ON THE USE OF THE BINARY MULTIPLYING CHANNEL IN A PRIVATE COMMUNICATION SYSTEM

B.J.M. Smeets
Department of Computer Engineering
University of Lund
P.O. Box 725, S-220 07 Lund/SWEDEN

Abstract. A novel cryptosystem is presented in which the protection of the messages is based on the special properties of the binary multiplying channel. In the system the receiver is mainly responsible for the protection of the messages and not the transmitter. In the paper a small area network realization with a binary multiplying channel is discussed.

The research was supported in part by the National Swedish Board for Technical Development under grants 81-3323 and 83-4364 at the University of Lund.

T. Beth, N. Cot, and I. Ingemarsson (Eds.): Advances in Cryptology - EUROCRYPT '84, LNCS 209, pp. 339-348, 1985.

1. Introduction.

In this paper a novel cryptosystem will be discussed that is based on a special two-way communication channel, i.e. the binary multiplying channel (BMC). New in this system is that the task of protecting the messages is mainly one for the receiver. This in contrast with the classic cryptosystems where the transmitter has this task. The receiver in a classic cryptosystem must know the key used by the transmitter in order to be able to invert the encryption mapping. The fact that keys must be shared causes great practical problems since practical classic cryptosystems require large keys [1],[3],[4]. One of the reasons for using large keys is the fact that the encrypted message is publicly known [1].

When a BMC is used in a communication system it will be possible to realize the protection of the messages in a simpler way. In Section 2 the problem of the construction of communication strategies for the BMC will be discussed without considering the security aspects. Though recently there has been much progress in solving this problem [7],[8], the actual construction of communication strategies for the BMC requires some ad-hoc solutions. In Section 3 the special aspects of security are discussed when the BMC is used in a communication network. Furthermore a communication strategy is presented that provides a good protection of the messages sent via a network. In the last section an application of the new system is discussed.

2. Coding strategies for the BMC.

Consider the communication situation given in Fig. 1a. Two messages m_1 and m_2 are to be transmitted over the binary multiplying channel. The BMC is a deterministic two-way channel with two binary inputs x_1 and x_2 and a binary output $y=x_1x_2 \in \{0,1\}$, $x_i \in \{0,1\}$, $i=1,2$. A simple realization of the BMC is given in Fig. 1b.

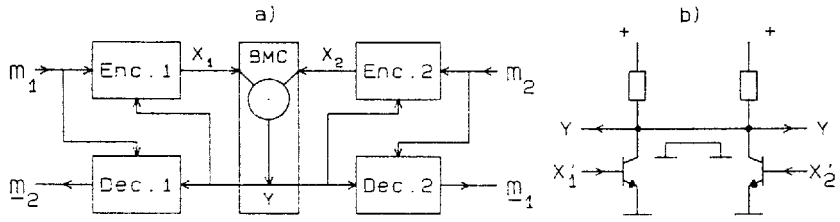

Fig. 1 The BMC in a two user communication network and a wired-and realization of the BMC.

To meet our later requirements and in order to keep the codes quite simple we assume that

a) the messages m_i, $i=1,2$ are taken from a finite set

of messages $M=\{0,1,\ldots,m-1\}$, and that

b) the encoders and decoders are pairwise identical.

Furthermore we assume that

c) the messages m_1 and m_2 are uniform and independently distributed.

Consider the situation where each terminal has chosen a message; say terminal 1 has chosen m_1 and terminal 2 has chosen m_2. The terminals start to communicate via the BMC in order to determine the messages chosen by their opponents. For that purpose they both use a set of rules. All these rules together make the encoder and the decoder. In the sequel the encoding rules will be called a coding strategy. If the reconstructed message $m_i=m_i$ for all sended messages m_i, then one calls the coding strategy complete. A complete coding strategy satisfying a) and b) is refered to as a symmetric discrete complete coding strategy; a SDC-strategy for short. If a coding strategy also optimizes the average transmission rates R_{12} and R_{21} then the coding strategy is called optimal as well. Here is $R_{12}:=n^{-1}I(M_1;Y|M_2)$ and $R_{21}:=n^{-1}I(M_2;Y|M_1)$, i.e. the normalized average mutual information between m_1 and y when m_2 is known and the normalized average mutual information between m_2 and y when m_1 is known, respectively; n is the average number of transmissions. The general problem of determining the region of rate pairs (R_{12},R_{21}) where reliable communication is possible, i.e. the capacity region, C(BMC), of the BMC has been studied for more then two decades [2]. Recently it has been shown by Schalkwijk [6] that the achievable rate region as discussed in [7] is indeed C(BMC). His coding scheme is however not constructive and therefore some coding strategies will be discussed in this section. Note that in the case of a SDC-strategy one has $R_{12}=R_{21}$.

