2014-10

New best equivocation codes for syndrome coding

Al-Hassan, S

10.1109/ictc.2014.6983251
2014 International Conference on Information and Communication Technology Convergence (ICTC)
IEEE

New best equivocation codes for syndrome coding

Conference Paper · October 2014

DOI: 10.1109/ICTC.2014.6983251

CITATIONS
3

READS
82

3 authors, including:

Salah al-hassan
University of Plymouth
5 PUBLICATIONS **9** CITATIONS
SEE PROFILE

M. Ahmed
University of Plymouth
110 PUBLICATIONS **889** CITATIONS
SEE PROFILE

New Best Equivocation Codes for Syndrome Coding

Salah Al-Hassan, Mohammed Zaki Ahmed and Martin Tomlinson
School of Computing and Mathematics
University of Plymouth
United Kingdom
Email: salah.al-hassan, M.Ahmed, M.Tomlinson @plymouth.ac.uk

***Abstract*—In this paper we present a code design technique which produces codes for syndrome coding which have better secrecy than the best error correcting codes. Code examples are given for the case where the number of parity bits of the code is equal to 15. The code design technique presented is based on extensions of the parity check matrix of a set of good equivocation codes of shorter length. It is also shown that syndrome coding can be implemented without the traditional syndrome look up table, enabling any length codes to be used. An efficient recursive method to calculate the equivocation rate for the binary symmetric channel (BSC) and any linear binary code is also presented. The design results show that the best equivocation codes (BEC) that are produced have better equivocation rate for the syndrome coding scheme compared to all previously published codes, including the best known codes (BKC).**

I. INTRODUCTION

The wiretap channel was proposed by Wyner [1], and is a physical layer model that takes the security of transmitted information into account. In this model, Alice (transmitter), wishes to send a secret message M to Bob (legitimate receiver) in the presence of an eavesdropper (Eve). The wiretap channel model is shown in Fig. 1, where the main channel (between Alice and Bob) is an error-free channel and the eavesdropper channel is a Binary Symmetric Channel (BSC) with a probability of error (p_e) [2]. Secrecy is measured by the equivocation rate.

Wyner showed that the equivocation rate approaches unity to the eavesdropper if codes are used that have length extending to infinity, if the syndrome space is chosen to be smaller than the Shannon entropy of the binary symmetric channel (BSC). Chen and Vinck [3] also investigated the binary symmetric wiretap channel, and they showed that the secrecy capacity can be obtained by using random linear codes with syndrome coding.

The syndrome coding scheme, whose basic idea is to convey information in the syndromes of a code so as to increase the communication security has been studied by several researchers. For example, Rouayheb and Soljanin [4] showed that network security can be achieved by using syndrome coding as an additional layer to a network code. Al-Hassan, Ahmed and Tomlinson [5] showed that the equivocation rate can be maximised on the eavesdropper side by using a combination of the technique of the McEliece cryptosystem using Best Known Codes (BKC) coupled with syndrome coding. Cohen and Zemor [6] analysed the information leakage of syndrome coding for the wiretap channel and proposed a method to select a syndrome function in order to minimise both the length of the transmitted vector and the information leakage to the eavesdropper. Code design for error correcting codes is an important and long standing topic in coding theory. Good codes can be designed by extending the parity check matrix of good codes as shown in [7], [8].

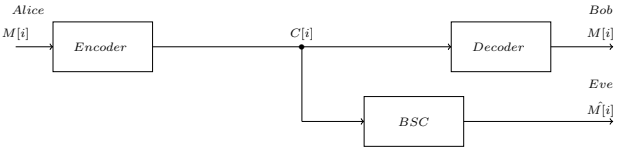

Fig. 1: Wiretap channel Model

In this paper, we present an efficient recursive method for evaluating the equivocation rate of any linear, binary code when used in syndrome coding for the Binary Symmetric Channel (BSC). In addition, we present a code design technique to extend the binary linear $[n, k]$ code to a $[n + 1, k + 1]$ code to produce best equivocation codes. We present examples for the code where the number of parity bits of the code is equal to 15 $(m = 15)$ where $m = n - k$. The code construction method for obtaining good equivocation codes is based on the observation that the syndrome probability mass function of a code extended in length is a function of the probability mass function of the original code, and good equivocation codes produce good extended codes. The design results for $m = 15$ show that these new best equivocation codes (BEC) have better equivocation rate compared to all previously published best error correcting codes, the best known codes (BKC) listed by Grassl [9].

II. SYNDROME CODING SCHEME

Wyner showed that the secrecy capacity of the wiretap channel [1] is :

$$C_s = -p_e.\log_2(p_e) - (1 - p_e).\log_2(1 - p_e) \qquad (1)$$

which is the highest transmission rate that can be obtained while maintaining perfect secrecy. In this model, Alice (transmitter) wants to transmit a sequence of independent and uniformly distributed m-bit binary messages to Bob (legitimate receiver),$M[1], ...M[r]$. This sequence of messages is encoded into n-bit words $C[1], ...C[r]$. Bob receives the same sequence of n-bit words $C[1], ...C[r]$ and Eve receives the sequence of n-bit words $D[1], ...D[r]$ where

