding is simply

$$\hat{s}^k = \mathbf{C}^{-1} \begin{pmatrix} w_A \\ w_B \end{pmatrix}. \tag{47}$$

In [16] we showed the following lemma.

Lemma 1. *Suppose Eve knows $g_A < (1-\alpha)k$ symbols of s^k given W_A, or $g_B < \alpha k$ symbols of s^k given W_B. Then these g_A or g_B symbols do not reveal any other symbols if any αk columns of $\mathbf{C}_1$ have non-zero determinant and any $(1-\alpha)k$ columns of $\mathbf{C}_2$ have non-zero determinant.*

Of course the matrix $\mathbf{C}$ itself also has to be invertible. We provided a sufficiency condition in [16] on the field size that guarantees the existence of codes that satisfy Lemma 1.

This second class of codes (presented above) is useful when Eve can correctly guess many symbols. For example the message may be a JPEG encoded image that contains an abundance of delimiter symbols (e.g. end-of-block symbol) that may be guessed by Eve. In this case, the JPEG encoded image may be partitioned into k blocks of symbols s^k, and the above code may be applied to each s^k. With proper partitioning, it may be possible to prevent Eve from learning any other symbols via Lemma 1 even if she knows exactly where some of the delimiter symbols are located in the stream.

Finally, it is easy to incoroporate non-zero distortion reconstruction into the schemes above. Alice and Bob each compress s^k using the same lossy compressor with the same compressor parameters, and then apply the above codes to their compressed result. This matches the two-stage construction discussed in Appendix A.1.

4.2 DE Codes

In [17], we showed that distributed source codes for the distortionless case using the method of [22] can be secured practically by careful choice of the parity check matrices. The same criteria used in Lemma 1 can be applied to each of the parity check matrices $\mathbf{H}_1$ and $\mathbf{H}_2$. However, the difference from the DSS version is that $\mathbf{H}_1$ and $\mathbf{H}_2$ are created from a partitioning of a generator matrix for a linear code with good distance properties to ensure decodability. We demonstrated in [17] a method of obtaining $\mathbf{H}_1$ and $\mathbf{H}_2$ that satisfy Lemma 1 by judiciously partitioning the dual generator matrix of a Reed-Solomon code.

The extension of the DE code from the distortionless case to the non-zero distortion case is not a straightforward two-stage construction as in Section 4.1, since Alice and Bob's messages are different. Design of secure non-zero distortion DE codes is still an open problem the authors are currently investigating.

5. APPLICATION TO IMAGE DATA

In this section we outline how the codes summarized in Section 4 may be applied to images. A good review of some existing encryption techniques for images (and videos) can be found in [7]. Most of these techniques share a common architecture illustrated in Fig. 2. Here compression and encryption can be performed jointly, not necessarily in the order depicted in Fig. 2. As we mentioned in the introduction, the signal processing unit is usually a transform that acts as a pre-processor to the actual coding (compression, encryption, watermarking, etc.). The goal of the transform is to make coding easier, e.g. reduce the complexity by making the data amenable to scalar quantization instead of vector quantization in the case of image compression [21].

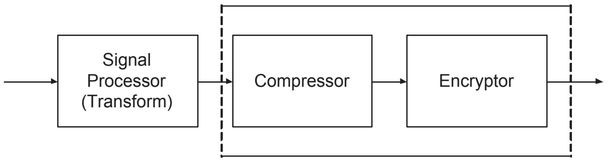

Figure 2: Common Image Encryption Architecture

5.1 Background

Existing image encryption techniques may be broadly classified as either *selective*, *naive* or a combination of the two. *Selective* encryption techniques encrypt select portions of the signal, while other portions are not encrypted. Selective encryption provides weak security, but greatly reduces complexity. *Naive* encryption techniques treat images no differently than text data, such that the entire image is encrypted using powerful ciphers such as DES or AES.

An alternative approach to the above techniques is to use powerful ciphers such as DES or AES on a portion of the image, while applying heuristics to the other portion. In [23], approximately half of a compressed I-frame is encrypted using DES, while the other half is added (bit-wise) to the half to be processed by DES. The authors show that the addition of the two halves *may* provide one-time-pad-like security by showing that the empirical distribution of bytes for the entire I-frame is approximately uniform. While such empirical evidence is likely the best statistical information available, we shall analyze an ideal situation in which such an assumption is true.

5.2 Proposed Distributed Image Encryption

Following [23], the image is first compressed (in practice using a standard such as JPEG), and then the resulting compressed image is fed into the encoders summarized in Section 4.

5.3 Analysis of an Ideal Image Model

In Section 5.1, we mentioned that [23] used empirical evidence to show that their heuristic *may* achieve a one-time-pad-like cipher. This assumption is also necessary in order for our proposed distributed image encryption (cf. Section 5.2) to be as secure as possible, since in Section 4 we assumed the messages are uniformly distributed. In this section we demonstrate that in theory, this uniform distribution assumption requires a substantial compression tradeoff even under an ideal (unrealistic) image model.