Based upon ideas given in [5] there exists a convenient method for representing the coding strategies. Let $(m_1,m_2)\in MxM$, the cartesian product of the message sets, and let us further associate a unit-square with each message pair (m_1,m_2). Then one can imagine regions, clusters of unit-squares, in a mxm square of possible message pairs in which the actual message pair has to lie. The coding strategy is used in successive transmissions to partition these regions into smaller sub-regions until at both sides of the channel the position of the message pair in the mxm square is unambiguously known.

For example, consider the case $M=\{0,1,2,3\}$. The channel input x_i for the first transmission is taken 1 if $m_i=0,1$ or 2 and 0 if $m_i=3$, i=1,2, see Fig. 2a. The result of the first transmission will be $y_1=1$ if $x_1=x_2=1$ and $y_1=0$ otherwise, Fig. 2b. Note that one has obtained two regions. One characterized by $y_1=1$ and one characterized by $y_1=0$. Suppose that $y_1=1$ has been received. The fact that both terminals know that $y_1=1$ is used in the second transmission. The channel inputs for the second transmission are taken 1 if $m_i=0,1$ and 0 if $m_i=2$. If $y_2=0$ is received then one knows that $(m_1,m_2)\in\{(2,0),(2,1),(2,2),(1,2),(0,2)\}$. Since the correct message pair cannot be determined at this stage of the transmission session one continues by sending a 1 if $m_i=1,2$ and 0 if $m_i=0$. Suppose one has received $y_3=0$, then one has $(m_1,m_2)\in\{(2,0),(0,2)\}$. Now it is possible for the terminals to remove the remaining ambiguity by taking their own messages into account. Hence the transmission

session is finished. Fig. 2c gives a complete coding strategy for the 4x4 square.

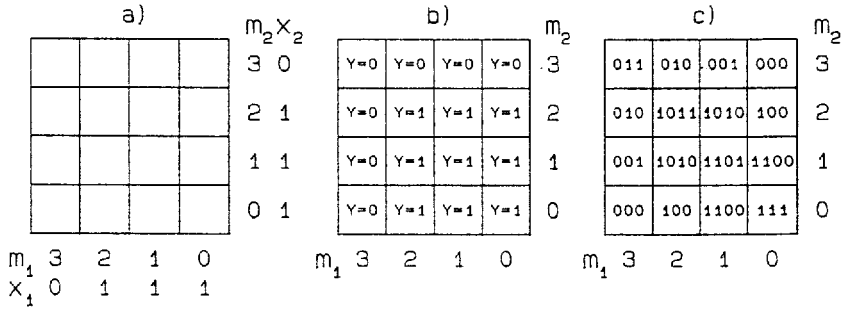

Fig. 2 A coding strategy for the 4x4 square.

The transmission rates R_{12} and R_{21} are easily calculated by exploiting condition c). If $w(m_1=i,m_2=j)$ denotes the number of transmissions required to determine the message pair (i,j) in the mxm square and $\overline{w}$ is the average of w over all message pairs then $R_{12}=R_{21}=H(M_1)/\overline{w}=.593$ bits per transmission. Here is $H(M_1)$ the average binary entropy of the messages m_1. Note that $R_{12}=R_{21}>.5$ bits/tr, hence the rate pair (R_{12},R_{21}) lies outside the time-sharing region !. Larger instances of m have been studied by Post and Ligtenberg [8]. They looked for methods to construct high rate coding strategies.

Some comments should be made concearning the message pairs and the corresponding y-sequence entries in the mxm square, Fig. 2c. Let $S(\underline{y})$ denote the number of message pairs that have $\underline{y}$ as the y-sequence entry in the mxm square. Then the following holds for all SDC-strategies.

Proposition 1 If $\underline{y}$ is a y-sequence entry corresponding with (m_1,m_2), then $S(\underline{y})=1 \iff m_1=m_2$.

From the above follows instantaneously.

Corollary There are m different message pairs for which $S(\underline{y})=1$.

