Distributed Keyless Secret Sharing over Noiseless Channels

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

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

***Abstract*—In traditional secret sharing, a central trusted authority must divide a secret into multiple parts, called shares, such that the secret can only be recovered when a certain number of shares are available for reconstruction [1], [2]. In this paper, we consider a secret sharing problem in which each share must be created separately by independent entities such that no collaboration or shared cryptographic keys are required; we call this the distributed keyless secret sharing problem. For this problem, general tradeoffs between compression and secrecy are characterized yielding the impossibility result that perfect secrecy is unachievable. In response to this impossibility, we define a practical measure of secrecy and design a low-cost solution based on this measure of secrecy.**

I. Introduction and Motivation

We consider the sensor network (SN) problem in which a cluster of sensors compress and encrypt *common* observed information and then each sensor relays its encrypted share to a base station or a local cluster head. We assume that the sensors cannot communicate with one another (thus they must encrypt *in situ* without direct aid from other sensors), nor do they use any cryptographic keys for encryption. Any encryption methodology and associated parameters used by the sensors to separately encrypt the secret information are known by an eavesdropper, who is able to eavesdrop on *only* a small subset of the sensors. This assumption is reasonable when the legitimate SN is large or the sensors are physically separated, making comprehensive eavesdropping difficult. In addition, in the case where the eavesdropper has enough resources to intercept all legitimate SN communications, the eavesdropper may as well deploy his own SN instead of consuming resources in attacking the legitimate SN.

The SN problem presented above is related to the problems of conventional secret sharing [1], [2] and that of the wiretap channel II [3], [4]. The main difference is that in our problem the creation of shares is performed by separate entities that do not share *any* keys or common randomness, which is in contrast to existing research in which a *central* authority may exploit randomness to achieve secrecy.

In Sect. II, we introduce notation and formulate the problem. Sect. III provides novel analysis to study the associated optimal compression-secrecy trade-off, resulting in an impossibility statement: perfect secrecy is not achievable. Sect. IV first presents a practical measure of secrecy given that Sect. III established perfect secrecy is impossible, then presents an innovative cost-effective encoder implementation for this practical measure of secrecy.

II. Preliminaries

A. Notation

Unless otherwise stated, let upper-case letters denote random variables, e.g. X, caligraphic upper-case letters denote finite sets, e.g. $\mathcal{X}$, lower-case letters denote realizations, e.g. x, and superscripted letters denote vectors, e.g. x^n. The probability mass function (pmf) 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. $\mathbf{A}$.

B. Problem Formulation

Consider the simplified scenario with two sensors called Alice and Bob. Let Alice and Bob share the same message $S^k \in \mathcal{S}^k$ created by a discrete memoryless source (DMS) in (1).

$$P_S^k(s^k) = \prod_{i=1}^{k} P_S(s_i) \tag{1}$$

Our problem is summarized in Fig. 1. Alice and Bob are to each encipher their S^k *separately without cooperation* creating $X_A^n \in \mathcal{X}_A^n$ and $X_B^N \in \mathcal{X}_B^N$, respectively (note, n and N may be different, and N is not a RV). The base station receives

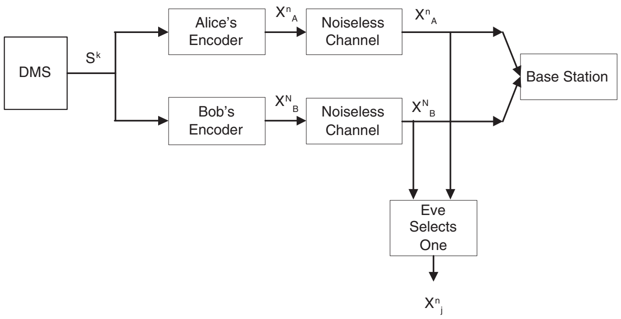

Fig. 1. Separate enciphering by Alice and Bob with eavesdropping by Eve.

