On Achieving Capacity on the Wire Tap channel using LDPC Codes

Andrew Thangaraj
Indian Institute of Technology, Madras, India

Souvik Dihidar
Georgia Institute of Technology, Atlanta

A. Robert Calderbank
Princeton University

Steven W. McLaughlin
GTL-CNRS Lab, Metz, France

Jean-Marc Merolla
GTL-CNRS Lab, Metz, France

***Abstract*— We investigate the use of capacity and near-capacity achieving LPDC codes on the wire tap channel, where the dual conditions of reliable communications and security are required. We show that good codes for conventional channels (like BSC and BEC) also have interesting and useful security properties. In this paper we show the connection between the decoding threshold of the code and its security against eavesdropping. We also give practical code constructions for some special cases of the wire tap channel and show that security (in the Shannon sense) is a function of the decoding threshold. Some of these constructions achieve the *secrecy capacity* as defined by Wyner. These codes provide secure communications without conventional key distribution and provide a physical-layer approach for either secure communications or key distribution.**

I. Introduction

The notion of communication with perfect security was defined in information-theoretic terms by Shannon [1]. Suppose a k-bit message $\mathbf{S}$ is to be transmitted securely from Alice to Bob across a public channel. Perfect security is said to be achieved if the encoding of $\mathbf{S}$ into a transmitted word $\mathbf{X}$ is such that the mutual information $I(\mathbf{S};\mathbf{X}) = 0$. From this definition, Shannon concluded that Alice and Bob should necessarily share k bits of key for achieving perfect security.

An alternative notion of communication with perfect security was introduced by Wyner [2] for the more general wire tap channel. In a general wire tap channel system (Fig. 1), D_1 and D_2 are discrete memoryless channels (DMCs). The two DMCs have the same input alphabet but may have different output alphabets. D_1 and D_2 of a wire tap channel system are called the main channel and the wire tap channel, respectively. Wyner's notion of secrecy capacity is the maximum possible rate of information transmission between Alice and Bob that still keeps Eve totally ignorant. If the main channel is less noisy than the wire tap channel [4], then the secrecy capacity is

$$C_s = \max_{P_X(x)} \left[I(X;Y) - I(X;Z) \right], \tag{1}$$

where the maximum is over all possible channel input distributions $P_X(x)$ of X.

Wyner showed that if D_2 is a degraded version of D_1 (D_2 is D_1 concatenated with another DMC) then secrecy capacity is positive. Csiszár et al. [4] showed that the secrecy capacity is positive for the cases when D_1 is "less noisy" than D_2.

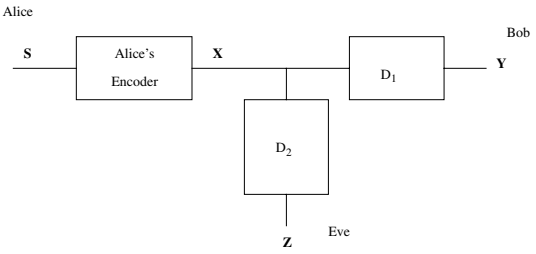

Fig. 1. The wiretap channel system

Maurer [5], [6] generalized this even further and was able to conclude several very powerful results for a general D_1 and D_2.

In this paper, we investigate the use of LDPC-based codes for perfectly secure information exchange in some special cases of wire tap channel systems with a binary erasure channel (BEC) or binary symmetric channel (BSC) for the wire tapper's channel. There are several results in this paper:

1) We make the connection between the threshold of LDPC codes (under message-passing decoding) and perfect security.
2) For the case of a noiseless main channel and BEC wire tap channel we construct codes based on LDPC codes that achieve perfect security and have rates approaching the secrecy capacity.
3) For the case of the BEC main and BEC wire tap channel we provide code constructions and give conditions for achieving perfect security on the wire tap channel and zero probability of error on the main channel. Perfect security in this case is achieved only when capacity-achieving erasure-correcting codes are used, and the code rate is below secrecy capacity.
4) For the case of a noiseless main channel and a binary symmetric channel (BSC) as the wiretapper's channel, we provide a coding solution using codes that have good error-detecting capability. Perfect security is achieved asymptotically, but at rates tending to zero.