The proof is given in the appendix.

3. The BMC and private communication.

In this section a communication network is considered that uses a BMC. Recalling the realization in Fig. 1b it is clear that the channel outputs y are public in a communication system in which several terminals are connected; see Fig. 3. In such a system communication is considered to take place between two terminals at the same time while

the other terminals cannot interrupt.

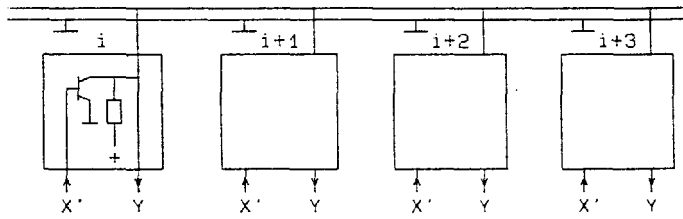

Fig. 3 A communication system with a BMC.

Like in other communication systems is jamming a severe threat to our system. However, here we will only consider a wire tapping attack of an "unfriendly" terminal. Therefore we will look at how much information the wire tapper gets by looking at the channel signals y. The worst that can happen is that during a message transfer one terminal is always a receiver since there is no real difference between the legal receiver and the wire-tapper. Assume for the time being that messages are only sent from one terminal to another. Without loss of generality we may assume that terminal 1 sends to terminal 2. Communication is totally insecure in the system. In order to disturbe the channel signals terminal 2 starts to transmit randomly chosen messages. From Section 2 it is clear that the wire tapper knows immediately the correct (message,noise message) pair if the noise message was equal to the message m_1 at terminal 1. Is however the noise message $m_2 \neq m_1$ then $S(\underline{y})>1$, where $\underline{y}$ is the y-sequence produced by (m_1,m_2). These observations are now to be analysed under the conditions a) and b) in Section 2.

Let p_{ij} denote the probability that message j is chosen at terminal i, i=1,2. Assume that $p_{ij}>0$ for all j=0,1,...,m-1, i=1,2,and let m_1 and m_2 be independently chosen from the message set M. Using proposition 1 of the previous section we obtain the average probability of correct interception, P_{int}, by the wire tapper:

$$P_{int} = \sum_{S(\underline{y})=1} pr(\underline{y}) = \sum_{i=0}^{m-1} pr(m_1=i, m_2=i) = \sum_{i=0}^{m-1} p_{1i}p_{2i}.$$

It can be shown that

Proposition 2 If the messages are chosen independently from the set M and none of the messages has probability zero, then the receiver can make the probability of interception $P_{int} \geq 1/m$ for all SDC-strategies for the BMC, (see appendix).

At this point one could stop and use the coding strategies of the type discussed in Section 2. However, note that if $S(\underline{y})>1$ then the message pair (m_1,m_2) is not unambiguously determined by $\underline{y}$, hence $H(M_i|\underline{y})>0$. Therefore coding strategies that obtain higher values for $S(\underline{y})$ then those of the previous type are of interest. In Fig. 4 such a coding strategy is

given for the 4x4 square. The transmission rate of this coding strategy is less (.57 bits/transm.) than of the one shown in Fig. 2c. However, the new coding strategy has a y-sequence for which $S(\underline{y})=4$.

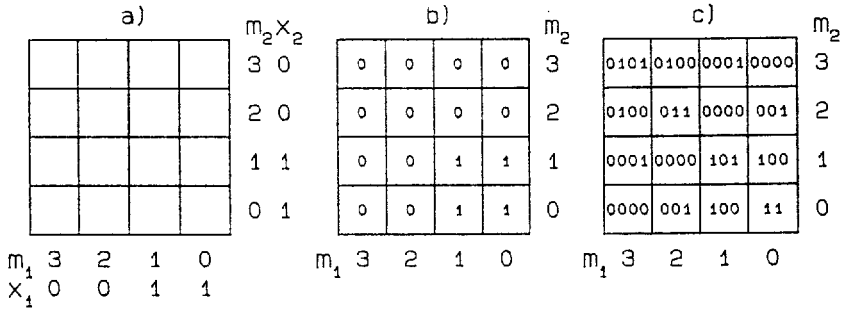

Fig. 4 An alternative coding strategy for the 4x4 square

For both the coding strategies, Fig. 2c and Fig. 4c, the average conditional entropies $H(M_1 | y_1,...,y_k)$ have been calculated. Here denotes $y_1,...,y_k$ the first k y-signals obtained by using a given strategy. In Fig. 5 these calculations are summarized. One sees that the coding strategy of Fig. 4c is better from a security point of view.