Images are not created from an uniform distribution, thus we must transform the image data into a form usable by the encoders in Section 4. Suppose the image data is modeled by a random vector S^k, whose components are jointly Gaussian RVs with different means and variances, i.e. $S_i \sim \mathcal{N}(m_i, \sigma_i^2)$.[3] Suppose the mean vector of S^k is given by m^k, and the covariance matrix is given by $\mathbf{K}$, and are known

[3] This model does not accurately model the anomalies, i.e the high frequency components or the edges in an image. However it is suitable for our analysis. For a more realistic model see [12].

by both encoder and decoder. The eigenvector (Hotelling) transform results in

$$\bar{s}^k = \mathbf{F}(s^k - m^k) \tag{48}$$

where $\mathbf{F}$ is a matrix consisting of the orthonormal eigenvectors of $\mathbf{K}$ [26]. The components of $\bar{s}^k$ are known to be uncorrelated. Furthermore, since s^k is jointly Gaussian and the transform is linear, $\bar{s}^k$ is also jointly Gaussian, and so the components of $\bar{s}^k$ are independent.

Reverse waterfilling is a method to allocate the (theoretical) minimum number of bits to each component of a vector of independent zero-mean Gaussian RVs, such that a mean square error (MSE) distortion criterion is satisfied [5]. If the variance of a particular RV is below a set threshold, 0 bits are allocated to that RV. Equivalently, reverse waterfilling is also a method of determining how much distortion each component of the said Gaussian vector is to incur in order to reach a target distortion criterion. The salient point of reverse waterfilling to our discussion is that it assigns a distortion to each component of $\bar{s}^k$, and a component whose variance does not exceed a threshold is allocated 0 bits.

The second interpretation will be used in our discussion by assigning each component $\bar{s}^k$ a target distortion, and then using an optimal scalar quantizer [15, 19] to reach this target distortion. Since the quantizer is scalar instead of vector, the actual rate achieved will be greater than that optimally predicted by reverse waterfilling, and the distortion will be slightly higher if 0 bits are allocated to components whose variances do not exceed a threshold. Since an optimal scalar quantizer is used, each of the quantizer bins have different *a priori* probabilities, thus further Huffman coding of the bins can reduce the average number of bits. However Huffman codes are variable length codes, which means its output may differ in length depending on its input. If we encode (viz. Section 4) such quantized and Huffman coded $\bar{s}^k$, variations in the length may provide information to Eve.

We discuss two methods of equalizing the variations in length (i.e. eliminating clues for Eve), both of which reduce the compression rate. The first method is the obvious method: pad the output of the compressor with additional bits such that all possible padded outputs have the same length. The amount of padding is dictated by the longest Huffman codeword, so this method is undesirable. Additionally in order to make the padded output look uniform, no delimiters should be placed between the real Huffman codeword and the padding. This of course means the decoder may not know when the true codewords terminate, if the padding happens to be valid Huffmans codewords.

The second method is to use a quantizer whose quantization bins have equal probability. The output of the quantizer will always contain the same number of bits, and each bit is equally likely to occur. This means Eve's *a priori* knowledge of which bin and even which bits are likely to be outputted by the quantizer, is now uniform. However this sacrifices the compression rate since no further Huffman coding can be applied. Fig. 3 shows the performance of the equal probability (deemed "secure") scalar quantizer for a zero-mean and unit-variance Gaussian RV compared to an optimal scalar quantizer and equally-spaced scalar quantizer [19]. The performance gap widens as finer resolutions are required (i.e. more quantization bins are required). When a MSE distortion of 10^{-2} is desired, on average each bin of the secure scalar quantizer requires about 1.5 bits more than the optimal scalar quantizer (see Fig. 3b). This may be substantial when we are looking at images with around half a million pixels, which translates to approximately an additional 92KB (twice the size of an average JPEG image). However most components in $\bar{s}^k$ may not require such a fine resolution, thus the foregoing estimate may represent a worst case scenario. The decision levels and reconstruction levels for the secure scalar quantizer are provided in Appendix B.

This analysis of the ideal case shows that in practice the heuristic used in [23] may not achieve the one-time pad security as desired. The analysis also suggests that in practice, sacrifice of compression may be required for security. This kind of sacrifice is common in many secrecy systems, such as [30] or [20], but is not necessary if the input distribution is already uniform.

5.4 Summary

Once the quantizer/compressor in Section 5.3 outputs the equiprobable bits, the codes summarized in Section 4 may be applied. The encoder will have to group the bits into equal length, such that each group of m bits represents an element from $GF(2^m)$. The BS decoder can recover the original stream of bits, and re-group them to form a quantized version of $\bar{s}^k$. The inverse transform is applied to retrieve $\hat{s}^k$. Of course the BS must know in advance the means, variances, as well as the number of bits allocated to each component in $\bar{s}^k$.

Eve is permitted to know the number of bits allocated, which does not help her since each bit appears equally likely viz. using the secure scalar quantizer. However, if Eve has the mean and variance of s^k, this alone could provide her sufficient information regarding s^k. In practice, the discrete cosine transform (DCT) or subband transforms (wavelet) may be used in place of the Hotelling transform, thus true means and variances are not needed or known by either the BS or Eve. However, a uniformly distributed output is not guaranteed when using these more practical transforms.

6. CONCLUSIONS AND FUTURE WORK

This paper reviewed the problem of separately encoding correlated sources with the goals of compression *and* confidentiality in mind. A novel analysis is provided that shows non-zero distortion can increase the secrecy rate, whereas base station feedback usually does not increase the secrecy rate in contrast to wiretap secrecy with feedback and other multiuser information theory results. Further, this paper addresses the application of simple codes to image data by analyzing the ideal image model, and showing the difficulty of achieving the desired assumptions for secrecy.

