Some restrictions on weight enumerators of singly even self-dual codes

doi: 10.1109/TIT.2005.864416

TABLE III
RM CODES OF LENGTH 256: THE LIST SIZES, COMPLEXITIES, AND THE CORRESPONDING SNRS, AT WHICH THE PERMUTATION ALGORITHM $\Upsilon_r^m(l)$ PERFORMS WITHIN $\Delta = 0.25$ dB FROM ML DECODING AT WER 10^{-4}

RM Code	$\{^8_2\}$	$\{^8_3\}$	$\{^8_4\}$	$\{^8_5\}$
List size $l(\Delta)$	64	128	128	16
Complexity $\lvert\Upsilon_r^m(l)\rvert$	216752	655805	777909	94322
SNR at 10^{-4}	2.91	2.65	3.38	5.2

TABLE IV
RM CODES OF LENGTH 256: THE LIST SIZES, COMPLEXITIES, AND THE CORRESPONDING SNRS, AT WHICH THE PERMUTATION ALGORITHM $\Upsilon_r^m(l)$ PERFORMS WITHIN $\Delta = 0.5$ dB FROM ML DECODING AT WER 10^{-4}

RM Code	$\{^8_2\}$	$\{^8_3\}$	$\{^8_4\}$	$\{^8_5\}$
List size $l(\Delta)$	32	64	64	8
Complexity $\lvert\Upsilon_r^m(l)\rvert$	116471	333506	389368	37756
SNR at 10^{-4}	3.12	2.82	3.55	5.4

Note, however, that the algorithm $\Upsilon_r^m(l)$ gives almost no advantage for the subcodes considered in the previous subsection. Indeed, these subcodes are obtained by eliminating the leftmost (least protected) information bits. However, any new permutation $\pi(i)$ assigns the new information bits to these leftmost nodes. Thus, the new bits also become the least protected. Another unsatisfactory observation is that increasing the size of the permutation set T—say, to include all $m!$ permutations of all m indices—helps little in improving decoding performance. More generally, there are a number of important open problems related to these permutation techniques. We name a few:

— find the best permutation set T for the algorithm $\Upsilon_r^m(l)$;
— analyze the algorithm $\Upsilon_r^m(l)$ analytically;
— modify the algorithm $\Upsilon_r^m(l)$ for subcodes.

V. CONCLUDING REMARKS

In this correspondence, we considered recursive decoding algorithms for RM codes that can provide near-ML decoding with feasible complexity for RM codes or their subcodes on the moderate lengths $n \leq 512$.

Our study still leaves many open problems. First, we need to tightly estimate the error probabilities $p(\xi)$ on the different paths ξ. To optimize our pruning procedures for specific subcodes, it is important to find the order in which information bits should be removed from the original RM code. Finally, it is still an open problem to analytically estimate the performance of the algorithms $\Psi_r^m(L)$ and $\Upsilon_r^m(l)$.

ACKNOWLEDGMENT

The authors wish to thank an anonymous referee for helpful suggestions.

REFERENCES

[1] I. S. Reed, "A class of multiple error correcting codes and the decoding scheme," *IEEE Trans. Inf. Theory*, vol. IT-4, no. 4, pp. 38–49, Sep. 1954.
[2] S. N. Litsyn, "On decoding complexity of low-rate Reed-Muller codes" (in Russian), in *Proc. 9th All-Union Conf. Coding Theory and Information Transmission*, Odessa, Ukraine, U.S.S.R., 1988, pp. 202–204.
[3] F. Hemmati, "Closest coset decoding of $u|u+v|$ codes," *IEEE Sele. Areas Commun.*, vol. 7, no. 6, pp. 982–988, Aug. 1989.
[4] G. A. Kabatyanskii, "On decoding of Reed-Muller codes in semicontinuous channels," in *Proc. 2nd Int. Workshop "Algebraic and Combinatorial Coding Theory"*, Leningrad, Russia, U.S.S.R., 1990, pp. 87–91.
[5] R. Lucas, M. Bossert, and A. Dammann, "Improved soft-decision decoding of reed-muller codes as generalized multiple concatenated codes," in *Proc. ITG Conf. Source and Channel Coding*, Aahen, Germany, 1998, pp. 137–141.
[6] N. Stolte and U. Sorger, "Soft-decision stack decoding of binary Reed-Muller codes with "Look-Ahead'" technique," in *Proc. 7th Int. Workshop "Algebraic and Combinatorial Coding Theory"*, Bansko, Bulgaria, Jun. 18–24, 2000, pp. 293–298.
[7] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1981.
[8] I. Dumer, "Recursive decoding of Reed-Muller codes," in *Proc. 37th Allerton Conf. Communications, Control, and Computing*, Monticello, IL, Sep. 1999, pp. 61–69.
[9] I. Dumer and K. Shabunov, "Recursive constructions and their maximum likelihood decoding," in *Proc. 38th Allerton Conf. on Communications, Control, and Computing*, Monticello, IL, Oct. 2000, pp. 71–80.
[10] I. Dumer, "Soft decision decoding of Reed–Muller codes: A simplified algorithm," *IEEE Trans. Inf. Theory*, vol. 52, no. 3, pp. 954–963, Mar. 2006.