The closest previous work to this is in [9] where certain

aspects, such as the existence of LDPC codes for coding over wire tap channels have been studied in the context of key generation from correlated source outputs; however, the context and methods in our work are different than [9].

The coding problem for Alice in the wire tap channel system involves adding redundancy for enabling Bob to correct errors (across the main channel) and adding randomness for keeping Eve ignorant (across the wire tap channel). Let us assume that Alice needs to transmit one out of M equally likely messages i.e. a message denoted u (denoted as $\mathbf{S}$ in Fig. 1) is such that $u \in \{1, 2, \cdots, M\}$ and Prob$\{u = i\} = 1/M$. Alice uses M codes C_i, $1 \leq i \leq M$ with $|C_i| = L$ and block-length N. A message u is encoded into a transmitted word $\mathbf{x}$ as follows: $\mathbf{x}$ is chosen uniformly at random from the code C_u. The transmitted word $\mathbf{x}$, in general, belongs to the overall code $C = \cup_i C_i$. The rate of information transmission from Alice to Bob (in terms of bits per channel use) in such a setting is given by $\log_2 M/N$. The receiver on the main channel (Bob) decodes a received word $\mathbf{y}$ with respect to the overall code C into a decoded message $\hat{u}$ (say, by Maximum-Likelihood decoding). The eavesdropper on the wire tap channel is assumed to have unlimited power to process the received word $\mathbf{z}$.

The objective of Alice and Bob in a wire tap channel system can now be given a precise definition. Let $\mathbf{U}$, $\hat{\mathbf{U}}$, and $\mathbf{Z}$ be random variables denoting Alice's message, Bob's decoded message, and Eve's received word, respectively. Let $H(V)$ represent the entropy of a random variable V. Then, the objective is to achieve the following:

$$Prob\{\mathbf{U} \neq \hat{\mathbf{U}}\} \to 0. \tag{2}$$

$$H(\mathbf{U}|\mathbf{Z}) \to H(\mathbf{U}) = \log_2 M. \tag{3}$$

The constraint (3) is referred to as the security constraint, while (2) is called the reliability constraint. If an encoder (as in Fig. 1) with $R_s = \log_2 M/N$ satisfies the security and reliability constraints for a given wire tap channel system, then such an encoder is said to achieve a secrecy rate R_s. In [12], we have shown that, if each C_i is chosen to be a capacity-achieving code on D_2, and $\cup_i C_i$ is chosen to be a capacity-achieving code on D_1, then we can achieve the secrecy capacity of any wire-tap system (Fig. 1), where both D_1 and D_2 are DMCs. We now give a sketch of the proof in the next section.

II. Proof of Existence of codes and Coding method

A sufficient condition for perfect security on the wire tap channel is : Each C_u should approach capacity over the wire tap channel (similar to the special case considered by Wyner in [2]). We present the criterion in the following theorem without proof.

Theorem 1: If the codes $C_u, u \in \{1, 2, \cdots, M\}$ achieve capacity over the wire tap channel, then Prob$\{\mathbf{U} = u|\mathbf{Z} = \mathbf{z}\} = Prob\{\mathbf{U} = u\}$.

We now focus on the probability of error on the main channel. Let $\overline{P}_E$ be the probability of erro averaged over an ensemble of codes and all possible transmitted messages. Let $ML = e^{NR_1}$; $L = e^{NR_2}$. Note that the secrecy rate of a code from the ensemble is $R_s = R_1 - R_2$. We now give the following theorem without proof.

Theorem 2: The average probability of error is bounded by

$$\overline{P}_E \leq \exp\{[-NE_m(R_1)]\} + \exp\{[-NE_w(R_2)]\}.$$

where $E_m(R_1)$ and $E_w(R_2)$ are the random coding exponents for the wire tap channel and the main channel respectively.