Our ongoing work examines the problem of codes for distributed encryption with non-zero distortion. The authors are also looking at a variation of the problem, whereby the messages are considered to be noisy versions of one another, and thus the base station only has to reconstruct *one* version of the messages. This problem is similar to the CEO problem [4] without the security requirement.

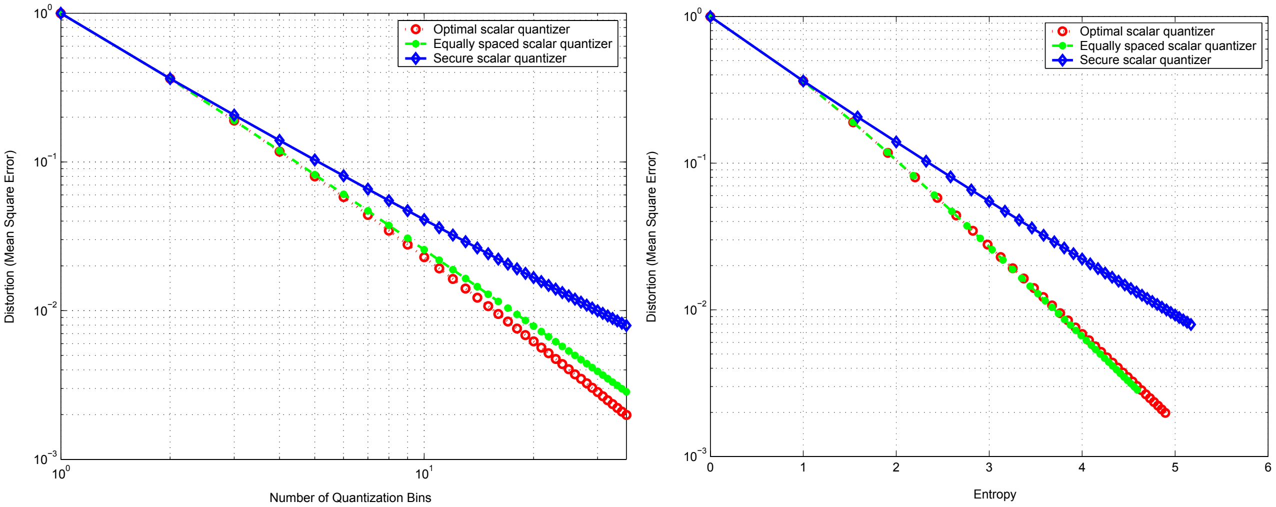

Figure 3: (a) Number of Quantization Bins vs. MSE Distortion for Standard Normal RV; (a) Entropy vs. MSE Distortion for Standard Normal RV

7. REFERENCES

[1] R. Ahlswede and I. Csiszár. Common randomness in information theory and cryptography - part I: Secret sharing. *IEEE Trans. on Information Theory*, 39(4):1121–1132, July 1993.

[2] J. Barros and S. D. Servetto. On the rate-distortion region for separate encoding of correlated sources. In *IEEE International Symposium on Information Theory*, page 171, Yokohama, Japan, June 29 - July 4 2003.

[3] C. H. Bennett, G. Brassard, C. Crépeau, and U. M. Maurer. Generalized privacy amplification. *IEEE Trans. on Information Theory*, 41(6):1915–1923, November 1995.

[4] T. Berger, Z. Zhang, and H. Viswanathan. The CEO problem. *IEEE Trans. on Information Theory*, 42(3):887 – 902, May 1996.

[5] T. M. Cover and J. A. Thomas. *Elements of Information Theory*. John Wiley & Sons, Inc., 2nd edition, 2006.

[6] I. Deslauriers. Distributed encryption and the Slepian-Wolf theorem. In *Canadian Conference on Electrical and Computer Engineering*, pages 93–97, Saskatoon, Sask., Canada, May 2005.

[7] B. Furht, D. Socek, and A. M. Eskicioglu. *Multimedia Security Handbook*, chapter 3. Fundamentals of Multimedia Encryption Techniques, pages 95–132. CRC Press, 2005.

[8] O. Goldreich. *Foundations of Cryptography: Basic Tools*, volume I. Cambridge University Press, 2001.

[9] K. B. Housewright. *Source Coding Studies for Multiterminal Systems*. PhD thesis, University of California, Los Angeles, 1977.

[10] R. M. Kahn. *Privacy in Multi-user Information Theory*. PhD thesis, Stanford University, 1979.

[11] E. D. Karnin, J. W. Greene, and M. E. Hellman. On secret sharing systems. *IEEE Trans. on Information Theory*, 29(1):35–41, January 1983.

[12] O. Koval, S. Voloshynovskiy, T. Holotyak, and T. Pun. Information-theoretic analysis of steganalysis in real images. In *ACM Multimedia & Security Workshop*, Geneva, Switzerland, September 26–27 2006.

[13] L. Lai, H. E. Gamal, and H. V. Poor. The wiretap channel with feedback: Encryption over the channel. *IEEE Trans. on Information Theory*, 2007. submitted.

[14] S. K. Leung-Yan-Cheong. *Multi-User and Wire-Tap Channels Including Feedback*. PhD thesis, Stanford University, Stanford, CA, 1976.