1930-529X/07/$25.00 © 2007 IEEE
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE GLOBECOM 2007 proceedings.

both X_A^n and X_B^N, and its goal is to reconstruct S^k error-free with high probability. Let the triple (f_A, f_B, φ) denote Alice's (possibly stochastic) encoder, Bob's (possibly stochastic) encoder, and the base station's decoder respectively. Here $f_A : \mathcal{S}^k \to \mathcal{X}_A^n$, $f_B : \mathcal{S}^k \to \mathcal{X}_B^N$, and $\varphi : \mathcal{X}_A^n \times \mathcal{X}_B^N \to \mathcal{S}^k$ such that f_A, f_B do not depend on any shared materials or common randonmness. The rate of Alice and Bob's enciphered messages are defined as

$$R_A \triangleq \frac{\log_2 \|f_A\|}{k} \tag{2}$$

$$R_B \triangleq \frac{\log_2 \|f_B\|}{k}. \tag{3}$$

Here $\|f_A\|$ is the notation denoting the number of possible outputs from Alice's encoder and similarly $\|f_B\|$ for Bob's encoder.

In Fig. 1, the eavesdropper Eve is allowed to select either X_A^n or X_B^N, but not both. Depending on which enciphered message Eve selects, the equivocation rate of Eve with respect to (w.r.t.) Alice and Bob are defined as

$$\Delta_A \triangleq \frac{H(S^k|X_A^n)}{k} \tag{4}$$

$$\Delta_B \triangleq \frac{H(S^k|X_B^N)}{k}. \tag{5}$$

An equivocation rate of $H(S)$ is desired as this implies $H(S^k|X_j^n) = kH(S) = H(S^k)$ (last equality follows since source is a DMS) for $j = A$ or $j = B$, which means Eve is no better off with X_j^n than she was without it.

We say a quadruple (d_A, d_B, r_A, r_B) (corresponding to $(\Delta_A, \Delta_B, R_A, R_B)$) is *achievable* if there exists a (f_A, f_B, φ) such that for *all* $\epsilon > 0$ and k sufficiently large the following are satisfied:

$$Pr\{S^k \neq \hat{S}^k\} \leq \epsilon \tag{6}$$

$$R_A \leq r_A + \epsilon \tag{7}$$

$$R_B \leq r_B + \epsilon \tag{8}$$

$$d_A - \epsilon \leq \Delta_A \leq d_A \tag{9}$$

$$d_B - \epsilon \leq \Delta_B \leq d_B \tag{10}$$

where

$$X_A^n = f_A(S^k) \tag{11}$$

$$X_B^N = f_B(S^k) \tag{12}$$

$$\hat{S}^k = \varphi(X_A^n, X_B^N). \tag{13}$$

Knowledge of (f_A, f_B, φ) and any other data stored on Alice and Bob's sensors as well as at the base station are known to all parties including Eve, hence no cryptographic keys of any sort are allowed.

Ideally one desires $(d_A, d_B, r_A, r_B) = (H(S), H(S), r_A, r_B)$ for small positive r_A and r_B, because having an equivocation rate of $H(S)$ implies perfect secrecy, while having small rates means less communications overhead. However, we shall see that perfect secrecy is impossible, no matter what finite rates are used by Alice and Bob's encoders.

III. The Capacity Region

The capacity region $\mathcal{R}$, defined to be the closure of the set of rate quadruples (d_A, d_B, r_A, r_B) that are achievable (see Sect. II-B), is described in Theorem 1 for the general distributed keyless secret sharing problem.

Theorem 1: The capacity region is given by

$$\mathcal{R} = \{(d_A, d_B, r_A, r_B) : 0 \leq d_A + d_B \leq H(S),$$
$$r_A + r_B \geq H(S), r_A + d_A \geq H(S), r_B + d_B \geq H(S)\}. \tag{14}$$

Theorem 1 also gives us the impossibility result that unconditional secrecy cannot be achieved by both Alice and Bob simultaneously. Fig. 2 shows the achievable (Δ_A, Δ_B) equivocation pair given rates satisfying Theorem 1; if Alice's enciphered message is unconditionally secure, i.e. $\Delta_A = H(S)$, then necessarily Bob's enciphered message will have no secrecy whatsoever, i.e. $\Delta_B = 0$ (point A in Fig. 2).

A. Proof of Converse Part of Theorem 1

First we show (15) holds.

$$X_B^N \leftrightarrow S^k \leftrightarrow X_A^n. \tag{15}$$

Without loss of generality, let $f_B(S^k) = f'_B(S^k, T_B)$ where f'_B is a determinstic function, and T_B is a random variable generated locally that may depend on the input s^k, but independent of the stochastic encoder f_A in following with the lack of common randomness assumption. Therefore

$$H(f_A(S^k)|S^k, T_B) = H(f_A(S^k)|S^k) \tag{16}$$

and

$$\begin{aligned} & I(X_A^n; X_B^N|S^k) \\ = \; & I(f_A(S^k); f_B(S^k)|S^k) \\ = \; & H(f_A(S^k)|S^k) - H(f_A(S^k)|S^k, f'_B(S^k, T_B)) \\ \leq \; & H(f_A(S^k)|S^k) - H(f_A(S^k)|S^k, T_B) = 0 \end{aligned} \tag{17}$$

so (15) holds.