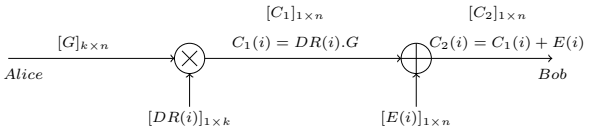

Fig. 2: Block Diagram of Syndrome Coding scheme for (n, k, d) linear block code

$$D(i) = C(i) + E_{BSC}(i), \quad i = 1, ..., r$$

and $E_{BSC}(i)$ represents a n-bit error vector generated by the binary symmetric channel, r is the block length. The syndrome coding scheme uses a (n, k, d) linear block code which guarantees to correct all error patterns of weight t, where $t = \lfloor (d-1)/2 \rfloor$. All 2^m syndromes are used to send messages where $m = n - k$ and not just the syndromes corresponding to weight t or less error patterns. For any linear block code there exist 2^m distinct minimum weight error patterns, the coset leaders, in which each pattern produces a distinct syndrome of the total 2^m syndromes. Therefore, these error patterns can be represented in a table of 2^m syndromes. In the traditional syndrome coding, the look up table for error patterns and syndromes is known by Alice, Bob and Eve.
For long codes a syndrome table is impractical, but it is shown below that this look up table is unnecessary, and that the parity check matrix H of the code is sufficient taking into consideration the structure of H in systematic format. A block diagram for syndrome coding for a (n, k, d) linear block code is shown in Fig. 2.

A. Encoding Algorithm

Alice starts the encryption process in order to generate a n-bit vector $C_2(i)$ from each m-bit message $M(i)$ at time i such that $C_2(i) \times H^T = M(i)$ as shown in **Algorithm 1**.

Algorithm 1 Encoding Algorithm

Require: $[G]_{k\times n}$ ▷ The Generator Matrix of (n,k,d) Code
Require: $[DR(i)]_{1\times k}$ ▷ random, uniformly distributed vector
1: **Generate** $[DR(i)]_{1\times k}$
2: $[C_1(i)]_{1\times n} \leftarrow [DR(i)]_{1\times k}.[G]_{k\times n}$
3: $[E(i)]_{1\times n} \leftarrow [M(i)|0...0]$ ▷ Generate n-bit zero padded message
4: $[C_2(i)]_{1\times n} \leftarrow [C_1(i)]_{1\times n} + [E(i)]_{1\times n}$
5: **return** $[C_2(i)]_{1\times n}$

Now, we show how to calculate the error pattern $[E(i)]_{1\times n}$. Since the syndrome of any codeword is zero, any codeword added to an error pattern will produce the same syndrome. Hence Alice may produce the required syndrome by generating an n-bit zero padded message vector $E(i)$, which consists of the original message $M(i)$ which is m-bits long followed by k 0's where $m = n - k$.

B. Decoding Algorithm

1) Legitimate Receiver's Decoder: Bob receives the transmitted vector $[C_2(i)]_{1\times n}$ via the main channel that is error-free. He recovers the original message $M(i)$ by using the parity check matrix of the code as shown in **Algorithm 2**.

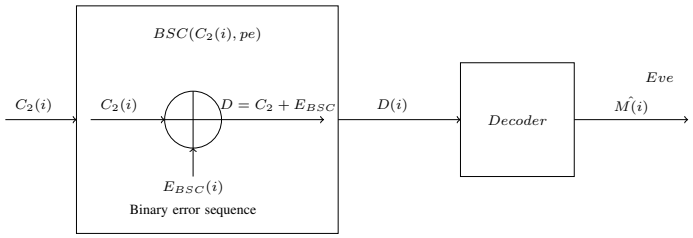

Fig. 3: Block Diagram of the BSC channel and Eavesdropper's Decoder

Algorithm 2 Legitimate Receiver's Decoder

Require: $C_2(i), H^T$ ▷ Bob using H^T of (n, k, d) code
1: $S(i) \leftarrow C_2(i).H^T$ ▷ Bob computes $[S(i)]_{1\times n}$
2: $\hat{M(i)} \leftarrow S(i), M(i) = \hat{M(i)}$ ▷ Bob recovers the original message $M(i)$
3: **return** $M(i)$

From **Algorithm 2**, we can prove that $C_2(i) \times H^T = M(i)$ as follows:
$S(i) = C_2(i) \times H^T \longrightarrow S(i) = (C_1(i) + E(i)) \times H^T$
$S(i) = C_1(i) \times H^T + E(i) \times H^T$
$S(i) = DR(i) \times G \times H^T + E(i) \times H^T$, but $G.H^T = 0$.
So, $S(i) = E(i) \times H^T = M(i)$.
The syndrome formed from $E(i) \times H^T$, because of the k leading zeros of $E(i)$ is simply $M(i)$ multiplied by the identity sub-matrix of H^T which produces $M(i)$.

2) Eavesdropper's Decoder: The block diagram of the BSC channel and eavesdropper's decoder is shown in Fig. 3. Eve receives a corrupted vector $D(i)$ instead of the transmitted vector $[C_2(i)]$ as a result of passing through the BSC which adds additional errors $[E_{BSC}]_{1\times n}$:
$[D(i)]_{1\times n} = [C_2(i)]_{1\times n} + [E_{BSC}(i)]_{1\times n}$, Where $[E_{BSC}(i)]_{1\times n}$ is a random binary error vector which depends on the crossover probability pe of BSC. Assuming Eve uses the same type of decoder that has been used by Bob, the following steps explains how she gets the estimated message $\hat{M(i)}$ from the corrupted vector $D(i)$:

Algorithm 3 Eavesdropper's Decoder

Require: $D(i), H^T$ ▷ Eve using H^T of (n, k, d) code
1: $S_{Eve}(i) \leftarrow D(i).H^T$ ▷ Eve computes $[S_{Eve}(i)]_{1\times n}$
2: $\hat{M(i)} \leftarrow S_{Eve}(i), M(i) \neq \hat{M(i)}$ ▷ Eve recovers an estimate of the message $\hat{M(i)}$
3: **return** $\hat{M(i)}$