[15] S. P. Lloyd. Least squares quantization in PCM. *IEEE Trans. on Information Theory*, 28(2):129–137, March 1982.

[16] W. Luh and D. Kundur. Distributed keyless secret sharing over noiseless channels. In *IEEE Globecom*, Washington, D.C., November 25–30 2007.

[17] W. Luh and D. Kundur. Separate enciphering of correlated messages for confidentiality in distributed networks. In *IEEE Globecom*, Washington, D.C., November 25–30 2007.

[18] U. M. Maurer. Secret key agreement by public discussion from common information. *IEEE Trans. on Information Theory*, 39(3):733–742, May 1993.

[19] J. Max. Quantizing for minimum distortion. *IRE Trans. on Information Theory*, 6:7–12, March 1960.

[20] M. Naor and A. Shamir. Visual cryptography. In *Advances in Cryptology - EUROCRYPT '94. Workshop on the Theory and Application of Cryptographic Techniques. Proceedings*, pages 1 – 12, 1995.

[21] A. Nosratinia, G. Davis, Z. Xiong, and R. Rajagopalan. *Wavelet, subband and block transforms in communications and multimedia*, chapter Subband Image Compression, pages 1 –49. Kluwer, 1999.

[22] S. Pradhan and K. Ramchandran. Distributed source coding: Symmetric rates and applications to sensor networks. In *Proc. DCC'00*, Snowbird, UT, March 2000.

[23] L. Qiao and K. Nahrstedt. A new algorithm for MPEG video encryption. In *International Conference*

on Imaging Science, Systems and Technology, pages 21–29, 1997.

[24] A. Shamir. How to share a secret. In *Communications of the ACM 22*, number 11, pages 612–613, November 1979.

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

[26] Y. Q. Shi and H. Sun. *Image and Video Compression for Multimedia Engineering - Fundamentals, Algorithms, and Standards.* CRC Press, 2003.

[27] D. Slepian and J. K. Wolf. Noiseless coding of correlated information sources. *IEEE Trans. Inform. Theory*, 19(4):471–480, July 1973.

[28] D. R. Stinson. *Cryptography: Theory and Practice.* Chapman and Hall, 1st edition, 1995.

[29] S.-Y. Tung. *Multiterminal Source Coding.* PhD thesis, Cornell University, 1978.

[30] A. D. Wyner. The wire-tap channel. *The Bell System Technical Journal*, 54(8):1355–1387, October 1975.

[31] H. Yamamoto. On secret sharing communication systems with two or three channels. *IEEE Trans. on Information Theory*, 32(3):387–393, May 1986.

[32] H. Yamamoto. Rate-distortion theory for the Shannon cipher system. *IEEE Trans. on Information Theory*, 43(3):827–835, May 1997.

APPENDIX

A. PROOFS

The proofs in this appendix rely heavily on previous work. We shall only present portions of the proofs that are novel to this paper, while referencing previous works to avoid lengthy re-derivations.

A.1 Proof of DSS Capacity Region

The proof of Theorem 1 is based on our previous work in which reconstruction is distortionless, thus we shall skip most of the details found in [16] and provide only novel details pertaining to the addition of the non-zero distortion.

First we show the inequalities defining $\mathcal{R}_{DSS}(D)$ are necessary, i.e. a point (d_A, d_B, r_A, r_B) achievable w.r.t. D *must* be in $\mathcal{R}_{DSS}(D)$. In [16] we implicitly showed

$$H(S^k|W_A) + H(S^k|W_B) \leq H(S^k) + H(S^k|\hat{S}^k). \qquad (49)$$

Now

$$\begin{aligned} H(S^k|\hat{S}^k) &= H(S^k) - I(S^k;\hat{S}^k) \\ &\leq H(S^k) - kR(D) \qquad (50) \end{aligned}$$

by using Eq. 20. Substituting Eq. 50 into Eq. 49, using the definition of equivocation rate (cf. Eqs. 9 and 10) and using the fact that $\frac{1}{k}H(S^k) = H(S)$ since the source is a DMS, establishes one of the desired inequalities

$$\Delta_A + \Delta_B \leq 2H(S) - R(D). \qquad (51)$$

In [16] we also showed Eq. 52.

$$\begin{aligned} R_A + R_B &\geq \frac{1}{k}I(S^k;W_A,W_B) \qquad (52) \\ &\overset{(a)}{\geq} \frac{1}{k}I(S^k;\hat{S}^k) \\ &\overset{(b)}{\geq} R(D) \end{aligned}$$

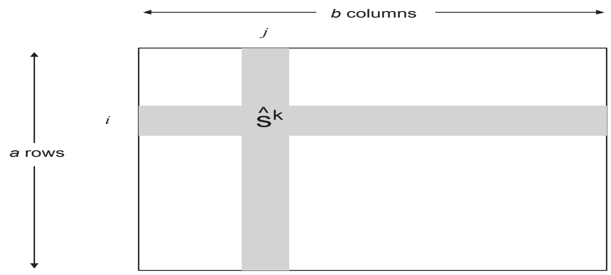

Figure 4: Second Stage of Coding After Compression

The above inequalities arise from: (a) $S^k \leftrightarrow (W_A, W_B) \leftrightarrow \hat{S}^k$ and the data processing inequality; (b) follows Eq. 20. The other inequalities of $\mathcal{R}_{DSS}(D)$ are derived in exactly the same way as those from [16], while some are basic entropy inequalities.