Next, assume that some (d_A, d_B, r_A, r_B) is achievable such that (6) to (13) are satisfied with the Markov constraint in (15).

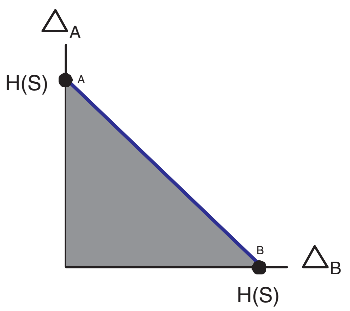

Fig. 2. The capacity region $\mathcal{R}$ for rates satisfying Theorem 1.

1930-529X/07/$25.00 © 2007 IEEE

Then we shall show that the following bounds

$$\begin{aligned} d_A + d_B &\leq H(S) \quad (18)\\ r_A + r_B &\geq H(S) \quad (19)\\ r_A + d_A &\geq H(S) \quad (20)\\ r_B + d_B &\geq H(S) \quad (21)\end{aligned}$$

are necessarily true.

First we prove (18). To make use of (6), we call upon Fano's inequality

$$\begin{aligned} H(S^k|\hat{S}^k) &\leq h(\epsilon) + \epsilon k \log_2 |\mathcal{S}| \triangleq k\epsilon_k \\ &\triangleq k\epsilon_k \quad (22)\end{aligned}$$

where $Pr\{S^k \neq \hat{S}^k\} < \epsilon$, $k\epsilon_k \to 0$ as $k \to \infty$ and $h(p)$ is the entropy function defined as

$$h(p) = -p \log_2 p - (1-p)\log_2(1-p). \quad (23)$$

$$\begin{aligned} H(S^k) &= H(S^k|\hat{S}^k) + I(S^k;\hat{S}^k) \\ &\overset{(a)}{\leq} k\epsilon_k + I(S^k;\hat{S}^k) \\ &\overset{(b)}{\leq} k\epsilon_k + I(S^k;X_A^n,X_B^N) \\ &\overset{(c)}{=} k\epsilon_k + I(S^k;X_A^n) + I(S^k;X_B^N|X_A^n) \\ &\overset{(d)}{=} k\epsilon_k + I(S^k;X_A^n) + I(S^k;X_B^N) - I(X_A^n;X_B^N) \\ &= k\epsilon_k + H(S^k) - H(S^k|X_A^n) + \\ &\quad H(S^k) - H(S^k|X_B^N) - I(X_A^n;X_B^N) \quad (24)\end{aligned}$$

The above (in)equalities arise from:

(a) Fano's inequality (see (22));

(b) $S^k \to (X_A^n, X_B^n) \to \hat{S}^k$ forms a Markov chain and usage of the data processing inequality;

(c) chain rule for mutual information;

(d) well-known identity $I(X;Y|Z) = I(X;Y) - I(X;Z)$ when $X \leftrightarrow Y \leftrightarrow Z$.

Now rearranging (24) gives

$$\begin{aligned} H(S^k|X_A^n) + H(S^k|X_B^N) &\leq H(S^k) - I(X_A^n;X_B^N) + k\epsilon_k \\ &\leq kH(S) + k\epsilon_k. \quad (25)\end{aligned}$$

Dividing by k and noting the definition of eqivocation rate (see (4) and (5)) results in

$$\Delta_A + \Delta_B \leq H(S) + \epsilon_k. \quad (26)$$

Finally employing (9) and (10) gives

$$\begin{aligned} (d_A - \epsilon) + (d_B - \epsilon) &\leq \Delta_A + \Delta_B \\ &\leq H(S) + \epsilon_k \quad (27)\end{aligned}$$

and letting $k \to \infty$ and $\epsilon \to 0$ we obtain the desired (18).

