Capacity of a Shared Secret Key

Imre Csiszár* and Prakash Narayan†

*A. Rényi Institute of Mathematics
Hungarian Academy of Sciences
H-1364 Budapest, Hungary
Email: csiszar@renyi.hu

†Dept. of Electrical and Computer Engineering
and Institute for Systems Research
University of Maryland, College Park, MD 20742, USA
Email: prakash@umd.edu

***Abstract*—Shannon theoretic shared secret key generation by multiple terminals is considered for a source model in which the components of a discrete memoryless multiple source and a noiseless public channel of unlimited capacity are available for accomplishing this goal. A shared secret key is generated for distinct coalitions of terminals, with all the terminals cooperating in this task through their public communication. A communication from a terminal can be a function of its observed source component and of all previous communication. Member terminals of a coalition unite in recovering the key. Secrecy is required from an eavesdropper that observes the public interterminal communication. A single-letter characterization of the shared secret key capacity is obtained. When the key must be concealed additionally from subsets of coalition members, we provide an upper bound for the strict shared secret key capacity.**

I. Introduction

Suppose that terminals $1, \ldots, m$ observe distinct but correlated signals, following which all the terminals can communicate interactively over a noiseless public channel of unlimited capacity, with the communication being observed by all the terminals. A communication from a terminal can be a function of its own observed signal and of all previous communication. The goal is to generate a *shared secret key* (SSK), i.e., secret common randomness of near uniform distribution, for given coalitions $A_1, \ldots, A_l$ of terminals in $\mathcal{M} = \{1, \ldots, m\}$ of the largest rate possible, with secrecy being required from an eavesdropper that observes the public interterminal communication; member terminals constituting a coalition unite in forming the key for the coalition from the cumulation of their observed signals and the public communication. A more severe requirement calls for an SSK to be recoverable by a coalition only through the concerted action of *all* its member terminals; any smaller subset of the coalition *must* fail to recover the key. Such a restricted SSK is termed a *strict shared secret key* (S*SK). All the terminals in $\mathcal{M}$ cooperate in generating an SSK for the secrecy-seeking coalitions $A_1, \ldots, A_l$. The resulting SSK can be used for encrypted communication by terminals as legitimate members of a coalition but not of a poseur subset.

We consider Shannon theoretic secrecy generation in this new setting which is in the spirit of early work by Shamir [10] on "secret sharing" that generalized a problem considered by Liu [6]. In [10], it was shown how data D, i.e., a "secret," could be divided into n pieces $D_i,\ i = 1, \ldots, n$, in such a manner that D was efficiently computable from a knowledge of any k or more pieces D_i, but could not be deduced from a knowledge of any $k-1$ or fewer pieces.

Our multiterminal source model for SSK generation with public communication builds on our prior work on secret key (SK) generation [4], [5]. The fact that secrecy generation could be enhanced by public communication was first illustrated by Maurer [7]. Models for secrecy generation which entailed two terminals communicating over a noiseless public channel, were examined in detail by Maurer [8] and Ahlswede and Csiszár [1]. These models involve either a discrete memoryless multiple source with two components accessible to one terminal each, or a discrete memoryless channel with one input terminal and one output terminal. In both types of models, an additional "wiretapped" terminal may or may not be present. The sumptuous literature on such models includes, in particular, [9], [2], [3], [4], [5], that are of direct relevance to the present work. A single-letter characterization of the SK capacity – the largest rate at which a SK can be generated – is known in special cases, e.g., when an additional "wiretapped" terminal is absent or when the wiretapped terminal reveals itself to the parties generating secrecy.

We restrict ourselves to models where all the terminals in $\mathcal{M}$ cooperate in generating an SSK for the coalitions $A_1, \ldots, A_l$, with secrecy being required from the eavesdropper which has access to only the public interterminal communication. An S*SK additionally must be kept secret from each subset of every coalition. We assume the eavesdropper to be passive, i.e., unable to tamper with the communication of the legitimate terminals.

Our main contributions are two-fold. First, we give a single-letter characterization of SSK capacity which is derived based on general techniques developed in our previous work on SK capacity [4], [5]. Second, we provide an upper bound on S*SK

capacity that is obtained using our previous characterization of private key (PK) capacity in the same cited works. By way of comparison, we also provide a single-letter characterization of *team secret key* (TSK) capacity for the circumstance in which member terminals in each set $A_j,\ j = 1, \ldots, l$, act as a unified team in the stages of public communication as well as key recovery.