Next we show that any point in $\mathcal{R}_{DSS}(D)$ is achievable, i.e. their exists encoders/decoder (f_A, f_B, φ) for any point in $\mathcal{R}_{DSS}(D)$. The encoders are deterministic and follow a *two-stage* construction. In the first stage, for a given D, both Alice and Bob compress their shared message S^k to the rate-distortion limit. By the proof of the rate-distortion theorem, as $k \to \infty$, the compressed result $\hat{S}^k$ can be represented by approximately $kR(D)$ bits, such that each typical realization $\hat{s}^k$ has approximately the same probability (i.e. almost uniformly distributed).

The second stage is the table construction from [16]. Each of the (almost) equally likely typical realizations $\hat{s}^k$ are arranged in a table such that the number of rows and columns define the rates for Alice and Bob. Fig. 4 shows an example of the table for the second stage. Let $a \times b \approx 2^{kR(D)}$. If $\hat{s}^k$ is to be sent to the BS, Alice sends index i, giving a rate of $\frac{\log_2 a}{k}$ and Bob sends index j, giving a rate of $\frac{\log_2 b}{k}$. If Eve intercepts i, she still has to guess one of the b columns (along the horizontal gray) bar, and hence her equivocation rate is $\Delta_A = \frac{\log_2 b}{k} + (H(S) - R(D))$. The extra $H(S) - R(D)$ term arises from the fact that lossy compression removes $k(H(S) - R(D))$ bits that Eve will never recover (neither will the BS) [32]. On the other hand if Eve intercepts j, she still has to guess one of the a rows (along the vertical gray bar), and hence her equivocation rate is $\Delta_B = \frac{\log_2 a}{k} + (H(S) - R(D))$. The reader can check the rates and equivocation rates satisfy the boundaries (limits of the inequalities) of $\mathcal{R}_{DSS}(D)$. Therefore, any rates and equivocation rates lying strictly inside $\mathcal{R}_{DSS}(D)$ can also be achieved, since the boundaries denote the optimal operating scenario.

Interpretation of Proof

Intermediate stages of the necessity proof (not shown above) resulting only from the use of Eq. 50 and the data processing inequality are given by the following equations.

$$\Delta_A + \Delta_B \leq 2H(S) - R(D) - \frac{1}{k}I(W_A;W_B) \qquad (53)$$

$$R_A + R_B \geq R(D) + \frac{1}{k}I(W_A;W_B) \qquad (54)$$

$$R_j + \Delta_j \geq H(S) + \frac{1}{k}H(T_j|S^k), \quad j = A, B \qquad (55)$$

However, the inequalities for the capacity region $\mathcal{R}_{DSS}(D)$ differ from Eqs. 53 to 55. It can be seen that by making $I(W_A; W_B) = 0$, the first two inequalities (Eqs. 53 and 54) are improved (i.e. higher equivocation rates, lower source coding rates). The interpretation is that optimality is achieved by making Alice and Bob's encoded messages independent. This makes sense since if Eve only intercepts Alice's encoded message, its independence from Bob's message imply Eve will be ignorant of Bob's message. Secondly, by eliminating statistical overlap, the allocation of bits for each user's message results in lower rates; this idea is similar to the SW theorem [27] in that one user is required to only code the information *not* contained in the side-information present at the decoder.

We can also conclude that stochastic encoders provide us with no advantage. The equivocation rate is not increased by T_A, T_B as seen through Eq. 53, nor does it decrease the source coding rate as seen through Eq. 54. Thus if the encoders are determinstic, we can decrease the lower bound in Eq. 55.

The two-stage encoding technique outlined in the achievability proof, i.e. source coding (compression) followed by secrecy coding, can also be found in [32]. A similar table construct from the second stage can also be found in [31]. The important aspect of the proof is that practical systems with non-zero distortion criteria should first compress the input, and then secrecy code the compressed signal. This also follows the general philosophy in [25] for key-based cryptography in which lowering redundancy improves equivocation of key, i.e. $(H(K) - H(K|E) \leq \log_2 |\mathcal{M}| - H(M)$, where K is the key, E is the cryptogram, $M \in \mathcal{M}$ is the message).

A.2 Proof of the Outer Region for DE

Most of the inequalities in the outer region

$$\mathcal{R}_{DE-out}(D_A, D_B)$$

follow from [29, 9] except for Eq. 27. As for the other inequalities we only prove that they still hold for stochastic encoding ([29] proves them for determinstic encoders).