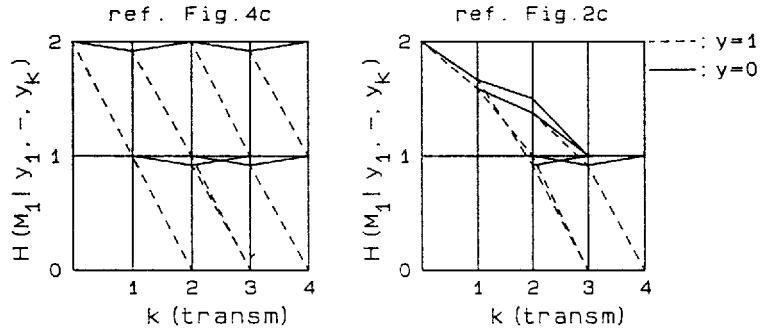

Fig. 5 The average conditional entropies $H(M_1 | y_1,...,y_k)$ of the coding strategies of Fig. 4c and Fig. 2c.

The coding strategy given here can be regarded as a generalization of a code given by Hagelbarger [2]. From the successive squares shown in Fig. 4 it is not difficult to see how one should proceed to construct structural equivalent coding strategies in cases where $m=2^n, n=1,2,3,....$

4. Practical considerations.

In many practical situations the number of correct intercepted messages will be too high. Especially, this will be the case if the source statistics are such that there is a high probability of having $S(\underline{y})=1$. In such a case one should try to obtain a more uniform probability distribution of the message pairs. If condition c) is satisfied one needs only to take a large value of m to lower P_{int}. If this is not satisfactory one could think of using one of the following solutions to the problem. First one could still use some classic cryptosystem to encrypt the messages. This cryptosystem could be quite rudimentary since most of the encrypted messages cannot be correctly intercepted. For the same reason the use of source encoding would be a solution too. A different type of solution would be the use of a randomly determined permutation. Suppose the two communicating terminals will not start with communicating their messages but they will send randomly generated messages first. If at a certain moment enough, say N, noise pairs are generated for which $S(\underline{y})>1$ (or maximal), then these noise pairs determine a permutation of the messages. If the probabilities $pr(m_1=i,m_2=i)$ are the same for all values of $i \in M$, it will be difficult for a wire-tapper to reconstruct this permutation.

Besides the listen-only attack and the problem of jamming, there are some other severe attacks on a network such as the one given in Fig. 3. If an attacker splits the network into two groups he will be able to monitor all communications between the groups. Furthermore if two attackers work closely together they can in principle tap the "wire" by comparing the timing of the signal patterns at different points. Therefore the channel itself must be well protected to provide security.

5. Conclusions.

The binary multiplying channel has interesting properties for use in a private communication system. First, one can send with a total average transmission rate which is larger than 1 bit per channel use. Furthermore, in a communication system that uses a BMC the protection of the messages can be realized by the receiver. Therefore there is no need to use keys when protecting the messages. However, keys might be used to solve the problem of determining the authenticity of the user.
A "wired-and" realisation of the BMC gives the opportunity to construct a small communication network that is well protected against tapping. In general, the security of a communication network that uses a BMC requires saveguarding of the channel itself against attacks.

6. Acknowledgement.

Thanks are due to J.P.M. Schalkwijk, who got me interested in the subject. Furthermore

the stimulating conversations with R. Johannesson and T. Herlestam are gratefully acknowledged.

Appendix.

Consider a SDC-strategy for the coding of a mxm square. The condition that the strategy is complete is here reformulated as having $H(M_i; \underline{y} \mid m_j)=0$, i,j=1,2, i≠j, for all possible y-sequence entries in a completed square.

Let $y^k(m_1,m_2)$ denote the y-sequence $y_1,\ldots,y_k$ produced by the message pair $(m_1,m_2) \in M^2$ up to the k-th transmission. Furthermore denotes $y^c(m_1,m_2)$ the y-sequence obtained by using (m_1,m_2) when the communication is completed. Let $E(m_1,y^k(m_1,m_2))$ denote the encoding of message m_1 after receiving $y^k(m_1,m_2)$.