We know that $E_w(R_2) > 0$ for $0 \leq R_2 < C_w$, where C_w is the channel capacity of the wire tap channel. Hence, Theorem 2 says that there exists a code in a suitable ensemble such that the security constraint can be satisfied (each C_u can approach capacity on the wire tap channel) with arbitrary accuracy by increasing the block-length; at the same time, the same code can satisfy the reliability constraint with arbitrary accuracy provided the rate R_1 is such that $E_m(R_1) > 0$. Hence, the maximum secrecy rate achievable by a code from the ensemble is $I(Q_2; S) - C_w$, where Q_2 is the distribution on $\mathbf{X}$ that maximizes the random coding exponent $E_w(R_2)$. Thus, if both the main channel and wire tap channel are symmetric, secrecy capacity is achievable.

We now study the design and use of linear codes over a wire tap channel system. To transmit k-bit messages, we first select a (n, l) linear binary code C such that $k \leq n - l$. Out of the 2^{n-l} cosets of C, we choose 2^k cosets and let each message correspond to a chosen coset. The selection of the cosets is done in a linear fashion. Suppose G is a generator matrix for C with rows $\mathbf{g}_1, \mathbf{g}_2, \cdots$, and $\mathbf{g}_l$. We select k linearly independent vectors $\mathbf{h}_1$, $\mathbf{h}_2$, $\cdots$, and $\mathbf{h}_k$ from $\{0, 1\}^n \setminus C$. Let G^* be the matrix with rows as $\mathbf{h}_1$, $\mathbf{h}_2$, $\cdots$, and $\mathbf{h}_k$. The coset corresponding to a k-bit message $\mathbf{s} = [s_1 \ s_2 \cdots s_k]$ is determined as follows:

$$\mathbf{s} \to s_1\mathbf{h}_1 + s_2\mathbf{h}_2 + \cdots + s_k\mathbf{h}_k + C. \tag{4}$$

Though the above correspondence is deterministic, the encoding procedure has a random component in the selection of the transmitted word. A k-bit message $\mathbf{s}$ is encoded into a n-bit word randomly selected from the coset of C corresponding to $\mathbf{s}$. Hence, the transmitted word, $\mathbf{x}$, is given by

$$\mathbf{x} = s_1\mathbf{h}_1 + s_2\mathbf{h}_2 + \cdots + s_k\mathbf{h}_k + v_1\mathbf{g}_1 + v_2\mathbf{g}_2 + \cdots + v_l\mathbf{g}_l,$$

where $\mathbf{v} = [v_1 \ v_2 \cdots v_l]$ is an uniformly random l-bit vector.

III. Erasure wire tap systems

We now concentrate on wire-tap systems in which D_2 (Fig. 1) is a binary erasure channel (BEC). Such systems appear in the quantum key distribution problems. In [12], we considered the problem where D_2 is a BEC, and D_1 is noiseless. We showed that dual codes of good erasure correcting LDPC codes can be used to design codes for such systems. We used the following result from [3, Lemma 3].

Theorem 3 (Ozarow, Wyner '84): Let an $(n, n-k)$ code C have a generator matrix $G = [\mathbf{a}_1 \cdots \mathbf{a}_n]$, where $\mathbf{a}_i$ is the i-th column of G. Consider an instance of the eavesdropper's observation $\mathbf{z} \in \{0, 1, ?\}^n$ with μ unerased positions given by $\{i : \mathbf{z}_i \neq ?\} = \{i_1, i_2, \cdots, i_\mu\}$. $\mathbf{z}$ is secured by C iff the matrix $G_\mu = [\mathbf{a}_{i_1} \mathbf{a}_{i_2} \cdots \mathbf{a}_{i_\mu}]$ has rank μ.

We now give the following examples from [12].