To derive Eq. 27, write

$$\begin{aligned} & H(S_A^k, S_B^k) \\ = \; & H(S_A^k, S_B^k | W_A, W_B) + I(S_A^k, S_B^k; W_A, W_B). \quad (56) \end{aligned}$$

In [17] we upper bounded the second term in Eq. 56 with the following inequality

$$\begin{aligned} & I(S_A^k, S_B^k; W_A, W_B) \\ \leq \; & H(S_A^k) + H(S_B^k) - H(S_A^k|W_A) - H(S_B^k|W_B). (57) \end{aligned}$$

Eq. 56 can also be rearranged as follows.

$$H(S_A^k, S_B^k|W_A, W_B) = H(S_A^k, S_B^k) - I(S_A^k, S_B^k; W_A, W_B) \quad (58)$$

In [29] a lower bound for $I(S_A^k, S_B^k; W_A, W_B)$ is derived for determinstic encoders as

$$I(S_A^k, S_B^k; W_A, W_B) \geq kI(X_A, X_B; Y_A, Y_B) \quad (59)$$

for some $(Y_A, Y_B) \in \mathcal{P}(D_A, D_B)$. It can easily be verified that Eq. 59 also holds for stochastic encoders by proving $(Y_{A,i}, Y_{B,i}) \in \mathcal{P}(\delta_{A,i}, \delta_{B,i})$ where

$$\begin{aligned} Y_{A,i} & \triangleq (S_A^{i-1}, S_B^{i-1}, W_A) & (60) \\ Y_{B,i} & \triangleq (S_A^{i-1}, S_B^{i-1}, W_B) & (61) \\ \delta_{A,i} & \triangleq E[\rho_A(S_{A,i}, \hat{S}_{A,i})] & (62) \\ \delta_{B,i} & \triangleq E[\rho_A(S_{B,i}, \hat{S}_{B,i})] & (63) \end{aligned}$$

and that $\mathcal{R}_{DE-out}(D_A, D_B)$ is convex (proved in [9]). Therefore using Eq. 59, Eq. 58 becomes

$$\begin{aligned} & H(S_A^k, S_B^k|W_A, W_B) \\ \leq \; & H(S_A^k, S_B^k) - kI(X_A, X_B; Y_A, Y_B). \quad (64) \end{aligned}$$

Now combining Eqs. 57 and 64 into Eq. 56 and then rearranging gives

$$\begin{aligned} & H(S_A^k|W_A) + H(S_B^k|W_B) \\ \leq \; & H(S_A^k) + H(S_B^k) - kI(X_A, X_B; Y_A, Y_B). \quad (65) \end{aligned}$$

Dividing by k yields Eq. 27.

As mentioned above, in order to apply results from [29], we must prove the inequalities from [29] also apply under stochastic encoding. Towards this end, we prove

$$(Y_{A,i}, Y_{B,i}) \in \mathcal{P}(\delta_{A,i}, \delta_{B,i})$$

for all $i = 1, \ldots, k$. First we show (i) in Def. 1 is satisfied.

$$\begin{aligned} & I(Y_{A,i}; S_{B,i}|S_{A,i}) \\ = \; & I(S_{B,i}; Y_{A,i}, S_{A,i}) - I(S_{A,i}; S_{B,i}) \\ \overset{(a)}{=} \; & I(S_{B,i}; S_A^{i-1}, S_B^{i-1}, W_A, S_{A,i}) - I(S_{A,i}; S_{B,i}) \\ \overset{(b)}{\leq} \; & I(S_{B,i}; S_A^{i-1}, S_B^{i-1}, S_A^k, T_A, S_{A,i}) - I(S_{A,i}; S_{B,i}) \\ = \; & I(S_{B,i}; S_A^k, T_A) - I(S_{A,i}; S_{B,i}) \\ \overset{(c)}{=} \; & I(S_{B,i}; S_{A,i}) + I(S_{B,i}; T_A|S_A^k) - I(S_{A,i}; S_{B,i}) \\ \overset{(d)}{=} \; & 0 \qquad (66) \end{aligned}$$

The explanations of the above are: (a) from applying Eq. 60; (b) from applying Eq. 2; (c) the sources are DMS; (d) $T_A \leftrightarrow S_A^k \leftrightarrow S_B^k$ form a Markov chain since T_A is locally generated by Alice. Eq. 66 shows $Y_{A,i} \leftrightarrow S_{A,i} \leftrightarrow S_{B,i}$ forms a Markov chain (the other Markov chain in (i) can be proved the same way), thus satisfying (i) of Def. 1. To show (ii), let $\hat{S}_{A,i} = F_{A,i}(Y_{A,i}, Y_{B,i})$ be the i^{th} letter of $\varphi_A(W_A, W_B)$, which is possible to define since $Y_{A,i}$, $Y_{B,i}$ contain W_A, W_B resp. via Eqs. 60 and 61. Therefore $E[\rho_A(S_{A,i}, \hat{S}_{A,i})] = \delta_{A,i}$, and using the same argument $E[\rho_B(S_{B,i}, \hat{S}_{B,i})] = \delta_{A,i}$. Therefore by Def. 1 $(Y_{A,i}, Y_{B,i}) \in \mathcal{P}(\delta_{A,i}, \delta_{B,i})$ for all $i = 1, \ldots, k$. Stochastic encoding does not affect the rest of the results found in [29, 9] required for our proof, thus the proof is complete by referring to the proofs in [29, 9].

A.3 Proof of the Inner Region for DE

Eqs. 36 to 38 are directly from [2], and since there is no need to use stochastic encoding as seen in Theorem 2 and its proof in Appendix A.2, we do not attempt to adapt the proof for stochastic encoding. Thus only Eq. 35 needs to be proved.