Next we show the rate sum bound of (19). Writing

$$\begin{aligned} 0 &\leq I(X_A^n;X_B^N) = H(X_A^n) + H(X_B^N) - H(X_A^n,X_B^N) \\ &\leq \log_2 |\mathcal{X}_A^n| + \log_2 |\mathcal{X}_B^n| - H(X_A^n,X_B^N) \\ &= \log_2 \|f_A\| + \log_2 \|f_B\| - H(X_A^n,X_B^N) \quad (28)\end{aligned}$$

where the second inequality follows since the maximum entropy of a set T is $\log_2 |T|$. Now dividing by k, and using the definition of the rate of enciphered messages (see (2) and (3)) gives

$$\begin{aligned} R_A + R_B &\geq \frac{1}{k} H(X_A^n,X_B^N) \\ &= \frac{1}{k}(H(S^k|X_A^n,X_B^N) + I(S^k;X_A^n,X_B^N)) \\ &\geq \frac{1}{k} I(S^k;X_A^n,X_B^N) \\ &\geq \frac{1}{k}(k(H(S) - \epsilon_k)) \quad (29)\end{aligned}$$

where the last step follows by working from (24b) back to the start of (24). Finally using (7) and (8) gives

$$\begin{aligned} (r_A + \epsilon) + (r_B + \epsilon) &\geq R_A + R_B \\ &\geq H(S) - \epsilon_k \quad (30)\end{aligned}$$

and letting $k \to \infty$ and $\epsilon \to 0$ we get the desired (19).

Finally we show the rate-equivocation sum bound for Alice, see (20), while noting the same follows for Bob. This follows simply from the chain rule for entropy

$$\begin{aligned} H(S^k) &= kH(S) \\ &\leq H(S^k, X_A^n) \\ &= H(X_A^n) + H(S^k|X_A^n) \\ &\leq \log_2 \|f_A\| + H(S^k|X_A^n). \quad (31)\end{aligned}$$

Now dividing by k and employing the definitions for rate and equivocation rate (see (2) and (4)), and then using the definition of achievability of these rates (see (7) and (9)) gives

$$\begin{aligned} H(S) &\leq R_A + \Delta_A \\ &\leq (r_1 + \epsilon) + d_1 \quad (32)\end{aligned}$$

and letting $\epsilon \to 0$ (since the definition requires for all $\epsilon > 0$), the desired (20) is obtained. ■

B. Proof Sketch of Direct Part of Theorem 1

We will show that any point on the line boundary in Fig. 2 (i.e. $\Delta_A + \Delta_B = H(S)$) along with boundaries $R_A + R_B = H(S)$, $R_A + \Delta_A = H(S)$, and $R_B + \Delta_B = H(S)$ of the overall capacity region are achievable.

We use the fact that when the block length k of S^k approaches infinity, almost all S^ks (approx. $2^{kH(S)}$) are strongly typical and are also almost equally likely [5].

Let us construct a $2^{nR_A} \times 2^{nR_B}$ table that contains all (approx.) $2^{kH(S)}$ typical strings (which implies $R_A + R_B = H(S)$), that is shared by Alice, Bob the base station and Eve. To share a typical string s^k, Alice will send the row index corresponding to the row that s^k is in the table, using approx. kR_A bits, or a rate of R_A. Eve who has access to the enciphered results of either Alice or Bob, but not both, gains partial information. If Eve intercepts Alice, then $\Delta_A \approx R_B$, since all typical strings are almost equally likely and indeed $R_A + \Delta_A \approx H(S)$. If Eve intercepts Bob, then $\Delta_B \approx R_B$, and indeed $R_B + \Delta_B \approx H(S)$. Also, $\Delta_A + \Delta_B \approx H(S)$.

The base station receiving both Alice and Bob's enciphered messages can decode by finding the exact entry in the table.

If s^k is not typical, an error is made, but the probability of this event is negligible as $k \to \infty$. ■

The encoding strategy of the above proof is not suitable for low-cost implementation as a table of size of (approx.) $2^{kH(S)}$ entries is required. In the next section we provide design rules for low-cost encoder implementation.

IV. Practical Measure of Secrecy and Codes

In the previous section, the capacity region yielded the impossibility of achieving perfect secrecy. It can be verified that the capacity region suggests that simply compressing and splitting the message is sufficient. For instance, Alice may send the first block of compressed common message and Bob may send the remaining block. However this is obviously a poor strategy as the eavesdropper learns a block of the message without any effort.