From **Algorithm 3**, Eve estimates $\hat{M(i)}$ as follows:
$S_{Eve}(i) = D(i) \times H^T$
$S_{Eve}(i) = [C_2(i) + E_{BSC}(i)] \times H^T$
$S_{Eve}(i) = C_2(i) \times H^T + E_{BSC}(i) \times H^T$
$S_{Eve}(i) = [C_1(i) + E(i)] \times H^T + E_{BSC}(i) \times H^T$
$S_{Eve}(i) = E(i) \times H^T + E_{BSC}(i) \times H^T = \hat{M(i)}$
$\hat{M(i)} = S_{Eve}(i) = M(i) + S_e(i)$

III. Calculation of the secrecy achieved by syndrome coding

The secrecy realised by syndrome coding is measured by the eavesdropper decoder output equivocation, $H(M(i)|\hat{M}(i))$:

$$\begin{aligned} H(M(i)|\hat{M}(i)) &= H(M(i), \hat{M}(i)) - H(\hat{M}(i)) \\ &= H(M(i)) - H(\hat{M}(i)) + H(\hat{M}(i)|M(i)) \\ &= H(M(i)) - H(M(i) + S_e(i)) + \\ &\quad H(M(i) + S_e(i)|M(i)) \\ &= m - m + 0 + H(S_e(i)|M(i)) \quad (2) \\ &= H(S_e(i)) \quad (3) \end{aligned}$$

$$H(M(i)|\hat{M}(i)) = -\sum_{i=0}^{2^m-1} p(S_e(i)).\log_2 p(S_e(i)) \quad (4)$$

where $H(S_e(i))$ is the entropy of $Se(i)$. The simplifications in equations (2) and (3) are due to $M(i)$ being uniformly distributed and independent of $S_e(i)$. The equivocation is calculated after deriving the probability mass function of the syndromes due to errors from the BSC, $p(S_e(i))$ and is a function of the code being used through the parity check matrix of the code.

A. Code Representation

Any binary linear (n, k, d) code is defined by its $(k \times n)$ generator matrix G or by its $(m \times n)$ parity check matrix H. The best equivocation codes are constructed by designing the parity check matrix of the code. H can be defined by representing each column of H by an integer, b_i, in the range 0 to $(2^{n-k} - 1)$. The binary parity check matrix of a code of length n is defined by $n.k$ binary integers, the first m columns of H is an identity matrix if H is in systematic form, as shown below:

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & \dots & 0 & a_{m0} & \dots & a_{(n-1)0} \\ 0 & 1 & \dots & 0 & a_{m1} & \dots & a_{(n-1)1} \\ \vdots & \vdots & \dots & \vdots & \vdots & a_{ij} & \vdots \\ 0 & 0 & \dots & 1 & a_{m(m-1)} & \dots & a_{(n-1)(m-1)} \end{bmatrix}$$

in which $0 \leq j \leq m-1$, $m \leq i \leq n-1$ and $a_{i,j}$ takes a value of 0 or 1. Each column can be represented as a packed integer defined as $b_i = \sum_{j=0}^{m-1} a_{ij}.2^j$. Then the systematic format of H can be represented as following:

$$H = [1,2,\dots,2^{m-1}, b_m, \dots, b_{n-1}]$$

where the first m integers represent the identity matrix and the other integers have values between 3 and $2^m - 1$. Usually no integers are repeated ensuring $d \geq 3$ and higher values of d are ensured by constraining no integer is a modulo 2 sum of any other $d-2$, or smaller, number of integers.

B. Evaluation of the syndrome probability distribution

The code construction technique that produces codes with good equivocation is based on the realisation that the syndrome probability mass function (pmf) of a new extended code is a function of the probability mass function of the original code and good equivocation codes produce good extended codes. For Eve, there are 2^n possible error patterns, e(i), occur for each transmitted vector $C(i)_{1\times n}$. These error patterns occur with probability:

$$p(e(i)) = pe^{w(i)}.(1-pe)^{n-w(i)} \quad (5)$$

where $w(i)$ is the weight of $e(i)$. Each error pattern results in one of the 2^m syndromes being produced.

$$S_e(i)) = e(i) \times H^T \quad (6)$$

As the code is linear, for each syndrome there are 2^k error patterns that produce the same syndrome and the probability of each syndrome due to all possible error patterns is given by:

$$p(S_j) = \sum_{i=0}^{2^n-1} p(e(i)).\delta(S_e(i) - S_j) \quad (7)$$

where $\delta()$ is the Dirac function and

$$H(S_e(i)) = -\sum_{j=0}^{2^m-1} p(S_j).Log_2[p(S_j)] \quad (8)$$

This method for evaluating the equivocation works well for short codes ($n < 40$), but for the long codes it is impracticable because it involves the evaluation of 2^n error patterns. Due to the limitation of this method, the probability distribution of the syndromes may be determined recursively, this method leads to reduce the number of terms from 2^n to 2^m as shown in the following theorem.

Theorem : The probability mass function (pmf) of S_j for j=0 to 2^m-1 can be defined as $p(S_j) = \beta(j)$ where $\beta(j)$ are coefficients of the probability generating function using the Z transform, denoted as $p_z(S)$ and $p_z(S)$ only depends on the columns of the parity check matrix H and the probability error of the binary symmetric channel p_e.

$$p_z(S) = \sum_{j=0}^{2^m-1} \beta(j)Z^j = \prod_{i=0}^{n-1}((1-pe) + pe.Z^{b_i}) \quad (9)$$

where b_i are the integers representations of the columns of H and exponent sums of powers of Z are added modulo 2.