One can achieve the equivocation sum bound promised by Eq. 35 without any secrecy coding. If Alice and Bob each compress their messages to the boundaries promised by Eqs. 36 to 38 for some $(Y_A, Y_B) \in \mathcal{P}(D_A, D_B)$, then it is easy to see that

$$\begin{aligned}\Delta_A + \Delta_B &= H(S_A) - R_A + H(S_B) - R_B \\ &= H(S_A) + H(S_B) - H(S_A, S_B) \\ &\quad + H(S_A|S_B, Y_A) + H(S_B|S_A, Y_B) \quad (67)\end{aligned}$$

where the first equality follows since approximately

$$k(H(S_A) - R_A)$$

bits (for k sufficiently large) are unknown to Eve given she possess the kR_A bits of W_A, and similarly $k(H(S_B) - R_B)$ bits for Bob. The second equality follows by using Eq. 38 with equality. Eq. 67 is also equal to the upper bound in Eq. 35.

A.4 BS Feedback Proofs

Case 110

For the following discussion, suppose the BS knows Eve intercepted W_A, which we will denote as $\tilde{W}_A$, where the tilde is used to indicate a previous round (the reader can prove the other case when the BS knows Eve intercepted $\tilde{W}_B$ using the same method). We put forth a lemma which helps us show there is no advantage in feedback from the **BS to Alice**.

Lemma 2. *If*

$$I(\tilde{S}_A^k; \tilde{W}_A, \tilde{W}_B|\tilde{W}_A) \leq k\tilde{\Delta}_A - H(\tilde{S}_A^k|\tilde{W}_A, \tilde{W}_B) \quad (68)$$

then feedback from BS to Alice provides no advantage, given the BS knows Eve possesses $\tilde{W}_A$.

Proof. Without feedback, Alice can distill a secret key (from $\tilde{S}_A^k$ and $\tilde{W}_A$) of length $k\tilde{\Delta}_A$ bits that is independent of $\tilde{W}_A$. However since the BS reconstruction is distorted, Alice's secret key must be reduced by $H(\tilde{S}_A^k|\tilde{W}_A, \tilde{W}_B)$, which represents the unrecoverable distortion. Thus Alice and the BS can distill a secret key without feedback of length given by the right hand side (RHS) of Eq. 68.

Theorem 3 of [1] shows that through feedback from the BS to Alice, a secret key of *maximum* length $I(\tilde{S}_A^k; \tilde{W}_A, \tilde{W}_B|\tilde{W}_A)$ bits can be established. Thus feedback from the BS to Alice given the BS knows Eve posses Alice's $\tilde{W}_A$ results in a secret key of maximum length given by the left hand side (LHS) of Eq. 68.

Clearly, if a secret key derived using feedback has length less than or equal to a secret key derived without feedback, then feedback offers no advantage; this represents Eq. 68. Furthermore, both keys cannot be used at the same time since they are both derived from $\tilde{S}_A^k$ and $\tilde{W}_A$. □

We can show that Lemma 2 is true, and thus feedback provides no advantage.

$$\begin{aligned}I(\tilde{S}_A^k; \tilde{W}_A, \tilde{W}_B|\tilde{W}_A) &= H(\tilde{S}_A^k|\tilde{W}_A) - H(\tilde{S}_A^k|\tilde{W}_A, \tilde{W}_B) \\ &= k\tilde{\Delta}_A - H(\tilde{S}_A^k|\tilde{W}_A, \tilde{W}_B) \quad (69)\end{aligned}$$

Thus Lemma 2 is true and feedback from the BS to Alice provides no advantage.

Next, under the same assumption that the BS knows Eve has $\tilde{W}_A$, we show that feedback from the **BS to Bob** has no advantage either. Let

$$m \triangleq I(\tilde{S}_B^k; \tilde{W}_A, \tilde{W}_B|\tilde{W}_A) \quad (70)$$

where m is the maximum number of bits of secret key that can be established between the BS and Bob through feedback, given the BS knows Eve posses $\tilde{W}_A$ [1]. In this case, it can be shown that m does *not* satisfy a modified Lemma 2 (for Bob instead of Alice). However Lemma 2 (and a modified version for Bob) provides a sufficient condition only, and thus failure to satisfy the condition in Lemma 2 does not imply there is an advantage using feedback.

Again, let tilde variables represent the previous round, while non-tilde variables represent the current round. To analyze the benefits of feedback, let $kR_B \geq m$, which allows the secret key derived through feedback to be fully used. Let W_B denote Bob's current enciphered message *without* feedback, and let W_B^F denote Bob's current enciphered message *using* feedback Z_B. Then

$$k\Delta_B^F = k\Delta_B + m \quad (71)$$

which results because the m bits of the secret key can be used as a one-time pad. For example, suppose W_B is in binary form, and $W_{B,1}$ is the first m bits of W_B, while $W_{B,2}$ is last $kR_B - m$ bits of W_B. Then

$$W_B^F = (W_{B,1} \oplus K_B, W_{B,2}) \quad (72)$$

where K_B is the m-bit key created from feedback.