Some Restrictions on Weight Enumerators of Singly Even Self-Dual Codes

Masaaki Harada and Akihiro Munemasa

***Abstract*—In this correspondence, we give some restrictions on weight enumerators of singly even self-dual $[n, n/2, d]$ codes whose shadows have minimum weight $d/2$. As a consequence, we determine the weight enumerators for which there is an extremal singly even self-dual $[40, 20, 8]$ code and an optimal singly even self-dual $[50, 25, 10]$ code.**

***Index Terms*—Extremal code, minimum weight, self-dual code, shadow, weight enumerator.**

I. INTRODUCTION

Let C be a singly even self-dual code and let C_0 denote the subcode of codewords having weight $\equiv 0 \pmod 4$. Then C_0 is a subcode of codimension 1. The *shadow* S of C is defined to be $C_0^{\perp} \setminus C$. Shadows for self-dual codes were introduced by Conway and Sloane [1] in order to derive new upper bounds for the minimum weight of singly even self-dual codes, and to provide restrictions on the weight enumerators of singly even self-dual codes. Using shadows, the largest possible minimum weights of singly even self-dual codes of lengths up to 72 are determined in [1, Table I]. The work was extended to lengths up to 100 in [2, Table VI]. The possible weight enumerators of singly even self-dual codes with the largest possible minimum weights are

Manuscript received March 29, 2005; revised September 28, 2005.

M. Harada is with the Department of Mathematical Sciences, Yamagata University, Yamagata 990-8560, Japan.

A. Munemasa is with the Graduate School of Information Sciences, Tohoku University, Sendai 980-8579, Japan.

Communicated by A. E. Ashikhmin, Associate Editor for Coding Theory.
Digital Object Identifier 10.1109/TIT.2005.864416

given in [1] for lengths up to 64 and length 72 (see also [3] for length 60), and the work was extended to lengths up to 100 in [2] (see also [4] for length 68).

It was shown in [5] that the minimum weight d of a singly even self-dual code of length n is bounded by $d \leq 4[n/24] + 4$ unless $n \equiv 22 \pmod{24}$ when $d \leq 4[n/24] + 6$. We call a singly even self-dual code meeting this upper bound *extremal*. It is known that no extremal singly even self-dual code exists for some lengths. According to [6], a singly even self-dual code is called *optimal* if it has the largest minimum weight among all singly even self-dual codes of that length.

In this correspondence, we give some restriction on the number of vectors of weight $d/2$ in the shadow of a singly even self-dual $[n, n/2, d]$ code. We eliminate some of the possible weight enumerators determined in [1] and [2] for singly even self-dual codes with the largest possible minimum weight. In particular, we determine the weight enumerators for which there is an extremal singly even self-dual $[40,\ 20,\ 8]$ code and an optimal singly even self-dual $[50,\ 25,\ 10]$ code.

II. Preliminaries

Throughout this section, let C be a singly even self-dual code of length n and let C_0 denote the subcode of codewords having weight $\equiv 0 \pmod 4$. There are cosets C_1, C_2, C_3 of C_0 such that $C_0^{\perp} = C_0 \cup C_1 \cup C_2 \cup C_3$ where $C = C_0 \cup C_2$ and $S = C_1 \cup C_3$ is the shadow. Let B_i be the number of vectors of weight i in the shadow S.

Lemma 1 (Brualdi and Pless [7]): Let x, x' be vectors of C_1 and let y, y' be vectors of C_3. Then we have the following:

1) if $n \equiv 0 \pmod 4$ then x, y are not orthogonal;
2) if $n \equiv 2 \pmod 4$ then x, x' are not orthogonal and y, y' are not orthogonal.