In lieu of perfect secrecy, we must define a practical measure of secrecy that is more reasonable than the above trivial splitting technique. Our measure of secrecy is based on the weakly secure network coding problem [6]. This measure of secrecy is based on the eavesdropper's *inability* to solve for any of the unknown variables in a set of linear equations, even when he is given the values of *some* of the unknowns. This is formally summarized in Lemma 1. Thus the eavesdropper must guess the unknown variables in contrast to the trivial splitting technique. Even when the eavesdropper somehow learns some limited part of the message, his knowledge of the other parts is not improved, and he still must guess.

In [6], sufficiency results on the field size are derived, but no simple implementation was provided. We not only derive a simple convolutional-type encoder (opposed to a matrix multiplication in [6]), but also derive a new field size condition that is tighter for our encoder structure.

A. Operational Overview

Let $\mathbf{C} = \begin{pmatrix} \mathbf{C}_1 \\ \hline \mathbf{C}_2 \end{pmatrix}$ be a non-singular $k \times k$ matrix over $GF(q)$ (finite field of size q) such that $\mathbf{C}_1$ is $\alpha k \times k$, and $\mathbf{C}_2$ is $(1-\alpha)k \times k$ where α is a fraction of the form $\frac{m}{k}$, $1 \leq m \leq k-1$. Let s^k, which is to be shared by Alice and Bob, be a column vector whose components are uniformly distributed over $GF(q)$. Then Alice sends $\mathbf{C}_1 s^k$ and Bob sends $\mathbf{C}_2 s^k$.

The base station receives $\mathbf{C}_1 s^k$ and $\mathbf{C}_2 s^k$ or in other words $\begin{pmatrix} \mathbf{C}_1 \\ \hline \mathbf{C}_2 \end{pmatrix} s^k = \mathbf{C} s^k$, and can solve for s^k by inverting $\mathbf{C}$. Alice sends αk symbols over $GF(q)$ or $\alpha k \log_2 q$ bits (since any symbol in $GF(q)$ is assumed to be equally likely), and so her rate is $\alpha \log_2 q$. Similarly Bob's rate is $(1-\alpha)\log_2 q$. $H(S) = \log_2 q$ again since $\mathcal{S} = GF(q)$, and from the uniformity assumption. Therefore we indeed have $R_A + R_B = H(S)$. Also since the rank of $\mathbf{C}_1$ is αk, given $\mathbf{C}_1 s^k$, there are $q^{(1-\alpha)k}$ equally likely s^k [3], and so $\Delta_A = (1-\alpha)\log_2 q$. Similarly $\Delta_B = \alpha \log_2 q$ and so $R_A + \Delta_A = H(S)$, $R_B + \Delta_B = H(S)$, $\Delta_A + \Delta_B = H(S)$, achieving the optimal tradeoffs as promised by the information theoretic results.

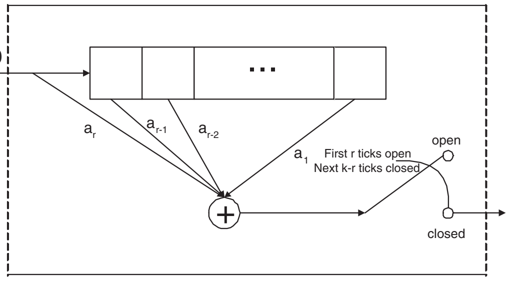

Fig. 3. Alice's encoder (switch operates after clock tick).

Let $\mathbf{C}$ be defined as follows.

$$\mathbf{C} = \left(\begin{array}{cccccccc} a_1 & a_2 & \cdots & a_r & 0 & \cdots & \cdots & 0 \\ 0 & a_1 & a_2 & \cdots & a_r & 0 & \cdots & 0 \\ \vdots & & \ddots & & & \ddots & & 0 \\ 0 & \cdots & \cdots & 0 & a_1 & a_2 & \cdots & a_r \\ \hline b_1 & b_2 & \cdots & b_l & 0 & \cdots & \cdots & 0 \\ 0 & b_1 & b_2 & \cdots & b_l & 0 & \cdots & 0 \\ \vdots & & \ddots & & & \ddots & & 0 \\ 0 & \cdots & \cdots & 0 & b_1 & b_2 & \cdots & b_l \end{array}\right) = \begin{pmatrix} \mathbf{C}_1 \\ \hline \mathbf{C}_2 \end{pmatrix} \tag{33}$$