Preliminaries and the problem formulation are contained in section II. Our main results are presented in section III.

II. Preliminaries

Let $X_1, \ldots, X_m,\ m \geq 2$, be rvs with finite alphabets $\mathcal{X}_1, \ldots, \mathcal{X}_m$, respectively. For $A \subset \mathcal{M} = \{1, \ldots, m\}$, we denote $X_A = (X_i,\ i \in A)$. We shall denote n i.i.d. repetitions of $X_{\mathcal{M}} = (X_1, \ldots, X_m)$ by $X_{\mathcal{M}}^n = (X_1^n, \ldots, X_m^n)$, and of X_A by $X_A^n = (X_i^n,\ i \in A)$. All logarithms and exponentials are with respect to the base 2.

We consider a multiterminal source model for secret sharing with public communication. In this model, the components of a discrete memoryless multiple source with generic rvs $X_1, \ldots, X_m$ are observed respectively by m different terminals. Thus, with observation length n, terminal i observes $X_i^n,\ i \in \mathcal{M}$. Randomization at the terminals is permitted; we assume that terminal i generates an rv $U_i,\ i \in \mathcal{M}$, such that $U_1, \ldots, U_m$ and $\mathcal{X}_{\mathcal{M}}^n$ are mutually independent. The terminals are allowed to communicate over a noiseless public channel of unlimited capacity, possibly interactively in several rounds. Formally, assuming without any loss of generality that the communication of the terminals in $\mathcal{M}$ occurs in consecutive time slots in r rounds, such communication is described in terms of the mappings

$$f_{11}, \ldots, f_{1m}, f_{21}, \ldots, f_{2m}, \ldots, f_{r1}, \ldots, f_{rm},$$

with f_{ti} corresponding to a message in time slot t by terminal $i,\ 1 \leq t \leq r,\ 1 \leq i \leq m$; in general, f_{ti} is allowed to yield any function of (U_i, X_i^n) and of previous communication described in terms of $\{f_{t'i'} : t' < t,\ i' \in \mathcal{M} \text{ or } t' = t,\ i' < i\}$. The corresponding rvs representing the communication will be depicted collectively as

$$\mathbf{F} = \{F_{11}, \ldots, F_{1m}, F_{21}, \ldots, F_{2m}, \ldots, F_{r1}, \ldots, F_{rm}\}.$$

For our purposes, it transpires that noninteractive communication without recourse to randomization suffices, i.e., with $\mathbf{F} = (F_1, \ldots, F_m)$, where $F_i = f_i(X_i^n),\ i \in \mathcal{M}$.

We consider *coalitions* of terminals from $\mathcal{M}$ given by *distinct* sets $A_j \subset \mathcal{M},\ A_j \neq \mathcal{M},\ j = 1, \ldots, l$, with intersections possible among coalitions and $A_j \not\subset A_{j'}, 1 \leq j \neq j' \leq l$.

The following concepts introduced in [4], [5] will be used. Given $\epsilon > 0$, a rv U is *ϵ-recoverable* from V if $\Pr\{U \neq f(V)\} \leq \epsilon$ for some function $f(V)$ of V. For rvs K and Y, to be interpreted as representing a secret and the eavesdropper's knowledge, respectively, the information theoretic *security index* is

$$s(K; Y) = \log |\mathcal{K}| - H(K|Y),$$

where $\mathcal{K}$ is the set of possible values of K. Smallness of this security index is tantamount jointly to a nearly uniform distribution for K (i.e., $\log |\mathcal{K}| - H(K)$ is small) and to the near independence of K and Y (i.e., the mutual information $I(K \wedge Y)$ is close to 0).