In order for an improvement in equivocation using feedback, we must show

$$\begin{aligned}H(S_B^k, \tilde{S}_B^k|Z_B, W_B^F, \tilde{W}_A) &> H(S_B^k, \tilde{S}_B^k|W_B, \tilde{W}_A) \\ &= H(\tilde{S}_B^k|\tilde{W}_A) + H(S_B^k|W_B). \\ &\qquad (73)\end{aligned}$$

The previous message block $\tilde{S}_B^k$ must be considered since the feedback Z_B is a function of $\tilde{S}_B^k$. Next we upper bound the LHS of Eq. 73.

$$\begin{aligned}&H(S_B^k, \tilde{S}_B^k|Z_B, W_B^F, \tilde{W}_A) \\ =\ & H(\tilde{S}_B^k|Z_B, W_B^F, \tilde{W}_A) + H(S_B^k|\tilde{S}_B^k, Z_B, W_B^F, \tilde{W}_A) \\ \leq\ & H(\tilde{S}_B^k|Z_B, \tilde{W}_A) + H(S_B^k|\tilde{S}_B^k, Z_B, W_B^F, \tilde{W}_A) \\ =\ & \Big(H(\tilde{S}_B^k|\tilde{W}_A) - I(\tilde{S}_B^k; Z_B|\tilde{W}_A)\Big) \\ & + \Big(H(S_B^k|W_B^F) - I(S_B^k; \tilde{S}_B^k, Z_B, \tilde{W}_A|W_B^F)\Big) \\ =\ & H(\tilde{S}_B^k|\tilde{W}_A) - I(\tilde{S}_B^k; Z_B|\tilde{W}_A) + \Big(H(S_B^k|W_B) + m\Big) \\ & - I(S_B^k; \tilde{S}_B^k, Z_B, \tilde{W}_A|W_B^F) \quad (74)\end{aligned}$$

The last equality follows from Eq. 71. Next we bound the final term in Eq. 74.

$$\begin{aligned}& I(S_B^k; \tilde{S}_B^k, Z_B, \tilde{W}_A|W_B^F) \\ \overset{(a)}{\geq}\ & I(S_B^k; K_B|W_B^F) \\ \overset{(b)}{=}\ & H(K_B|W_{B,1} \oplus K_B, W_{B,2}) \\ & - H(K_B|S_B^k, W_{B,1} \oplus K_B, W_{B,2}) \\ \overset{(c)}{=}\ & H(K_B|W_{B,1} \oplus K_B) \\ & - H(K_B|S_B^k, W_{B,1}, K_B, W_{B,2}) \\ \overset{(d)}{=}\ & H(K_B) = m \quad (75)\end{aligned}$$

The explanations are: (a) from the fact that K_B can be derived from $\tilde{S}_B^k$ and Z_B by Bob; (b) from Eq. 72; (c) $W_{B,2}$ is assumed to be independent of K_B and $W_{B,1}$, and $W_{B,1}$

can be derived from S_B^k (determinstic encoding); (d) K_B is used as a one-time pad [1].

Combining Eq. 75 into Eq. 74 shows Eq. 73 is not satisfied, thus feedback does not offer any advantage. In fact when $I(\tilde{S}_B^k; Z_B|\tilde{W}_A) > 0$ in Eq. 74, feedback strictly performs worst than no feedback.

This proves the case when the BS knows Eve possesses $\tilde{W}_A$. The other case when the BS knows Eve posses $\tilde{W}_B$ can be proved in the same way.

*Case 0*0*

We analyze the 010 case, while the result for the 000 case follows from the 010 case. Suppose the BS knows Eve possess W_A. Theorem 3 of [1] shows that a secret key of maximum length $I(S_j^k; M|W_A)$ bits may be distilled, where M is a RV generated by the BS independent of all messages and received material. This quantity is 0 since M is independent, and thus artificial feedback produces no shared secret key.

B. PARAMETERS FOR SECURE QUANTIZER

The secure quantizer for $\mathcal{N}(0, \sigma^2)$ is designed so that all bins have equal probability. This requirement automatically gives the decision levels. The reconstruction levels are computed to minimize the MSE distortion given the decision levels. Since the zero-mean Gaussian distribution is symmetric, we provide the decision and reconstruction levels for the positive side only, following [15, 19].

Let N be the number of desired bins. If N is odd, then the decision levels can be computed as

$$\begin{aligned} x_0 &= \sigma\sqrt{2}\,\mathrm{erf}^{-1}\left(\frac{1}{N}\right) \\ x_i &= \sigma\sqrt{2}\,\mathrm{erf}^{-1}\left(\frac{2i}{N}+\frac{1}{N}\right),\ i=1,\ldots,\frac{N-1}{2} \end{aligned} \tag{76}$$

and the reconstruction levels y_i defined to be for the interval $[x_{i-1}, x_i]$ are given by

$$\begin{aligned} y_0 &= 0 \\ y_i &= \sigma N \int_{x_{i-1}}^{x_i} x\frac{1}{\sqrt{2\pi}}e^{-\frac{x^2}{2}}dx,\ i=1,\ldots,\frac{N-1}{2}. \end{aligned} \tag{77}$$

If N is even, then the decision levels can be computed as

$$x_i = \sigma\sqrt{2}\,\mathrm{erf}^{-1}\left(\frac{2i}{N}\right),\ i=0,\ldots,\frac{N}{2} \tag{78}$$

and the reconstruction levels y_i defined to be for the interval $[x_i, x_{i+1}]$ are given by

$$y_i = \sigma N \int_{x_i}^{x_{i+1}} x\frac{1}{\sqrt{2\pi}}e^{-\frac{x^2}{2}}dx,\ i=0,\ldots,\frac{N}{2}. \tag{79}$$

Fig. 3 is for a zero-mean, unit-variance normal distribution. To use Fig. 3 for $\mathcal{N}(0, \sigma^2)$, the MSE distortion is multiplied by σ^2. The derivation of the above is trivial, thus omitted.