where the elements are from $GF(q)$. If $\mathbf{C}_1$ has αk rows then $r = k - \alpha k + 1$ as the reader can easily verify. Similarly if $\mathbf{C}_2$ has $(1-\alpha)k$ rows then $l = k - (1-\alpha)k + 1$. Fig. 3 shows Alice's encoder, implemented by $r-1$ registers capable of storing a $GF(q)$ element, and the adders and multipliers are over $GF(q)$. When the encoder first starts, a 0 is padded at the beginning of the stream, but never inserted again so that the encoder can run continuously. The registers can be loaded with any values initially, and never has to reset. The encoder is open for the first r ticks with the goal to load the symbols into the registers serially without outputting. Once all s_1 to s_{r-1} are serially loaded into the register (after the r^{th} tick), the switch closes (before the $(r+1)^{\text{th}}$ tick) to give the dot product of the first row of $\mathbf{C}_1$ with s^k. We chose the form in Fig. 3 because this encoder can also be interpreted as a finite impulse response (FIR) filter over a finite field with decimator (implemented as the switch). This implementation is novel to this paper, and not found in [6], in which the implementation in [6] is a matrix multiplication with a dense matrix (matrix containing few zero elements), since the matrix in [6] is generated randomly.

B. A New Sufficiency Condition on the Field Size

Lemma 1 is adapted from [6] for our problem.

Lemma 1: Let I_i be a $1 \times k$ vector of 0s except the i^{th} position is a 1. If Eve's number of guesses g is restricted to $g < (1-\alpha)k$ and $g < \alpha k$ for Alice and Bob's messages resp., and

$$\begin{pmatrix} \mathbf{C}_1 \\ \hline I_{j_1} \\ \hline \vdots \\ \hline I_{j_{(1-\alpha)k}} \end{pmatrix} \tag{34}$$

1930-529X/07/$25.00 © 2007 IEEE

is full rank for any distinct $(1-\alpha)k$ I_is, then Eve's guesses do not provide her with any additional information; similarly for $\mathbf{C}_2$ using αk I_is (Theorem 2, Lemmas 2 and 3 from [6]).

In [6] the sufficiency condition on the field size is derived by choosing rows of $\mathbf{C}$ one at a time. No restrictions besides those concerning span and dimensionality were placed on these row choices. Since we want a convolutional-type code, we must place further structural restrictions on $\mathbf{C}$ (see (33)), and hence the field size conditions in [6] do not apply. We further simplify Lemma 1 to Proposition 1 in order to derive new sufficiency conditions

Proposition 1: The full rank condition of (34) is satisfied iff any αk columns of $\mathbf{C}_1$ has a non-zero determinant; similarly any $(1-\alpha)k$ columns of $\mathbf{C}_2$ has a non-zero determinant.

The proof is trivial so we omit it. Using Proposition 1, we can formulate a new sufficiency condition for the $\mathbf{C}$ matrix with structure given by (33). The idea behind our proof is very different from [6], so we divulge the details.

Theorem 2: If

$$q > \alpha k \binom{k}{\alpha k} + (1-\alpha)k \binom{k}{(1-\alpha)k} + \max\{\alpha k, (1-\alpha)k\} \tag{35}$$

then there exists $a_i, b_i \in GF(q)$ from (33) such that Lemma 1 is satisfied.

Proof: First take $\mathbf{C}_1$ and choose all possible combinations of αk columns; there are $\binom{k}{\alpha k}$ such combinations. For every αk columns, we have a square matrix, and this has a determinant over the a_i variables, whose values from $GF(q)$ we have not yet chosen; this means that the determinant can be viewed as a multivariate polynomial in the a_i variables. It is easy to show that since there are αk a_i for each $1 \le i \le r$, the maximum degree of this multivariate polynomial does not exceed αk.[1] If we multiply each of the $\binom{k}{\alpha k}$ determinants/polynomials, then the maximum degree is $\alpha k \binom{k}{\alpha k}$. This is similarly true for $\mathbf{C}_2$, resulting in a polynomial with maximum degree $(1-\alpha)k\binom{k}{(1-\alpha)k}$. Finally we need the entire $\mathbf{C}$ itself to be non-singular, so we can take the determinant of $\mathbf{C}$ giving us a new polynomial whose maximum degree cannot exceed $\max\{\alpha k, (1-\alpha)k\}$. Multiplying all polynomials together results in a polynomial with maximum degree not exceeding $\alpha k\binom{k}{\alpha k} + (1-\alpha)k\binom{k}{(1-\alpha)k} + \max\{\alpha k, (1-\alpha)k\}$. In [7] it is shown that for a multivariate polynomial with maximum degree d, there exists a non-zero polynomial evaluation when the variables are chosen from $GF(q)$ with $q > d$. ■

Theorem 2 is only a sufficiency condition, and for small k, smaller field sizes can be found as demonstrated in the example.