Although the following sharpenings of [1, Theorem 6c), (19)] follow easily from Lemma 1, the consequences implied by them (cf. Sections III and IV) do not seem to be made explicit in the literature.

Lemma 2: Suppose that $n \equiv 2 \pmod 4$. Then $B_{d/2} \leq 2$. If $B_{d/2} = 2$, then each of C_1 and C_3 contains exactly one of the two vectors of weight $d/2$ in S.

Proof: Assume that S contains at least 3 vectors of weight $d/2$. Then we may suppose without loss of generality that C_1 contains at least two vectors of weight $d/2$. By Lemma 1, any two vectors in C_1 (or C_3) are not orthogonal. The sum of any two vectors in the shadow is a codeword of C. Hence, C contains a codeword of weight less than d which gives a contradiction. □

Lemma 3: Suppose that $n \equiv 0 \pmod 4$. Then $B_{d/2} \leq 2n/d$, and one of C_1 or C_3 contains all the vectors of weight $d/2$ in the shadow. Moreover, we have the following:

i) if n is divisible by $d/2$, then $B_{d/2} \neq 2n/d - 1$;
ii) if n is not divisible by d, then $B_{d/2} \leq 2[(n/d)] - 1$.

Proof: Let $x_1, x_2, \ldots, x_{B_{d/2}}$ be the vectors of weight $d/2$ in S. Since the sum of two vectors of S is a codeword of C, these vectors have disjoint supports. This implies $(d/2)B_{d/2} \leq n$, and that these vectors are pairwise orthogonal. In particular, one of C_1 or C_3 must contain all of them by Lemma 1.

i) Suppose contrary, that $B_{d/2} = 2n/d - 1$. Let y be the sum of the all-one vector and $x_1 + x_2 + \ldots + x_{B_{d/2}}$, so that y has weight $d/2$. Then y is a codeword if $B_{d/2}$ is even, while y belongs to the shadow and is different from $x_1, x_2, \ldots, x_{B_{d/2}}$ if $B_{d/2}$ is odd. Thus we obtain a contradiction in both cases.

ii) Suppose contrary, that $B_{d/2} \geq 2[n/d]$. Let y be the sum of the all-one vector and $x_1 + x_2 + \ldots + x_{2[(n/d)]}$. Then y is a nonzero codeword of weight less than d. This is a contradiction. □

Although the above lemmas can be applied to any singly even self-dual code, we concentrate on extremal singly even self-dual codes and optimal singly even self-dual codes in the next sections.

III. Self-Dual Codes of Lengths 40, 60, 68, 80 and 88

The possible weight enumerators of extremal singly even self-dual $[40,\ 20,\ 8]$ codes and their shadows are given in [1]:

$$\begin{cases} W_C = & 1 + (125 + 16\beta)y^8 + (1664 - 64\beta)y^{10} + \ldots \\ W_S = & \beta y^4 + (320 - 8\beta)y^8 + (21120 + 28\beta)y^{12} + \ldots \end{cases} \tag{1}$$

where β is an integer. By Lemma 3, $0 \leq \beta \leq 10$ and $\beta \neq 9$. For the weight enumerators W_C ($\beta = 0, 1, \ldots, 8$ and 10), it is known that there is a singly even self-dual $[40,\ 20,\ 8]$ code (see [6]). Hence, we have the following.

Proposition 4: There exists an extremal singly even self-dual $[40,\ 20,\ 8]$ code with weight enumerator given by (1) if and only if $0 \leq \beta \leq 10, \beta \neq 9$.

Let C be a singly even self-dual $[40,\ 20,\ 8]$ code whose shadow $C_1 \cup C_3$ has minimum weight 4. By Lemma 3, we may assume that C_3 contains the vectors of weight 4 in the shadow. For $\beta \neq 0$, the decomposition of the weight enumerator of the shadow S into the weight enumerators of C_1 and C_3 is uniquely determined. In fact, by Theorem 3 in [1], the decomposition is obtained as follows:

$$\begin{aligned} W_{C_1} =& (160 - 16\beta)y^8 + (10560 - 32\beta)y^{12} \\ &+ (120160 + 272\beta)y^{16} \\ &+ (262528 - 448\beta)y^{20} + \ldots \\ W_{C_3} =& \beta y^4 + (160 + 8\beta)y^8 + (10560 + 60\beta)y^{12} \\ &+ (120160 - 328\beta)y^{16} \\ &+ (262528 + 518\beta)y^{20} + \ldots. \end{aligned}$$

We remark that this decomposition holds also for $\beta = 0$ (see [8]).