Definition 1. Given any distinct sets $A_j \subset \mathcal{M},\ A_j \neq \mathcal{M},\ j = 1, \ldots, l$, an rv $K = K(X_{\mathcal{M}}^n)$ constitutes an *ϵ-shared secret key* (ϵ-SSK) for the coalitions $A_j,\ j = 1, \ldots, l$, achievable with randomization $U_{\mathcal{M}}$ and public communication $\mathbf{F}$ if K is ϵ-recoverable from $(U_{A_j}, X_{A_j}^n, \mathbf{F})$ for each $j = 1, \ldots, l$, and, in addition, it satisfies the secrecy condition

$$s(K; \mathbf{F}) \leq \epsilon. \tag{1}$$

An ϵ-SSK as above is called an *ϵ-strict shared secret key* (ϵ-S*SK) if it satisfies the stronger secrecy condition

$$s(K; \mathbf{F}, X_D^n) \leq \epsilon, \quad D \subset A_j,\ D \neq A_j,\ j = 1, \ldots, l. \tag{2}$$

By definition, an ϵ-SSK is recoverable concertedly by every coalition $A_j,\ j = 1, \ldots, l$, and is nearly uniformly distributed and effectively concealed from an eavesdropper with access to the public communication $\mathbf{F}$. It need not be concealed from terminals that constitute (proper and nonempty) subsets of the coalitions, namely $\{D :\ D \subset A_j,\ D \neq A_j,\ j = 1, \ldots, l\}$, or from the terminals in $\mathcal{M} \backslash \bigcup_{j=1}^{l} A_j$ (if nonempty). An ϵ-S*SK constitutes a more stringent version where the key K is recoverable only by each complete coalition but remains concealed from every smaller subset thereof. We stress that in the definitions of SSK and S*SK, the public communication of any terminal, say terminal i in $\mathcal{M}$, is a function (only) of (U_i, X_i^n) and of all previous public communication as above; however, the key K is recovered *jointly* by all the terminals in a coalition, say A_j, from the cumulation of $(U_{A_j}, X_{A_j}^n, \mathbf{F})$.

Definition 2. A number R is an achievable SSK (resp. S*SK) rate for the coalitions $A_j,\ j = 1, \ldots, l$, if there exist ϵ_n-SSKs (resp. ϵ_n-S*SKs) $K^{(n)}$ achievable with suitable randomization $U_{\mathcal{M}}$ and public communication $\mathbf{F}^{(n)}$, such that

$$\epsilon_n \to 0 \ \text{ and } \ \frac{1}{n} \log |\mathcal{K}^{(n)}| \to R \ \text{ as } \ n \to \infty, \tag{3}$$

where $\mathcal{K}^{(n)}$ is the set of possible values of $K^{(n)}$. The largest achievable SSK (resp. S*SK) rate for $A_j, j = 1, \ldots, l$ is the SSK (resp. S*SK) capacity $C_{SSK}(A_1, \ldots, A_l)$ (resp. $C_{S^*SK}(A_1, \ldots, A_l)$).

Remarks: (i) The definitions above are analogous to those for an SK for a multiterminal source model in [4], [5]. In the latter model, given a set $A \subset \mathcal{M}$, an SK K must be recovered by every terminal i in A from $(U_i, X_i^n, \mathbf{F})$ where the public communication $\mathbf{F}$ is as above.

(ii) Our achievability result for an SSK holds with ϵ_n decaying to 0 exponentially rapidly, yielding a "strong" key [9], [2], [3], while the converse stands under the weaker requirement that $\epsilon_n = o(n)$ [8], [1].

It is of interest to compare SSK capacity with that of a multiterminal source model in which the distinct sets $A_j \subset \mathcal{M},\ A_j \neq \mathcal{M},\ j = 1, \ldots, l$, represent *teams* of unified terminals. Now, the public communication among the teams is as above, possibly interactive and conducted in several rounds, but with each team playing the consolidated role of all its member terminals. Specifically, the public communication of team A_j is allowed to be any function of $(U_{A_j}, X^n_{A_j})$ and of all previous public communication, while the communication of a terminal $i \in \mathcal{M} \backslash \bigcup_{j=1}^{l} A_j$ (if nonempty) remains a function of (U_i, X^n_i) and of all previous communication. Such communication will be depicted collectively by $\mathbf{F}_T$.

Definition 3. Given any distinct sets $A_j \subset \mathcal{M},\ A_j \neq \mathcal{M},\ j = 1, \ldots, l$, an rv $K = K(X^n_{\mathcal{M}})$ constitutes an *ϵ-team secret key* (ϵ-TSK) for the teams $A_j,\ j = 1, \ldots, l$, achievable with randomization $U_{\mathcal{M}}$ and public communication $\mathbf{F}_T$ as above if K is ϵ-recoverable from $(U_{A_j}, X^n_{A_j}, \mathbf{F}_T)$ for each $j = 1, \ldots, l$, and, in addition, it satisfies the secrecy condition (1) with $\mathbf{F}_T$ in the role of $\mathbf{F}$. The corresponding largest achievable TSK rate is the TSK capacity $C_{TSK}(A_1, \ldots, A_l)$.