Lemma 1 Let $m_1,m_2,m_3,m_4 \in M$. Assume that $y^c(m_1,m_2)=y^c(m_3,m_4)$ and $x_{2,1},\ldots,x_{2,c}$ are the inputs produced by encoder 2 using (m_1,m_2) and $\tilde{x}_{2,1},\ldots,\tilde{x}_{2,c}$ those by using (m_3,m_4). If $x_{2,i}=\tilde{x}_{2,i}$ for i=1,...,c, then $y^c(m_1,m_4)= y^c(m_1,m_2)$.

Proof: Let (m_1,m_4) be the transmitted message. Obviously $y^1(m_1,m_4)=y^1(m_1,m_2)$ since the first input letters depend only on the m's. So let $y^k(m_1,m_4)=y^k(m_1,m_2)$ for all k<N+1<c. First observe that the encoder 1 output equals $x_{1,N+1}=E(m_1,y^N(m_1,m_4))=E(m_1,y^N(m_1,m_2))$. The encoder 2 output can be calculated as $x_{2,N+1}=E(m_4,y^N(m_1,m_4))=E(m_4,y_1,\ldots,y_N)=$ $=E(m_4,y^N(m_3,m_4))=\tilde{x}_{2,N+1}=E(m_2,y^N(m_1,m_2))$. Thus $y^{N+1}(m_1,m_4)=y^{N+1}(m_1,m_2)$.//

Let $(i,j) \in M^2$ and define $Reg^k(i,j):= \{ (m_1,m_2) \in M^2 \mid y^k(m_1,m_2)=y^k(i,j) \}$ for all $k \in N$ for which $y^k(i,j)$ is defined. $Reg^0(i,j)$ is equal to MxM for all $(i,j) \in M^2$.

Lemma 2 $(m,m) \in Reg^c(m,n)$ with m≠n is impossible.

Proof: Let $(m,m) \in Reg^c(m,n)$ with m≠n. Then $y^c(m,m) =y^c(n,m)=y^c(m,n)= \underline{y}$. This implies however that $H(M_1 ; \underline{y} \mid m_2=m)>0$ which contradicts with the completeness of the strategy.//

Lemma 3 $y^c(m_1,m_1)=y^c(m_2,m_2) \Rightarrow m_1=m_2$ for all $m_1,m_2 \in M$.

Proof: Let $y^c(m_1,m_1)=y^c(m_2,m_2)$ and let also $m_1 \neq m_2$. If $y^c(m_1,m_1)=y^c(m_2,m_2)$ then the inputs are the same at both sides of the channel. So by Lemma 1 we now have $y^c(m_1,m_2)=y^c(m_1,m_1) \in Reg^c(m_1,m_1)$ which is impossible by Lemma 2.//

Lemma 4 Let $m,m_1,m_2 \in M$, is $(m,m) \neq (m_1,m_2)$ then $y^c(m_1,m_2) \neq y^c(m,m)$.

Proof: let $y^c(m_1,m_2)=y^c(m,m)$ and $(m,m) \neq (m_1,m_2)$. If $m_1=m_2$ then by Lemma 3 $m_1=m_2=m$. So let $m_1 \neq m_2$ and because of Lemma 2 also $m_i \neq m$, i=1,2. Obviously we have $(m_1,m_2),(m_2,m_1),(m,m_2),(m_2,m) \in Reg^0(m,m)$. Let k be an integer and $(m_1,m_2),(m_2,m_1),$

$(m,m_2),(m_2,m) \in Reg^k(m,m)$ for all $k<N+1<c$. If $y_{N+1}(m,m)=y_{N+1}(m_1,m_2)=1$ then $E(m,y^N(m,m))=1$ and $E(m_2,y^N(m,m_2))=1$. Thus the y_{N+1}-th channel output using (m,m_2) is $y_{N+1}(m,m_2)=y_{N+1}(m_2,m)=1$. Is $y_{N+1}(m,m)=y_{N+1}(m_1,m_2)=0$ then $E(m,y^N(m,m))=$ $=E(m,y^N(m,m_2))=0$ $\because$ $y_{N+1}(m,m_2)=y_{N+1}(m_2,m)=0$. Therefore we have $(m_1,m_2),(m_2,m_1),(m,m_2),(m_2,m) \in Reg^{N+1}(m,m)$. This all ultimately leads to $(m_1,m_2),(m_2,m_1),(m,m_2),(m_2,m) \in Reg^c(m,m)$. In particular we have $(m,m) \in Reg^c(m,m_2)$ which is impossible by lemma 2.//

Proof of proposition 1

($\Rightarrow$) Let $\underline{y}=y^c(m_1,m_2)$ such that $S(\underline{y})=1$. If $m_1 \neq m_2$ then via $y^c(m_1,m_2)=y^c(m_2,m_1)$ we have $(m_1,m_2),(m_1,m_2) \in Reg^c(m_1,m_2)$ $\because$ $S(\underline{y})>1$. So $m_1=m_2$.