Now we give some restriction on the possible weight enumerators of extremal singly even self-dual codes of lengths 60, 68, 80, and 88.

- The possible weight enumerators of extremal singly even self-dual $[60,\ 30,\ 12]$ codes with shadows of minimum weight ≥ 6 and their shadows are

$$\begin{cases} W_C = & 1 + (2555 + 64\beta)y^{12} \\ & +(33600 - 384\beta)y^{14} + \ldots \\ W_S = & \beta y^6 + (396 - 12\beta)y^{10} + \ldots \end{cases}$$

  where β is an integer [3]. By Lemma 3, $0 \leq \beta \leq 10, \beta \neq 9$. Singly even self-dual $[60,\ 30,\ 10]$ codes with weight enumerators W_C are known for $\beta = 0, 1, 7, 10$ (see [6]).
- The possible weight enumerators of extremal singly even self-dual $[68,\ 34,\ 12]$ codes C with shadows S of minimum weight ≥ 6 and their shadows are

$$\begin{cases} W_C = & 1 + (442 + 4\beta)y^{12} + (14960 - 8\beta - 256\gamma)y^{14} \\ & +(174471 - 36\beta + 2048\gamma)y^{16} + \ldots \\ W_S = & \gamma y^6 + (\beta - 14\gamma)y^{10} + (29920 - 12\beta + 91\gamma)y^{14} \\ & +(2956096 + 66\beta - 364\gamma)y^{18} + \ldots \end{cases}$$

  where β, γ are integers. We remark that the weight enumerators of C and S given in [2] are incorrect and the correct possible weight enumerators for C are given in [4]. Here we give the possible weight enumerators of C along with those of S. By Lemma 3, $0 \leq \gamma \leq 9$. For $\gamma = 0, 1, 2$ only, singly even self-dual

$[68,\ 34,\ 12]$ codes with weight enumerators W_C are known for many values of β (see [6]).

- The possible weight enumerators of extremal singly even self-dual $[80,\ 40,\ 16]$ codes with shadows of minimum weight ≥ 8 and their shadows are

$$\begin{cases} W_C = & 1+(54045+256\alpha)y^{16} \\ & +(675840-2048\alpha)y^{18}+\dots \\ W_S = & \alpha y^8+(800-16\alpha)y^{12} \\ & +(88640+120\alpha)y^{16}+\dots \end{cases}$$

where α is an integer [2]. By Lemma 3, $0 \leq \alpha \leq 10, \alpha \neq 9$. It is not known whether there is a singly even self-dual $[80,\ 40,\ 16]$ code.

- The possible weight enumerators of extremal singly even self-dual $[88,\ 44,\ 16]$ codes with shadows of minimum weight ≥ 8 and their shadows are

$$\begin{cases} W_C = & 1+(14212+16\alpha)y^{16} \\ & +(285824-64\alpha-1024\beta)y^{18}+\dots \\ W_S = & \beta y^8+(\alpha-18\beta)y^{12} \\ & +(35904-16\alpha+153\beta)y^{16}+\dots \end{cases}$$

where α, β are integers [2]. By Lemma 3, $0 \leq \beta \leq 11, \beta \neq 10$. It is not known whether there is a singly even self-dual $[88,\ 44,\ 16]$ code.

IV. Self-Dual Codes of Lengths $50, 58, 78$, and 98

The possible weight enumerators of optimal singly even self-dual $[50, 25, 10]$ codes with shadows of minimum weight $\geq\ 5$ and their shadows are

$$\begin{cases} W_C = & 1+(580-32\beta)y^{10}+(7400+160\beta)y^{12}+\dots \\ W_S = & \beta y^5+(250-10\beta)y^9+\dots \end{cases} \tag{2}$$

where β is an integer [1]. By Lemma 2, $0 \leq \beta \leq 2$. For the weight enumerators $W_C (\beta = 0, 1, 2)$, it is known that there are singly even self-dual $[50,\ 25,\ 10]$ codes (see [6]). The other possible weight enumerator for singly even self-dual $[50, 25, 10]$ codes is

$$1+196y^{10}+11368y^{12}+\dots \tag{3}$$

and there are codes with the weight enumerator [9], [10], [11]. Hence, we have the following.