Example 1: Let D_2 be a BEC with erasure probability ϵ. The $C^n(x^2, x^5)$ ensemble of $(3, 6)$-regular LDPC codes has threshold $\alpha^*(x^2, x^5) \approx 0.42$. Let M be an adjacency matrix from the ensemble with large n (say, $n \geq 10^5$). M is an $n/2 \times n$ binary matrix with row weight 3 and column weight 6. The $(n, n/2)$ code $C^\perp$, dual of C, with generator matrix M can be used for $\epsilon \geq 0.58$ with perfect secrecy. The information rate between the honest parties in this case is $R = 0.5$ compared to the upper bound of $1 - (1 - \epsilon) = 0.58$ (from (1)).

Example 2 (Tornado codes): A rate-$2/3$ tornado code ensemble with threshold $\delta = 0.33257$ has been reported in [10]. A parity-check matrix M for a code from the ensemble will have dimensions $n/3 \times n$. The $(n, n/3)$ code $C^\perp$, dual of C, with generator matrix M can be used over an erasure wire tap channel for $\epsilon > 0.66743$ with perfect secrecy. The information rate between the honest parties in this case is $R = 2/3 = 0.66666...$ compared to the upper bound of $1 - (1 - \epsilon) = 0.66743$.

A. Erasure main channel and erasure wire tap channel

In this section, both D_2 and D_1 are BECs with erasure probabilities ϵ_w and ϵ_m respectively. Our results apply with a small modification to systems with DMCs other than the BEC as D_1. According to (1), the secrecy capacity of this system is $C_s = \epsilon_w - \epsilon_m$, which is positive whenever $\epsilon_w > \epsilon_m$.

We first pick an LDPC code C_1 of length n from an ensemble of codes having asymptotic erasure threshold ϵ_w. That means, as $n \to \infty$, C_1 recovers all the erasures on an erasure channel with erasure probability up to at least ϵ_w, using the standard iterative erasure decoding algorithm. Let C_1 have rate r_1, and let H_1 be the parity check matrix of the code C_1. Next we pick $n(1 - r_2)$ independent vectors from the dual space of C_1, where $r_1 < r_2$. Let H_2 be the matrix formed by these vectors as rows. H_2 has dimensions $n(1 - r_2) \times n$. Let $\overline{H}_2$ be the rest of the independent vectors in the dual space of C_1. As we will see shortly, we must have $\epsilon_w > (1 - r_2)$ in order to guarantee some equivocation for Eve. Let H_2 be the parity check matrix of a code C_2. We want C_2 to have asymptotic erasure threshold ϵ_m. We then have,

$$1 - r_2 \geq \epsilon_m, \tag{5}$$

and

$$1 - r_1 \geq \epsilon_w. \tag{6}$$

We now discuss the encoding procedure. Alice first takes a $n(r_2 - r_1)$-bit long message vector $\mathbf{S}$, and forms a $n(1 - r_1)$-bit long vector by adding $n(1 - r_2)$ 0's on top of $\mathbf{S}$. She now chooses an $\mathbf{X}$ at random from the solution set of the equation shown in Figure 2 and transmits it.

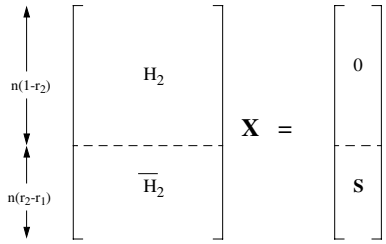

Fig. 2. The encoding procedure

We illustrate this encoding procedure in Figure 3. Note that, the number of solutions to the equation, $H_2\mathbf{X} = \mathbf{0}$, is $2^{n-n(1-r_2)} = 2^{nr_2}$. However, for some particular choice of $\mathbf{S}$, say $\mathbf{S_1}$, the number of solutions to the equation shown in Fig. 2 is $2^{n-n(1-r_1)} = 2^{nr_1}$. Obviously, the same $\mathbf{X}$ cannot be a solution for two different values of $\mathbf{S}$. This explains the splitting of the solution set space of the equation $H_2\mathbf{X} = \mathbf{0}$ into $\frac{2^{nr_2}}{2^{nr_1}} = 2^{n(r_2-r_1)}$ disjoint subsets, each corresponding to a different value of $\mathbf{S}$. Hence the rate of our code is $(r_2 - r_1)$. The interesting point to observe in Figure 3 is that we are not using the whole space of $\{0, 1\}^n$.