($\Leftarrow$) Now let $m_1=m_2=m$. Suppose $S(\underline{y})>1$. Then by Lemma 3 there exists a message pair $(k,l)=(m,m)$, $k \neq l$, for which $y^c(k,l)=\underline{y}$. This however contradicts with Lemma 4.//

Define for $n=2,3,4,5,\ldots$ the functions F_n as $F_n(a_0,\ldots,a_{n-1}) = a_0^{-1}+\ldots+a_{n-1}^{-1}$ with $a_i \in R^+$.

Lemma 5 F_n is convex over R^{+n}.

Proof: Let $\underline{a}=a_0,\ldots,a_{n-1}$ and $\underline{b}=b_0,\ldots,b_{n-1}$ with $a_i,b_i \in R^+$, then for $x \in (0,1)$ one has $xF_n(\underline{a})+(1-x)F_n(\underline{b})-F_n(x\underline{a}+(1-x)\underline{b}) = x(1-x)\sum_i [a_i-b_i]^2[a_ib_i(xa_i+(1-x)b_i]^{-1} \geq 0$.//

Proof of proposition 2

Let the receiver be terminal 2. Assume that the messages have a distribution such that $p_{2j}p_{1j}=$constant(>0). The channel outputs can be used to set the p_{2j}'s such that this is true. By straightforward calculations we get $P_{int}=m(\sum_j p_{1j}^{-1})^{-1}$. Now is P_{int} maximal when $\sum_j p_{1j}^{-1}$ is minimal. Observe that the latter summation is in fact $F_m(p_{1,0},\ldots,p_{1,m-1})$. Observe also that by Lemma 5 F_m is convex and $\sum_j p_{1j}=1$. Maximizing $-F_m+l\sum_j p_{1j}$, with l a Lagrange multiplier, gives a minimum for F_m at $p_{1j}=1/m$, $j=0,\ldots,m-1$. Hence $\min_{p_{1j}} F_m(p_{1,0},\ldots,p_{1,m-1})=m^2$ $\because$ $\max_{p_{1j}} P_{int}=m^{-1}$.//

REFERENCES:

[1] Shannon C.E., "Communication Theory of Secrecy Systems," Bell Systems Tech. J., Vol.28, No.4, October 1949, pp. 656-715.

[2] Shannon C.E., "Two-way communication channels," Proc. 4th. Berkely Symp. Math. Statist. and Prob., vol.1, pp. 611-644, 1961. Reprint in Key Papers in the Development of Information Theory, (D. Slepian, Ed) New York, IEEE Press, 1974, pp. 339-372.

[3] Rivest R.L., Shamir A. & Adleman L., "A method for obtaining digital signatures and public key cryptosystems," Comm. A.C.M., Vol.21, Feb. 1978, pp. 120-126.

[4] Odlyzko A.M., "Discrete logarithms in finite fields and their cryptographic significance," preliminary report.

[5] Schalkwijk J.P.M., "The binary multiplying channel- A coding scheme that operates beyond Shannon´s innerbound region", IEEE Trans. Inform. Theory, vol.IT-28, Jan. 1982, pp. 107-110.

[6] Schalkwijk J.P.M., private communication, Jan. 1984.

[7] Schalkwijk J.P.M., Rooyackers J.E. & Smeets B.J.M., "Generalized Shannon strategies for the binary multiplying channel," Proc. 4-th. Symp. on Inform. Theory in the Benelux, 1983, pp. 171-178. Acco Publ. Co., Leuven, Belgium, 1983.

[8] Post K.A. & Ligtenberg L.G.T.M., "Coding strategies for the binary multiplying channel in the discrete case," Proc. 4-th. Symp. on Inform. Theory in the Benelux, 1983, pp. 163-170. Acco Publ. Co., Leuven, Belgium, 1983.