Propostion 5: There exists an optimal singly even self-dual $[50, 25, 10]$ code with weight enumerator W if and only if $W = W_C$ in (2) with $\beta = 0, 1, 2$, or W is given by (3).

Let C be a singly even self-dual $[50, 25, 10]$ code with weight enumerator W_C in (2). By Lemma 2, the decomposition of the weight enumerator of the shadow S into the weight enumerators of C_1 and C_3 is uniquely determined. By Theorem 3 in [1], the decomposition is obtained as follows for $\beta = 1$

$$\begin{aligned} W_{C_1} =& y^5+108y^9+21228y^{13}+586728y^{17}+4014358y^{21} \\ & +7531440y^{25}+\dots, \\ W_{C_3} =& 132y^9+21617y^{13}+584952y^{17}+4016652y^{21} \\ & +7531440y^{25}+\dots \end{aligned}$$

under the assumption that C_1 contains the vector of weight 5 in the shadow, and for $\beta = 0, 2, W_{C_1} = W_{C_3} = (1/2)W_S$. We remark that for the weight enumerator (3) the decomposition is given in [1].

Now we give some restriction on the possible weight enumerators of optimal singly even self-dual codes of lengths 58, 78 and singly even self-dual $[98, 49, 18]$ codes.

- The possible weight enumerators of optimal singly even self-dual $[58, 29, 10]$ codes with shadows of minimum weight ≥ 5 and their shadows are

$$\begin{cases} W_C = & 1+(319-24\beta-2\gamma)y^{10} \\ & +(3132+152\beta+2\gamma)y^{12}+\dots \\ W_S = & \beta y^5+\gamma y^9 \\ & +(24128-54\beta-10\gamma)y^{13}+\dots \end{cases}$$

where β, γ are integers [1]. By Lemma 2, $\beta = 0, 1, 2$. For these values of β, singly even self-dual $[58, 29, 10]$ codes with weight enumerators W_C are known for many values of γ (see [6]).

- The possible weight enumerators of optimal singly even self-dual $[78, 39, 14]$ codes with shadows of minimum weight ≥ 7 and their shadows are

$$\begin{cases} W_C = & 1+(3705+8\beta)y^{14} \\ & +(62244-24\beta+512\alpha)y^{16}+\dots \\ W_S = & \alpha y^7+(-\beta-16\alpha)y^{11} \\ & +(31616+14\beta+120\alpha)y^{15}+\dots \end{cases}$$

where α, β are integers [2]. By Lemma 2, $\alpha = 0, 1, 2$. Singly even self-dual $[78, 39, 14]$ codes with weight enumerators W_C are known only for $\alpha = 0$ ($\beta = 0$ [2], -19 [12], -78 [13], -26 [14]).

- The possible weight enumerators of singly even self-dual $[98, 49, 18]$ codes with shadows of minimum weight $\geq\ 9$ and their shadows are

$$\begin{cases} W_C = & 1+(70756+32\beta)y^{18} \\ & +(1256752+2048\alpha-160\beta)y^{20}+\dots \\ W_S = & \alpha y^9+(-20\alpha-\beta)y^{13} \\ & +(27930+190\alpha+18\beta)y^{17}+\dots \end{cases}$$

where α, β are integers [2]. By Lemma 2, $\alpha = 0, 1, 2$. It is not known whether there is a singly even self-dual $[98, 49, 18]$ code, but such a code is optimal if it exists.

Acknowledgment

The authors would like to thank the anonymous referees for their useful comments.

References

[1] J. H. Conway and N. J. A. Sloane, "A new upper bound on the minimal distance of self-dual codes," *IEEE Trans. Inf. Theory*, vol. 36, no. 6, pp. 1319–1333, Nov. 1990.

[2] S. T. Dougherty, T. A. Gulliver, and M. Harada, "Extremal binary self-dual codes," *IEEE Trans. Inf. Theory*, vol. 43, no. 6, pp. 2036–2047, Nov. 1997.

[3] T. A. Gulliver and M. Harada, "Weight enumerators of extremal singly-even $[60, 30, 12]$ codes," *IEEE Trans. Inf. Theory*, vol. 42, no. 2, pp. 658–659, Mar. 1996.