Clearly,

$$\begin{aligned} C_{S^*SK}(A_1, \ldots, A_l) &\leq C_{SSK}(A_1, \ldots, A_l) \\ &\leq C_{TSK}(A_1, \ldots, A_l). \end{aligned} \tag{4}$$

III. Results

Our main results, stated as Theorems 1 and 2 below, provide a single-letter characterization of SSK capacity $C_{SSK}(A_1, \ldots, A_l)$ and an upper bound for S*SK capacity $C_{S^*SK}(A_1, \ldots, A_l)$, respectively. Their proofs rely on our general techniques developed in [4], [5]. The single-letter formula for TSK capacity $C_{TSK}(A_1, \ldots, A_l)$ in Proposition 3 is an immediate consequence of [4], [5].

In order to describe our results, the following notation will be used. For $A_j \subset \mathcal{M},\ A_j \neq \mathcal{M},\ j = 1, \ldots, l$, let

$$\mathcal{B}(A_1, \ldots, A_l) = \left\{ B \subset \mathcal{M} : B \neq \emptyset, B^c \supset A_j \text{ for some } j \in \{1, \ldots, l\} \right\}$$

and $\mathcal{B}_i(A_1, \ldots, A_l),\ i \in \mathcal{M}$, its subset consisting of those $B \in \mathcal{B}(A_1, \ldots, A_l)$ that contain i. Note that $\mathcal{B}(A_1, \ldots, A_l)$ comprises those nonempty subsets of $\mathcal{M}$ that do not intersect *simultaneously* all the coalitions $A_1, \ldots, A_l$. Let $\Lambda(A_1, \ldots, A_l)$ be the set of all collections $\lambda = \{\lambda_B : B \in \mathcal{B}(A_1, \ldots, A_l)\}$ of weights $0 \leq \lambda_B \leq 1$, satisfying

$$\sum_{B \in \mathcal{B}_i(A_1, \ldots, A_l)} \lambda_B = 1 \text{ for all } i \in \mathcal{M}.$$

Similarly, for a nonempty $D \subset A_j, D \neq A_j$ for some $j = 1, \ldots, l$, let

$$\mathcal{B}(A_1, \ldots, A_l | D) = \left\{ B \subset D^c : B \neq \emptyset, B^c \supset (A_j \backslash D) \text{ for some } j \in \{1, \ldots, l\} \right\}.$$

The set $\Lambda(A_1, \ldots, A_l | D)$ of collections of weights $\lambda = \{\lambda_B : B \in \mathcal{B}(A_1, \ldots, A_l | D)\}$ is defined analogously as above with the roles of $\mathcal{B}(A_1, \ldots, A_l)$ and $\mathcal{M}$ now played by $\mathcal{B}(A_1, \ldots, A_l | D)$ and D^c, respectively.

Our first result provides a single-letter characterization of SSK capacity. Its form is redolent of the expression in [4], [5] for the SK capacity for a set of terminals $A \subset \mathcal{M}$ in which a central role was played by the smallest rate of interterminal "communication for omniscience" (CO rate) that enabled all the terminals in A to recover all of $X^n_{\mathcal{M}}$. In an analogous manner, the maximum rate of an SSK for the coalitions $A_j, j = 1, \ldots, l$, is intertwined with the smallest CO rate for $A_1, \ldots, A_l$, denoted $R_{CO}(A_1, \ldots, A_l)$, namely the smallest R such that, for suitable communication $\mathbf{F}^{(n)} = (f_i(X^n_i), i \in \mathcal{M})$, and ϵ_n with

$$\epsilon_n \to 0, \quad \frac{1}{n} \log ||\mathbf{F}^{(n)}|| \to R, \tag{5}$$

$X^n_{\mathcal{M}}$ is ϵ_n-recoverable from $(X^n_{A_j}, \mathbf{F}^{(n)})$ for each $j = i, \ldots, l$.