Proof: Any error pattern may be represented as a sum of single bit error events: $e(i) = [e_1\ e_2\ \dots\ e_n]$
$e(i) = [e_1\ 0\ \dots\ 0] + [0\ e_2\ \dots\ 0] + \dots + [0\ 0\ \dots\ e_n]$
where e_i=1 with probability p_e and e_i=0 with probability $1 - p_e$. The linearity of the syndrome coding scheme means that the syndrome resulting from any error pattern is the linear sum of the syndromes for each bit error position:

$$S_e(i) = e(i) \times H^T = [e_1\ e_2\ \dots\ e_n] \times H^T \quad (10)$$

$$S_e(i) = b_1\delta(e_1 - 1) \oplus b_2\delta(e_2 - 1) \cdots \oplus b_n\delta(e_n - 1) \quad (11)$$

Since the probabilities of $e_1, e_2, \ldots, e_n$ are independent, the probability of $S_e(i)$ is the product of the probabilities of n separate error events. By adding the coefficients of the same powers of Z results in the coefficients, β_j, the number of terms to be reduced from 2^n to 2^m. If the columns of H of the shortened code of length r are taken from $i = 0$ to $r-1$ and the pmf generating function of the shortened code is represented as $p_z(S_r)$ then

$$p_z(S_r) = \prod_{i=0}^{r-1}[(1-pe) + pe.Z^{b_i}] \tag{12}$$

$$\begin{aligned} p_z(S_r) &= [(1-pe) + pe.Z^{b_0}].[(1-pe) + pe.Z^{b_1}] \ldots \\ &\quad .[(1-pe) + pe.Z^{b_{r-1}}] \\ &= (1-pe)^2 + pe(1-pe).Z^{b_1} + pe(1-pe).Z^{b_0} + \\ &\quad pe^2.Z^{b_0 \oplus b_1} + \ldots \end{aligned}$$

Now, we can extend the length of the original code from r to $r+1$ by adding one column to its parity check matrix H, the pmf generating function of the extended code $r+1$ is given by

$$p_z(S_{r+1}) = \prod_{i=0}^{r}[(1-pe)+pe.Z^{b_i}] = p_z(S_r)[(1-pe)+pe.Z^{b_r}] \tag{13}$$

Denoting the $\beta(j)$ coefficients of the original code of length r, as $\beta_r(j)$ then

$$p_z(S_r) = \sum_{j=0}^{2^m-1} \beta_r(j) Z^j \tag{14}$$

and for extended code $r+1$

$$p_z(S_{r+1}) = (1-pe) \sum_{j=0}^{2^m-1} \beta_r(j) Z^j + pe \sum_{j=0}^{2^m-1} \beta_r(j) Z^{j \oplus b_r} \tag{15}$$

which simplifies to

$$p_z(S_{r+1}) = (1-pe) p_z(S_r) + pe \sum_{j=0}^{2^m-1} \beta_r(j) Z^{j \oplus b_r} \tag{16}$$

Adding together the coefficients of the same powers of Z in the coefficients, $\beta_r(j)$ to obtain $\beta_{r+1}(j)$, simplifies the above equation to

$$p_z(S_{r+1}) = \sum_{j=0}^{2^m-1} \beta_{r+1}(j) Z^j \tag{17}$$

From equation (16), it is clear that the syndrome pmf of the new code of length $r+1$ is equal to the syndrome pmf of the original code of length r weighted by $1-p_e$ plus a permuted syndrome pmf of the original code of length r, weighted by p_e. The permutation arises from the results of the modulo 2 additions $j \oplus b_r$. This leads to the conclusion that the syndrome pmf of the code can be obtained recursively, starting with the generating function $p_z(S_1)$, determining $p_z(S_2)$ then $p_z(S_3)$ through to $p_z(S_n)$. The syndrome pmf of each (n,k,d) code of length r is stored and the syndrome pmf for each extended code of length $r+1$ is determined using the equation (16) which makes for a fast algorithm. It is also apparent that good equivocation codes will also produce good equivocation codes when extended in length.

IV. CODE DESIGN TECHNIQUE

To produce a best equivocation codes the pmf of the syndromes should be as uniform as possible. Since the eavesdropper channel is a binary symmetric channel, for low values of p_e the equivocation is dominated by error patterns of low weight. To produce best equivocation codes, we must take into account the following observations:

1) If the error pattern has low weight, then the probability of the error events is high. If each error pattern produces different syndrome sums, then this makes the pmf of the syndromes become more uniform.
2) By using the systematic format of the parity check matrix H, the packed integers of any information bit cannot have a weight less than $d-1$, where d is the minimum Hamming distance of the code. Otherwise the codeword formed from that information bit alone will have weight less than d.
3) If any column of the parity check matrix H is repeated, a weight 2 error event will produce a zero syndrome, that leads to a non uniform pmf of the syndrome.

The following code design algorithm shows how to extend an $[n,k]$ code into $[n+1,k+1]$ by adding the best column to the original parity check matrix H of the $[n,k]$ code.

Algorithm 4 Code Design Technique

Require: $p_z(S_r)$ ▷ syndrome pmf of (n,k)code
Require: H ▷ systematic format of H of (n,k)code
Require: $b[i]$ ▷ integer sequence(columns) of H
Require: (n,k,m,pe) ▷ code parameters and error probability of BSC
Require: C_{in} ▷ initial inequivalent codes of the highest equivocation rate
1: **Generate** (b_r) ▷ generating between 3 and 2^m-1
Ensure: $(b_r) \neq b[i]$ ▷ ensure no repeated columns
2: $p_{z1}(S_r) \leftarrow (1-pe).p_z(S_r)$
3: $p_{z2}(S_r) \leftarrow pe \sum_{j=0}^{2^m-1} \beta_r(j) Z^{j \oplus b_r}$
4: $p_z(S_{r+1}) \leftarrow p_{z1}(S_r) + p_{z2}(S_r)$ ▷ apply equations (16) and (17)
5: $Eq \leftarrow -\sum_{j=0}^{2^m-1} \beta_{r+1}(j).Log_2(\beta_{r+1}(j))$ ▷ calculate the equivocation of $[n+1,k+1]$ code
6: $EqN \leftarrow Eq/m$ ▷ calculate the Normalised equivocation
7: **return** $(b_r), EqN, C_{out}$ ▷ extended inequivalent codes, which are ranked by equivocation in descending order