[4] S. Buyuklieva and I. Boukliev, "Extremal self-dual codes with an automorphism of order 2," *IEEE Trans. Inf. Theory*, vol. 44, no. 1, pp. 323–328, Jan. 1998.

[5] E. M. Rains, "Shadow bounds for self-dual codes," *IEEE Trans. Inf. Theory*, vol. 44, no. 1, pp. 134–139, Jan. 1998.

[6] W. C. Huffman, "On the classification and enumeration of self-dual codes," *Finite Fields Appl.*, vol. 11, no. 3, pp. 451–490, 2005.

[7] R. A. Brualdi and V. S. Pless, "Weight enumerators of self-dual codes," *IEEE Trans. Inf. Theory*, vol. 37, no. 4, pp. 1222–1225, Jul. 1991.

[8] M. Harada and A. Munemasa, "Shadows, neighbors and covering radii of extremal self-dual codes," manuscript, submitted for publication.

[9] S. Bouyuklieva and M. Harada, "Extremal self-dual $[50, 25, 10]$ codes with automorphisms of order 3 and quasisymmetric 2-(49, 9, 6) designs," *Des., Codes, Cryptogr.*, vol. 28, no. 2, pp. 163–169, 2003.

[10] M. Harada and A. Munemasa, "A quasi-symmetric 2-(49,9,6) design," *J. Combin. Des.*, vol. 10, no. 3, pp. 173–179, 2002.

[11] W. C. Huffman and V. D. Tonchev, "The existence of extremal self-dual $[50, 25, 10]$ codes and quasisymmetric 2-(49,9,6)} designs," *Des., Codes, Cryptogr.*, vol. 6, no. 2, pp. 97–106, 1995.
[12] A. Baartmans and V. Yorgov, "Some new extremal codes of lengths 76 and 78," *IEEE Trans. Inf. Theory*, vol. 49, no. 9, pp. 1353–1354, Sep. 2003.
[13] T. A. Gulliver, M. Harada, and J.-L. Kim, "Construction of new extremal self-dual codes," *Discr. Math.*, vol. 263, no. 1–3, pp. 81–91, 2003.
[14] P. Gaborit and A. Otmani, "Experimental constructions of self-dual codes," *Finite Fields Appl.*, vol. 9, no. 3, pp. 372–394, 2003.

On the Shannon Cipher System With a Capacity-Limited Key-Distribution Channel

Neri Merhav, *Fellow, IEEE*

***Abstract*—We consider the Shannon cipher system in a setting where the secret key is delivered to the legitimate receiver via a channel with limited capacity. For this setting, we characterize the achievable region in the space of three figures of merit: the security (measured in terms of the equivocation), the compressibility of the cryptogram, and the distortion associated with the reconstruction of the plaintext source. Although lossy reconstruction of the plaintext does not rule out the option that the (noisy) decryption key would differ, to a certain extent, from the encryption key, we show, nevertheless, that the best strategy is to strive for perfect match between the two keys, by applying reliable channel coding to the key bits, and to control the distortion solely via rate-distortion coding of the plaintext source before the encryption. In this sense, our result has a flavor similar to that of the classical source–channel separation theorem. Some variations and extensions of this model are discussed as well.**

***Index Terms*—Cryptography, encryption, key distribution, Shannon cipher system, source–channel separation.**

I. Introduction

In the classical Shannon-theoretic approach to cryptology (see, e.g., [8], [6], [13], and references therein), two assumptions are traditionally made. The first is that the reconstruction of the decrypted plaintext source at the legitimate receiver is distortion free (or almost distortion free), and the second, which is related, is that the encryption and the decryption units share identical copies of the same key. Yamamoto [15] has relaxed the first assumption and extended the theory of Shannon secrecy systems into a rate–distortion scenario, allowing lossy reconstruction at the legtimate receiver.

In this correspondence, we examine also the second assumption. Referring to Fig. 1, we consider the case where the key is delivered to the legitimate receiver across a channel, which is cryptographically secure, but has limited capacity. For this setting, we characterize the achievable region in the space of three figures of merit: the security level (measured in terms of the equivocation), the compressibility of the cryptogram, and the distortion associated with the reconstruction of the plaintext source.

One conceptually simple approach to handle such a situation would be to apply a reliable channel code to the encryption key bits, at a rate below the capacity of the channel, and thereby obtain, with high probability, the exact copy of the transmitted key bits at the receiver side. With this approach, however, the effective key rate, and hence the security level in terms of the equivocation, is limited by the channel capacity. The question that naturally arises at this point, especially in the lossy reconstruction scenario, is whether this is the best one can do.