Theorem 1. *For a source model with generic rvs $X_{\mathcal{M}} = (X_1, \ldots, X_m)$, the (strong) SSK capacity for the coalitions $A_1, \ldots, A_m$, is*

$$C_{SSK}(A_1, \ldots, A_l) = H(X_{\mathcal{M}}) - R_{CO}(A_1, \ldots, A_m), \tag{6}$$

where

$$R_{CO}(A_1, \ldots, A_l) = \max_{\lambda \in \Lambda(A_1, \ldots, A_l)} \sum_{B \in \mathcal{B}(A_1, \ldots, A_l)} \lambda_B H(X_B | X_{B^c}). \tag{7}$$

Furthermore, SSK capacity can be achieved with noninteractive communication and without recourse to randomization at the terminals in $\mathcal{M}$.

Our next result provides a single-letter upper bound for S*SK capacity. For a fixed set $D \subset A_j, D \neq A_j$ with a given $1 \leq j \leq l$, the largest achievable rate for $A_j, j = 1, \ldots, l$ of an SSK that is concealed from the (cooperating) terminals in D, is redolent of PK capacity [4], [5]. A subsequent minimum over all such sets D yields an upper bound on $C_{S^*SK}(A_1, \ldots, A_l)$. We note that for a fixed D, the largest achievable rate of such a "private" SSK with privacy from D, is inherently linked to the smallest achievable CO rate for $A_j, j = 1, \ldots, l$, when each terminal $i \in D$ reveals all of X^n_i; the latter is denoted by $R_{CO}(A_1, \ldots, A_l | D)$. Such achievable CO rates are defined with the obvious modification of that in (5) above, namely that the communication in $\mathbf{F}^{(n)}$ has to satisfy $f_i(X^n_i) = X^n_i$ for $i \in D$, and the rate condition applies to not all of $\mathbf{F}^{(n)}$ but to $\tilde{\mathbf{F}}^{(n)} = (f_i(X^n_i), i \in D^c)$.

Theorem 2. *For a source model with generic rvs $X_{\mathcal{M}} = (X_1, \ldots, X_m)$, the S*SK capacity for the coalitions*

$A_1, \ldots, A_m$, is bounded above according to

$$C_{S^*SK}(A_1, \ldots, A_l) \leq \min_{1 \leq j \leq l} \min_{D \subset A_j, D \neq A_j} [H(X_{\mathcal{M}}|X_D) - R_{CO}(A_1, \ldots, A_m|D)], \quad (8)$$

where

$$R_{CO}(A_1, \ldots, A_l|D) = \max_{\lambda \in \Lambda(A_1,\ldots,A_l|D)} \sum_{B \in \mathcal{B}(A_1,\ldots,A_l|D)} \lambda_B H(X_B|X_{B^c}). \quad (9)$$

Our third result is a single-letter formula for TSK capacity and follows directly from ([4], Theorem 1 and [5], Theorem 3.1). It says that the TSK capacity for the teams A_j, $j = 1, \ldots, l$, is equal to the SK capacity for a modified source model with generic rvs $(X_{A_1}, \ldots, X_{A_l})$, or $(X_{A_1}, \ldots, X_{A_l}, X_{i'}, i' \in \mathcal{M} \backslash \bigcup_{j=1}^{l} A_j)$ if $\mathcal{M} \backslash \bigcup_{j=1}^{l} A_j$ is nonempty. The expression for TSK capacity involves the sets $\mathcal{B}_T(A_1, \ldots, A_l)$ and $\Lambda_T(A_1, \ldots, A_l)$ which are analogs of similar terms in Theorem 1 above but with the difference that B in $\mathcal{B}_T(A_1, \ldots, A_l)$ satisfies the additional requirement of $B \bigcap A_j$ being nonempty for any j implying $B \supset A_j$.

Proposition 3. *For a source model with generic rvs $X_{\mathcal{M}} = (X_1, \ldots, X_m)$, the (strong) TSK capacity for the teams $A_1, \ldots, A_m$, is*

$$C_{TSK}(A_1, \ldots, A_l) = H(X_{\mathcal{M}}) - R_{T,CO}(A_1, \ldots, A_m), \quad (10)$$

where

$$R_{T,CO}(A_1, \ldots, A_l) = \max_{\lambda \in \Lambda_T(A_1,\ldots,A_l)} \sum_{B \in \mathcal{B}_T(A_1,\ldots,A_l)} \lambda_B H(X_B|X_{B^c}). \quad (11)$$

Furthermore, TSK capacity can be achieved with noninteractive communication and without recourse to randomization at the terminals in $\mathcal{M}$.