The steps of the algorithm can be simplified as follows:

1) Calculate the syndrome pmf of the original code (n, k) from equation(14).
2) Represent the parity check matrix H of the (n, k) code in the systematic format:
$$H = [1,2,4,\ldots,2^{m-1}, b_m, \ldots, b_{n-1}]$$
3) Extend H with one integer (b_r) by generating randomly all possible integers between 3 and $2^m - 1$ with the constraint that there are no repeated integers included in the original H. This ensures that the minimum Hamming distance of each extended code is at least 3.
4) Eliminate all equivalent codes and evaluate the equivocation rate for each remaining code by using equation(4).
5) Rank the inequivalent codes by their equivocation rate in descending order, and select a best codes subset. These codes are used as the initial input for the next extension round.

V. RESULTS

By using the code design technique above, the best equivocation codes have been determined for $m = 15$. As a result of the large number of codes we only present here in Table 1 codes which provide at least 80% secrecy. The minimum Hamming distance (d) and the equivocation rate $(Eq.)$ for a BSC error probability of $p_e = 0.05$ is given for each code. The equivocation rates of the corresponding best error correcting codes previously published, the (BKC) codes listed by Grassl [9] with the same n and m are also given in Table 1 (in parentheses). The results show that significant improvements have been achieved on the equivocation rate for the best equivocation codes compared with best known codes.

Fig. 4 shows the equivocation rate $Eq.$ as a function of probability of error p_e of best equivocation and best known codes for $n = 82$ at different values of p_e. It shows that the equivocation rate of BECs has been increased by a large margin compared with BKCs not only for $p_e = 0.05$ but also for other values of p_e.

VI. CONCLUSIONS

In this paper, we presented a code design technique for obtaining best equivocation codes and also presented a method of implementing syndrome coding without the need for a syndrome look up table. The best equivocation codes for the syndrome coding scheme that achieve at least 80% secrecy to an eavesdropper using the BSC with an error probability of 0.05 are presented in Table 1. In addition, a recursive method for the evaluation of the probability mass function of the syndromes of a code which depends only on the columns of the parity check matrix and the probability of error of the binary symmetric channel has been presented. The results obtained show that the equivocation rate of the new best equivocation codes exceeds by a large margin the equivocation rates of the best error correcting codes, previously published.

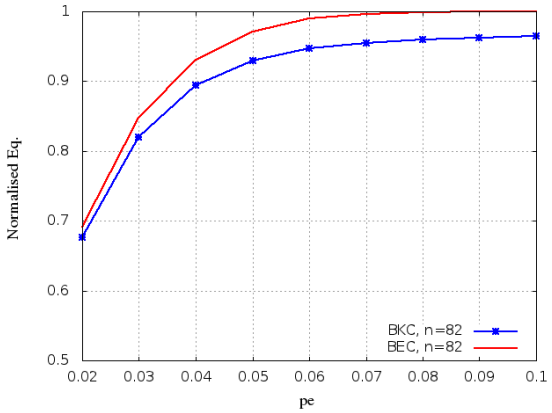

Fig. 4: Equivocation rate $Eq.$ vs. p_e of best equivocation (BEC) and best known (BKC) codes for $n = 82$

REFERENCES

[1] A. D. Wyner, "The Wire-Tap Channel," *The Bell System Technical Journal*, vol. 54, pp. 1355–1367, May 1975.

[2] L. H. Ozarow and A. D. Wyner, "Wire-tap channel ii," *The Bell System Technical Journal*, vol. 63, no. 10, pp. 2135–2157, 1984.

[3] Y. Chen and A. J. Vinck, "On the binary symmetric wiretap channel," *Int. Zurich Seminar on Communications(IZS)*, pp. 17–20, 3-5 March 2010.

[4] S. Y. E. Rouayheb and E. Soljanin, "On wiretap networks ii," *ISIT*, pp. 551–555, 24-29 June 2007.

[5] S. Al-Hassan, M. Ahmed, and M. Tomlinson, "Secrecy coding for the wiretap channel using best known linear codes," in *Global Information Infrastructure Symposium, 2013*, Oct 2013, pp. 1–6.

[6] G. Cohen and G. Zemor, "Syndrome-coding for the wiretap channel revisited," in *Information Theory Workshop, 2006. ITW '06 Chengdu. IEEE*, 2006, pp. 33–36.

[7] W. Alltop, "A method for extending binary linear codes (corresp.)," *Information Theory, IEEE Transactions on*, vol. 30, no. 6, pp. 871–872, Nov 1984.

[8] Y. Edel and J. Bierbrauer, "Inverting construction y1," *Information Theory, IEEE Transactions on*, vol. 44, no. 5, pp. 1993–, Sep 1998.

[9] M. Grassle, "Bounds on the minimum distance of linear codes and quantum codes," 2007,online, Available:http://www.codetables.de.