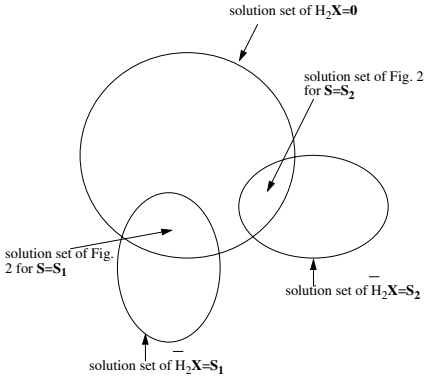

Fig. 3. The encoding space

B. Equivocation across the wire tap channel

In this section, we calculate the equivocation for Eve. Since Eve's channel is a BEC with erasure probability ϵ_w, with probability tending to 1, Eve will have $n\epsilon_w$ erasures as $n \to \infty$. If we have $\epsilon_w > (1 - r_2)$, using $H_2\mathbf{X} = \mathbf{0}$, Eve must

have at least $2^{n(\epsilon_w-(1-r_2))}$ solutions for $\mathbf{X}$, all of which are equally likely. All these solutions will differ from each other in the erased positions. Since ϵ_w is the erasure threshold of the code having H_1 as the parity-check matrix, any submatrix formed using $n\epsilon_w$ columns of H_1 will have full column rank. Thus every solution of $H_2\mathbf{X} = \mathbf{0}$ will give a different value of $\mathbf{S}$, all of which are equally likely. The equivocation for Eve is then $\Delta = n(\epsilon_w-(1-r_2))$. If H_1 is the parity-check matrix of a capacity-achieving code on an erasure channel with erasure probability ϵ_w, $\Delta = n(r_2 - r_1)$, and the message will be completely secure from Eve.

C. Probability of error on the main channel

When Bob receives a vector $\mathbf{Y}$, he first decodes it by using the standard iterative erasure decoding technique for LDPC codes on the Tanner graph of the code C_2. Let the erasure probability of the main channel be at most ϵ_m. Then, as $n \to \infty$, with probability tending to 1 he will be able to recover the transmitted word $\mathbf{X}$. Bob then can find out the product $\overline{H}_2\mathbf{X}$, which is his estimate of the message $\mathbf{S}$.

Example 3: Let C_2 be a $(3, 6)$-regular LDPC code with block-length n. C_2 has rate $r_2 = 1/2$. The code C_1 is chosen to be another LDPC code with all variable nodes having degree 5 and all check nodes having degree 6. C_1 has rate $r_1 = 1/6$. The LDPC code C_2 has an erasure threshold $\alpha^* \approx 0.42$. The code C_1 has an erasure threshold $\beta^* \approx 0.55$. Thus, the secrecy rate is $r_2 - r_1 = 1/3$, and an equivocation of $n(\beta^*-(1-r_2)) = 0.05n$ is guaranteed across the wiretap channel having erasure probability greater than $\beta^* = 0.55$. Bob can decode the message with asymptotically zero probability of error on the main channel having erasure probability at most $\alpha^* = 0.42$.

D. Remarks

Like in the case of noiseless main channel, we could have chosen C_1 to be an LDPC code with erasure threshold $1-\epsilon_w$. $C_1^\perp$ wil then have to be contained in C_2, which has erasure threhold ϵ_m. The matrices H_1 and H_2 will be the parity-check matrices of $C_1^\perp$ and C_2 respectively. Since the dual of an LDPC code is likely to have a significantly high number of low-weight codewords, this requirement appears to be contrary to intuition. A very similar code design problem arises in the construction of quantum error-correcting codes using sparse graphs [7]. After studying several constructions, the authors of [7] conclude that such codes are difficult to construct and are unlikely to have high thresholds.