Lastly, we illustrate our results by the following elementary example.

Example. Consider a source model with $m = 3$ terminals in which X_1 and X_2 are independent binary rvs with each distributed uniformly on $\{0, 1\}$, and $X_3 = X_1 + X_2 \mod 2$.

First, consider the case $A_1 = \{1\}$ and $A_2 = \{2, 3\}$. By [8], [1] or by Proposition 3, $C_{TSK}(A_1, A_2) = I(X_1 \wedge X_2, X_3) = 1$. With observation length $n = 1$ and with no public communication, $K_1 = X_{11}$ of rate 1 constitutes a perfect TSK (i.e., ϵ-TSK with $\epsilon = 0$). Since $K_1 = X_{11}$ is independent of X_{21} and also of X_{31}, it also constitutes a perfect S*SK and thereby a perfect SSK, both of maximal rate by (4).

Next, consider the case $A_1 = \{1, 2\}$, $A_2 = \{2, 3\}$ and $A_3 = \{1, 3\}$. By Proposition 3 or by ([4], Example 3), $C_{TSK}(A_1, A_2, A_3)$ is equal to the minimum of
$I(X_1, X_2 \wedge X_1, X_2, X_3)$,
$I(X_2, X_3 \wedge X_1, X_2, X_3)$,
$I(X_1, X_3 \wedge X_1, X_2, X_3)$
and
$\frac{1}{2}[H(X_1, X_2) + H(X_2, X_3) + H(X_1, X_3) - H(X_1, X_2, X_3)]$.

Hence, $C_{TSK}(A_1, A_2, A_3) = 2$. In fact, once again with observation length $n = 1$, it is easily seen that $K_2 = (X_{11}, X_{21})$ is a perfect TSK of rate 2, achievable without any public communication. Hence, K_2 is also a perfect SSK, and has maximum rate by (4). However, it is clear that K_2 cannot serve as an S*SK.

Turning to S*SK capacity, a straightforward computation shows that the upper bound in Theorem 2 is equal to 1. Thus, $C_{S^*SK}(A_1, A_2, A_3) \leq 1$. Observe that with $n = 2$, $K_3 = X_{11} + X_{22} \mod 2$ is a perfect S*SK of rate 0.5. □

ACKNOWLEDGEMENTS

The work of I. Csiszár was supported by the Hungarian National Foundation for Scientific Research under Grant T046376. The work of P. Narayan was supported by the U.S. National Science Foundation under Grants CCF0635271 and CCF0830697.

REFERENCES

[1] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography–part i: Secret sharing," *IEEE Trans. Inform. Theory*, vol. 39, pp. 1121–1132, 1993.

[2] C.H. Bennett, G. Brassard, C. Crépeau and U.M. Maurer, "Generalized privacy amplification," *IEEE Trans. Inform. Theory*, vol. 41, pp. 1915–1923, November 1995.

[3] I. Csiszár, "Almost independence and secrecy capacity," *Prob. Pered. Inform.*, vol. 32, no. 1, pp. 48–57, 1996.

[4] I. Csiszár and P. Narayan, "Secrecy capacities for multiple terminals," *IEEE Trans. Inform. Theory*, vol. 50, no. 12, pp. 3047–3061, 2004.

[5] ——, "Secrecy capacities for multiterminal channel models," *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2437–2452, 2008.

[6] C.L. Liu, *Introduction to Combinatorial Mathematics*, McGraw Hill, New York, NY, 1968.

[7] U. M. Maurer, "Provably secure key distribution based on independent channels," presented at the *IEEE Workshop Inform. Theory*, Veldhoven, The Netherlands, June 1990.

[8] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inform. Theory*, vol. 39, pp. 733–742, May 1993.

[9] U. M. Maurer, *Communications and Cryptography: Two sides of One Tapestry*, R.E. Blahut et al., Eds. Norwell, MA: Kluwer, 1994, ch. 26, pp. 271–285.

[10] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 2, no. 11, pp. 612–613, November 1979.