TABLE I: Best Equivocation Codes that achieve at least 80% secrecy in syndrome coding for $p_e = 0.05$

m	n	d	Eq.	Packed integer parity check matrix
15	48	5	0.804141 (0.744035)	1 2 4 8 16 32 64 126 128 256 512 826 1024 2048 3879 4096 7163 7913 8192 9215 9632 10552 16384 16975 17378 17779 18843 19664 21136 21973 22578 23393 24092 24495 25144 26321 26409 26640 26663 27411 28092 28622 29302 29977 31397 31871 32395 32607
15	49	5	0.813668 (0.772691)	1 2 4 8 16 32 64 128 256 512 1024 2048 3879 4096 5541 7031 7160 7913 8192 9215 13987 14289 16384 16975 17378 17579 18413 18843 18960 19350 19955 21973 23259 23393 24092 24495 25609 25698 26321 26409 27411 28092 28133 28622 28816 31397 31675 31871 32153
15	50	5	0.822836 (0.780014)	1 2 4 8 16 32 64 128 256 512 1024 2048 3879 4096 5541 7031 7160 7913 8192 9215 9683 10365 13987 16384 16975 17378 17579 18843 18960 19350 19955 21973 22294 23259 23393 24092 24495 25609 25698 25850 26321 26409 27411 28092 28622 28816 31397 31675 31871 32153
15	51	5	0.831624 (0.787048)	1 2 4 8 16 32 64 126 128 256 512 1024 1914 2048 3879 4030 4096 4956 6925 7913 8192 8508 9215 12422 12617 14876 16384 16975 17378 17799 18164 18843 20207 20569 21973 23393 24092 25048 26321 26409 27258 27411 27683 28092 28622 29302 30283 31397 31651 31871 32754
15	52	5	0.840045 (0.793774)	1 2 4 8 16 32 64 126 128 151 256 512 1024 1349 2048 3879 4096 4938 7913 8192 9215 12183 15202 16207 16384 16975 17378 17957 18843 19400 20477 20900 21021 21530 21973 22762 23393 24092 24260 25438 26077 26321 26409 27411 28092 28622 29302 29873 31199 31397 31871 32620
15	53	5	0.848118 (0.800219)	1 2 4 8 16 32 64 128 256 512 1024 2048 3879 4096 4797 5541 7031 7160 7913 8192 9215 13987 14289 14371 16384 16975 17378 17579 18180 18293 18843 18960 19350 19955 21973 22537 23259 23393 24092 24495 25609 25698 26321 26409 27411 28092 28133 28622 28816 31397 31675 31871 32153
15	54	5	0.855849 (0.806378)	1 2 4 8 16 32 64 128 256 512 1024 2048 3691 3879 4096 5541 6315 7031 7160 7489 7913 8192 9215 13987 14289 16384 16653 16975 17378 17579 18843 18960 19350 19955 21973 23259 23393 24092 24495 25609 25698 26321 26409 27411 27517 28092 28133 28622 28816 30717 31397 31675 31871 32153
15	55	5	0.863253 (0.812037)	1 2 4 8 16 32 64 126 128 235 256 512 1024 1914 2048 3879 4030 4096 4956 6743 6925 7913 8192 8508 9215 12422 12617 13288 14876 15371 16384 16975 17378 17799 18164 18843 20207 20569 21973 23393 24092 25048 26321 26409 27258 27411 27683 28092 28622 29302 30283 31397 31651 31871 32754
15	56	5	0.870337 (0.817515)	1 2 4 8 16 32 64 126 128 235 256 512 1024 1914 2048 3879 4030 4096 4956 6743 6925 7913 8192 8508 9215 12422 12617 13288 13767 14876 15371 16384 16975 17378 17799 18164 18843 20207 20569 21973 23393 24092 25048 26321 26409 27258 27411 27683 28092 28622 29302 30283 31397 31651 31871 32754
15	57	5	0.877108 (0.822674)	1 2 4 8 16 32 64 126 128 235 256 512 1024 1914 2048 3879 4030 4096 4956 6743 6925 7913 8192 8508 9215 12422 12617 13288 13767 14876 15371 16384 16975 17378 17799 18164 18358 18843 20207 20569 21973 23393 24092 25048 26321 26409 27258 27411 27683 28092 28622 29302 30283 31397 31651 31871 32754
15	58	5	0.883542 (0.827531)	1 2 4 8 16 32 64 126 128 235 256 512 1024 1914 2048 3879 4030 4096 4956 6743 6925 7913 8192 8508 9215 12422 12617 13288 13767 14876 15371 16384 16975 17378 17799 18164 18358 18843 20207 20569 21973 23393 23724 24092 25048 26321 26409 27258 27411 27683 28092 28622 29302 30283 31397 31651 31871 32754
15	59	5	0.889691 (0.832243)	1 2 4 8 16 32 64 128 256 512 1024 2048 3879 4096 4664 4797 5541 6674 7031 7160 7870 7913 8192 9215 13987 14289 14371 16384 16975 17378 17579 18180 18293 18843 18960 19350 19955 21973 22537 23259 23393 24092 24495 25609 25698 26321 26409 26993 27411 27570 28092 28133 28622 28816 31397 31675 31871 32153 32484
15	60	5	0.895581 (0.836659)	1 2 4 8 16 32 64 128 256 512 1024 2048 3879 4096 4664 4797 5541 6674 7031 7160 7870 7913 8192 9215 10420 13987 14289 14371 16384 16975 17378 17579 18180 18293 18843 18960 19350 19955 21973 22537 23259 23393 24092 24495 25609 25698 26321 26409 26993 27411 27570 28092 28133 28622 28816 31397 31675 31871 32153 32484
15	61	5	0.901181 (0.84071)	1 2 4 8 16 32 64 128 256 512 1024 2048 3879 4096 4664 4797 5541 6674 7031 7160 7870 7913 8192 9215 10420 13987 14289 14371 16384 16975 17378 17579 17795 18180 18293 18843 18960 19350 19955 21973 22537 23259 23393 24092 24495 25609 25698 26321 26409 26993 27411 27570 28092 28133 28622 28816 31397 31675 31871 32153 32484