Example: Let ξ be a primitive element in $GF(16)$ and a root of $p(x) = 1 + x^3 + x^4$ a binary primitive polynomial. Then one can show that for a block length of 8, and symmetric rates for Alice and Bob, the following $\mathbf{C}$ (which we generated randomly), is secure in the sense defined above.

$$\mathbf{C} = \left(\begin{array}{cccccccc}
\xi^4 & \xi^{11} & \xi^2 & \xi^{13} & \xi^0 & 0 & 0 & 0 \\
0 & \xi^4 & \xi^{11} & \xi^2 & \xi^{13} & \xi^0 & 0 & 0 \\
0 & 0 & \xi^4 & \xi^{11} & \xi^2 & \xi^{13} & \xi^0 & 0 \\
0 & 0 & 0 & \xi^4 & \xi^{11} & \xi^2 & \xi^{13} & \xi^0 \\
\hline
\xi^{10} & \xi^4 & \xi^{12} & \xi^8 & \xi^5 & 0 & 0 & 0 \\
0 & \xi^{10} & \xi^4 & \xi^{12} & \xi^8 & \xi^5 & 0 & 0 \\
0 & 0 & \xi^{10} & \xi^4 & \xi^{12} & \xi^8 & \xi^5 & 0 \\
0 & 0 & 0 & \xi^{10} & \xi^4 & \xi^{12} & \xi^8 & \xi^5
\end{array}\right) \tag{36}$$

We note that if we had just blindly used Theorem 2, we would be working in a field with more than 564 elements! To give the reader some idea as to the complexity of this example encoder, let us process a field element of $GF(16)$ by taking 4 bits per symbol and working in the binary field. The number of wires required to implement *all* the multipliers of $\mathbf{C}_1$ can be shown to be 38, while for $\mathbf{C}_2$, 51 wires are required. For each encoder, 36 *binary* adders are necessary to implement both the multipliers and the adders. ♦

Finally from Lemma 1, the protection against the "guess-based cryptanalysis" is proportional to the number of registers used.

Proposition 2: Alice and Bob's encoders protect up to $g_1 < r-1$ and $g_2 < l-1$ resp., where Alice has $r-1$ registers, and Bob has $l-1$ registers.

Proof: Easily verifiable by reader. ■

Increasing the number of registers may also increase the field size, which augments complexity.

V. Conclusion and Future Work

We have presented the distributed keyless secret sharing problem, described a capacity region that characterizes the compromise among associated parameters, and provided a low-cost implementation solution. The authors are extending this work to allow for distortion at the decoder-side by using rate-distortion theory.

Acknowledgment

The authors would like to thank Dr. Alex Sprintson and Kapil Bhattad for engaging with us in helpful discussions, and the reviewers for their helpful comments.

References

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

[2] 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.

[3] L. H. Ozarow and A. D. Wyner. Wire-tap channel II. *AT & T Bell Laboratories Technical Journal*, 63(10):2135–2157, 1984.

[4] Y. Luo, C. Mitrpant, and A. J. Han Vinck. Some new characters on the wire-tap channel of type II. *IEEE Trans. on Information Theory*, 51(3):1222–1229, March 2005.

[5] T. M. Cover and J. A. Thomas. *Elements of Information Theory*. John Wiley & Sons, New York, 2nd edition, 1991.

[6] K. Bhattad and K. R. Narayanan. Weakly secure network coding. In *Workshop on Network Coding, Theory, and Applications (NETCOD)*, pages 63–68, Riva Del Garda, Italy, April 2005.

[7] T. Ho, R. Koetter, M. Médard, M. Effros, J. Shi, and D. Karger. A random linear network coding approach to multicast. *IEEE Trans. on Information Theory*, 52(10):4413–4430, October 2006.

[1] The maximum degree of a multivariate polynomial is defined as the largest exponent in the polynomial without regard to which variable this is from.

1930-529X/07/$25.00 © 2007 IEEE