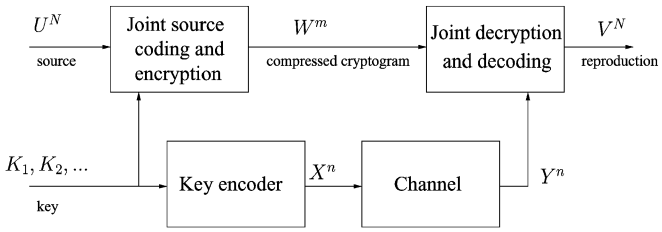

Fig. 1. A cipher system with capacity-limited key distribution.

To sharpen the question, let us even assume that there is an unlimited reservoir of random key bits at the transmitter side, denoted $\boldsymbol{K} = (K_1, K_2, \ldots)$, $K_i \in \{0,1\}$, $i = 1, 2, \ldots$. Then, perhaps one might wish to use more the key rate (somewhat above capacity) for encryption and thereby increase the security of the cryptogram at the expense of some distortion at the reconstruction, due to the unavoidable mismatch between the encryption and decryption keys. To explore this point, let us consider a few speculative strategies.

In the first strategy, one sends the key bits $\boldsymbol{K}$ uncoded across the channel (assuming, for simplicity, that the channel has a binary input–output alphabet). Referring to Fig. 1, let us take then $N = n$ and $X_i = K_i, i = 1, 2, \ldots$. In this case, the noisy version of the key, obtained at the receiver side $K_i' = Y_i$ is of course somewhat different from the original key. However, since only lossy reconstruction of the plaintext is required at the receiver side, it may seem conceivable that a reasonably small difference between the keys at both ends could be managable and thus cause a reasonably small distortion in the reconstruction. This is relatively easy to have if the encryption of the source precedes compression, as proposed in [3]: One may apply, for example, a certain memoryless mapping from the key bit stream into a stream of symbols $Z_1, Z_2, \ldots$ taking (two of the) values in the alphabet of plaintext source $\mathcal{U}$. Then assuming that $\mathcal{U}$ is a commutative group endowed with an addition operation $\oplus$ (e.g., addition modulo the alphabet size), one can create the encrypted sequence $U_i' = U_i \oplus Z_i, i = 1, 2, \ldots$ and then compress the block $(U_1', \ldots, U_n')$ with $(K_1', \ldots, K_n')$ as side information at the receiver, using a Slepian–Wolf encoder [9] in the lossless case, or a Wyner–Ziv code [11] in the lossy case. Assuming, for simplicity, lossless compression, then upon decompressing the source at the receiver side and obtaining $(\tilde{U}_1, \ldots, \tilde{U}_n)$ (which is with high probability equal to $(U_1', \ldots, U_n')$), one "subtracts" the noisy version of the key and obtain (with high probability) the reconstruction $V_i = U_i' \ominus Z_i', i = 1, 2, \ldots$, where Z_i' is the corresponding noisy version of Z_i. Now, since $V_i \ominus U_i = Z_i \ominus Z_i'$, for all i, then for a difference distortion measure $d(U_i, V_i) = \rho(V_i \ominus U_i)$, the distortion between U_i and its reconstruction V_i is identical to the distortion between the original key Z_i and its noisy version Z_i'.

A somewhat more sophisticated version of this scheme generates $Z_1, Z_2, \ldots$ from the key bits using a simulator of a certain (memoryless) process (see, e.g., [10] and references therein), and then applies a good source–channel code to encode $(Z_1, \ldots, Z_n)$ across the channel. The reconstructed version at the receiver side, $Z_1', Z_2', \ldots$, would then have the minimum possible distortion relative to $(Z_1, \ldots, Z_n)$, given by the distortion–rate function of $\{Z_i\}$ computed at the channel capacity, and therefore so would be also the distortion between $\{U_i\}$ and $\{V_i\}$. Moreover, there is an additional degree of freedom with regard

Manuscript received May 3, 2005; revised December 6, 2005.

The author is with the Department of Electrical Engineering, Technion–Israel Institute of Technology, Technion City, Haifa 32000, Israel (e-mail: merhav@ee.technion.ac.il).

Communicated by K. Kobayashi, Associate Editor for Shannon Theory.
Digital Object Identifier 10.1109/TIT.2005.864448