15	62	5	0.906529 (0.84471)	1 2 4 8 16 32 64 126 128 235 256 512 1024 1914 2048 3879 4030 4096 4956 6743 6925 7913 8192 8508 9215 10638 12422 12617 13288 13767 14876 15371 16384 16975 17378 17758 17799 18164 18358 18843 20207 20569 21973 23393 23724 23855 24092 25048 26321 26409 27258 27411 27683 28092 28622 29163 29302 30283 31397 31651 31871 32754
15	63	5	0.911620 (0.848502)	1 2 4 8 16 32 64 126 128 256 512 1024 1914 2048 3145 3879 4030 4096 4956 5368 6256 6454 6925 7913 8192 8508 9215 10627 11106 12422 12617 14876 15254 16384 16604 16975 17378 17799 18164 18324 18700 18843 20207 20569 21973 22743 23393 24092 25048 26321 26409 27258 27411 27683 28092 28622 29302 30283 30961 31397 31651 31871 32754
15	64	5	0.916471 (0.852014)	1 2 4 8 16 32 64 126 128 256 512 1024 1914 2048 3145 3879 3940 4030 4096 4956 5359 5368 6256 6454 6925 7913 8192 8508 9215 10627 11106 12422 12617 14876 15254 16384 16604 16975 17378 17799 18164 18324 18843 20207 20569 21973 22743 23393 24092 25048 26321 26409 27258 27411 27683 28092 28622 29302 30283 30961 31397 31651 31871 32754
15	65	5	0.921080 (0.855343)	1 2 4 8 16 32 64 126 128 256 512 1024 1914 2048 3145 3879 4030 4096 4956 5359 5368 6256 6454 6925 7913 8192 8508 9215 10627 11106 12422 12617 14876 15254 16384 16604 16975 17378 17799 18164 18324 18700 18843 20207 20280 20569 21973 22743 23393 24092 25048 26321 26409 27258 27411 27683 28092 28622 29302 30283 30961 31397 31651 31871 32754
15	66	5	0.925470 (0.858469)	1 2 4 8 16 32 64 126 128 256 512 1024 1914 2048 3145 3879 3940 4030 4096 4956 5368 6256 6454 6564 6925 7913 8192 8508 9215 9264 10627 11106 12422 12617 14876 15254 16384 16604 16975 17378 17799 18164 18324 18843 20207 20569 21973 22743 23393 24092 25048 25148 26321 26409 27258 27411 27683 28092 28622 29302 30283 30961 31397 31651 31871 32754
15	67	5	0.929650 (0.861375)	1 2 4 8 16 32 64 126 128 256 512 1024 1914 2048 3145 3879 3940 4030 4096 4956 5368 6256 6454 6564 6925 7913 8192 8508 9215 9264 10627 11106 12422 12617 14876 15254 16384 16604 16975 17378 17799 18164 18324 18843 20207 20569 21522 21973 22743 23393 24092 25048 25148 26321 26409 27258 27411 27683 28092 28622 29302 30283 30961 31397 31651 31871 32754
15	68	5	0.933609 (0.873716)	1 2 4 8 16 32 64 126 128 256 512 1024 1914 2048 3145 3879 3940 4030 4096 4956 5368 6256 6454 6564 6925 7913 8192 8508 9215 9264 10574 10627 11106 12422 12617 14876 15254 16384 16604 16975 17378 17799 18164 18324 18843 20207 20569 21554 21973 22743 23393 24092 25048 25148 26321 26409 27258 27411 27683 28092 28622 29302 30283 30961 31397 31651 31871 32754
15	69	5	0.937373 (0.883069)	1 2 4 8 16 32 64 126 128 256 512 1024 1914 2048 3145 3879 3940 4030 4096 4956 5368 6256 6454 6564 6925 7913 8192 8508 9215 9264 10627 11106 12422 12617 14876 15254 16384 16604 16975 17378 17602 17799 18164 18324 18843 20207 20569 21522 21973 22743 23393 24092 25048 25148 26321 26409 27211 27258 27411 27683 28092 28622 29302 30283 30961 31397 31651 31871 32754
15	70	5	0.940950 (0.890594)	1 2 4 8 16 32 64 126 128 256 512 1024 1914 2048 3145 3879 4030 4096 4956 5359 5368 6256 6454 6861 6925 7520 7913 8192 8508 9215 10627 11106 12422 12617 14876 15254 16082 16384 16604 16975 17378 17758 17799 18164 18324 18700 18843 20207 20569 21973 22743 23393 24011 24092 24326 25048 26321 26409 27258 27411 27683 28092 29302 30283 30961 31397 31651 31871 32754
15	71	5	0.944327 (0.896977)	1 2 4 8 16 32 64 126 128 256 512 1024 1914 2048 3145 3879 4030 4096 4956 5359 5368 6256 6454 6861 6925 7520 7913 8192 8508 9215 10627 11106 12422 12617 13924 14876 15254 16082 16384 16604 16975 17378 17758 17799 18164 18324 18700 18843 20207 20569 21973 22743 23393 24011 24092 24326 25048 26321 26409 27258 27411 27683 28092 28622 29302 30283 30961 31397 31651 31871 32754
15	72	5	0.947533 (0.902252)	1 2 4 8 16 32 64 126 128 256 512 1024 1914 2048 2697 3145 3879 4030 4096 4956 5359 5368 6256 6454 6861 6925 7520 7913 8192 8508 9215 10627 11106 12422 12617 14876 15254 16082 16384 16604 16975 17378 17758 17799 18164 18324 18700 18843 20207 20569 21973 22743 23393 24011 24092 24326 25048 26321 26409 27258 27411 27683 28092 28622 29302 30283 30961 31397 31651 31871 32007 32754
15	73	5	0.950577 (0.906807)	1 2 4 8 16 32 64 126 128 256 512 1024 1914 2048 3145 3879 4030 4096 4956 5359 5368 6256 6454 6861 6925 7520 7913 8192 8508 9215 10627 11106 11606 12422 12617 14876 15254 16082 16384 16604 16975 17378 17758 17799 18164 18324 18700 18843 20207 20569 21973 22743 23393 24011 24092 24326 25048 25968 26239 26321 26409 27258 27411 27683 28092 28622 29302 30283 30961 31397 31651 31871 32754
15	74	5	0.953458 (0.910715)	1 2 4 8 16 32 64 126 128 256 512 1024 1914 2048 3145 3879 4030 4096 4956 5359 5368 6256 6454 6564 6861 6925 7520 7913 8192 8508 9215 10627 11106 11606 12422 12617 14876 15254 16082 16384 16604 16975 17378 17758 17799 18164 18324 18700 18843 20207 20569 21973 22743 23393 24011 24092 24326 25048 25968 26239 26321 26409 27258 27411 27683 28092 28622 29302 30283 30961 31397 31651 31871 32754
15	75	5	0.956184 (0.914168)	1 2 4 8 16 32 64 126 128 256 512 1024 1914 2048 3145 3879 4030 4096 4956 5359 5368 6256 6454 6564 6861 6925 7520 7913 8192 8508 9215 10627 11106 11606 12422 12617 14876 15254 16082 16384 16604 16975 17378 17758 17799 18164 18324 18700 18843 20207 20569 21973 22743 23393 24011 24092 24326 25048 25968 26239 26321 26409 27258 27411 27683 28092 28622 29302 30283 30961 31397 31651 31871 32133 32754
15	76	5	0.958767 (0.91624)	1 2 4 8 16 32 64 126 128 256 512 1024 1914 2048 2697 3145 3726 3879 4030 4096 4109 4956 5359 5368 6256 6454 6861 6925 7520 7913 8192 8508 9215 10627 10636 11106 12422 12617 14876 15254 16082 16384 16604 16975 17378 17758 17799 18164 18324 18700 18843 18889 20207 20569 21973 22743 23393 24011 24092 24326 25048 26321 26409 27258 27411 27683 28092 28622 29302 30283 30961 31397 31651 31871 32007 32754
15	77	4	0.961205 (0.919134)	1 2 4 8 16 32 64 126 128 256 512 1024 1914 2048 3145 3879 4030 4096 4956 5359 5368 6256 6454 6564 6861 6925 7520 7913 8192 8508 9215 10627 11106 11606 12422 12617 13285 14876 15254 16082 16384 16604 16975 17378 17758 17799 18164 18324 18700 18843 20207 20569 20682 21973 22743 23393 24011 24092 24326 25048 25968 26239 26321 26409 27258 27411 27683 28092 28622 29302 30283 30961 31397 31651 31871 32133 32754
15	78	5	0.963517 (0.92183)	1 2 4 8 16 32 64 126 128 256 512 1024 1914 2048 3145 3879 4030 4096 4956 5359 5368 6256 6454 6564 6861 6925 7520 7913 8192 8508 9215 10627 11106 11606 12422 12617 13285 13685 13924 14876 15254 16082 16384 16604 16975 17378 17758 17799 18164 18324 18700 18843 20207 20569 21973 22743 23393 24011 24092 24326 25048 25968 26239 26321 26409 27258 27411 27683 28092 28622 29302 30283 30961 31397 31651 31871 32133 32754
15	79	5	0.963696 (0.924199)	1 2 4 8 16 32 64 126 128 256 512 1024 1914 2048 2697 3145 3726 3879 4030 4096 4109 4956 5359 5368 6256 6454 6861 6925 7254 7520 7913 8192 8508 9215 10627 10636 11106 12422 12617 14876 15254 16082 16384 16578 16604 16975 17378 17758 17799 18164 18324 18700 18843 18889 20207 20569 21973 22743 23393 24011 24092 24326 25048 26321 26409 27258 27411 27683 28092 28622 29302 30283 30961 31397 31651 31871 32007 32616 32754
15	80	5	0.967762 (0.926307)	1 2 4 8 16 32 64 126 128 256 512 1024 1914 2048 3145 3879 4030 4096 4956 5052 5359 5368 6256 6454 6564 6861 6925 7520 7913 8192 8508 9215 10627 11106 11606 12422 12617 13285 13685 14876 15254 15540 16082 16384 16604 16975 17378 17758 17799 18164 18324 18700 18843 20207 20569 21973 22743 23393 24011 24092 24326 25048 25358 25968 26239 26321 26409 27258 27411 27683 28092 28622 29302 30283 30961 31397 31651 31871 32133 32754
15	81	5	0.969716 (0.928241)	1 2 4 8 16 32 64 126 128 256 512 1024 1914 2048 3145 3429 3879 4030 4096 4956 5359 5368 6256 6454 6861 6925 7520 7913 8192 8508 8797 9215 10627 11106 11606 12422 12617 14876 15254 15644 16082 16384 16604 16975 17378 17758 17799 18164 18267 18324 18700 18843 18955 20207 20569 21824 21973 22743 23393 24011 24092 24326 25048 25968 26321 26409 26764 27258 27411 27683 27992 28092 28622 29302 30283 30961 31397 31651 31703 31871 32754
15	82	5	0.971556 (0.92999)	1 2 4 8 16 32 64 126 128 256 512 1024 1914 2048 3145 3429 3879 4030 4096 4956 5359 5368 6256 6454 6861 6925 7520 7913 8192 8508 8797 9215 10627 11106 11606 12422 12617 14876 15254 15644 16082 16384 16604 16975 17378 17758 17799 18164 18267 18324 18700 18843 18955 20207 20569 21824 21973 22743 23393 24011 24092 24326 25048 25968 26321 26409 26764 27258 27411 27683 27992 28092 28622 29302 30283 30961 31397 31651 31703 31871 32709 32754