IV. Noiseless main channel and BSC wiretap channel

In this section, D_1 is noiseless and D_2 is a binary symmetric channel (BSC) with error probability p in Fig. 1. We let C be an $(n, n-k)$ code and $\overline{C}$ be the entire space $\{0,1\}^n$. For an arbitrary k-bit message $\mathbf{S} = \mathbf{s}$, the transmitted word $\mathbf{X} \in \mathbf{s}G^*+C$. See section II for the definition of G^*. Since the cosets of C cover the entire space of n-tuples, Eve's received vector Z belongs to some coset of C, say $\mathbf{u}G^* + C$. If $\mathbf{e}$ denotes the error vector introduced by the BSC in the wire tap channel, we have,

$$Prob\{Z \in \mathbf{u}G^*+C|\mathbf{S} = \mathbf{s}\} = Prob\{\mathbf{e} \in (\mathbf{u}+\mathbf{s})G^*+C\} \quad (7)$$

and

$$Prob\{\mathbf{e} \in (\mathbf{u}+\mathbf{s})G^* + C\} = Prob\{e \in \mathbf{w} + C\} \quad (8)$$

for some n-tuple $\mathbf{w}$. We can now state the criterion for selecting the code C to guarantee security of the message $\mathbf{S}$: we choose C such that for any n-tuple $\mathbf{w}$, we have

$$Prob\{e \in \mathbf{w} + C\} \approx 2^{-k}. \quad (9)$$

Using the above condition in (7),(8), we see that Eve is equally likely to find $\mathbf{Z}$ in any coset of C given any message $\mathbf{S} = \mathbf{s}$. Assuming all $\mathbf{S} = \mathbf{s}$ are equally likely *a priori*, Prob$\{\mathbf{Z} \in \mathbf{u}G^*+C\}$ is independent of $\mathbf{u}$; hence, Prob$\{\mathbf{S} = \mathbf{s}|\mathbf{Z} \in \mathbf{u}G^*+C\} \approx 2^{-k}$, and perfect security is guaranteed.

Using the MacWilliams identities [8, Page 127] for the $(n, n-k)$ linear code C, we get

$$\sum_{e\in C} x^{n-wt(e)}y^{wt(e)} = \frac{1}{2^k}\sum_{i=0}^{n} A_i'(x+y)^{n-i}(x-y)^i, \quad (10)$$

where A_i' is the number of codewords of weight i in the dual code $C^\perp$. Using $x = 1-p$, $y = p$, and $A_0' = 1$ in (10), we get

$$\sum_{e\in C} p^{wt(e)}(1-p)^{n-wt(e)} = 2^{-k} + 2^{-k}\sum_{i=1}^{n} A_i'(1-2p)^i.$$

Using the MacWilliams identities [8, Page 137] for the coset $\mathbf{w} + C$, we get

$$\sum_{e\in \mathbf{w}+C} x^{n-wt(e)}y^{wt(e)} = \frac{1}{2^k}\sum_{i=0}^{n} A_i'(\mathbf{w})(x+y)^{n-i}(x-y)^i, \quad (11)$$

where

$$A_i'(\mathbf{w}) = \alpha_i(\mathbf{w}) - \beta_i(\mathbf{w}) \quad (12)$$

with $\alpha_i(\mathbf{w})$ equal to the number of codewords of weight i in the dual code $C^\perp$ orthogonal to $\mathbf{w}$, and $\beta_i(\mathbf{w})$ equal to the number of codewords of weight i in the dual code $C^\perp$ not orthogonal to $\mathbf{w}$. Using $x = 1-p$, $y = p$, and $A_0'(\mathbf{w}) = 1$ in (11), we get

$$\sum_{e\in \mathbf{w}+C} p^{wt(e)}(1-p)^{n-wt(e)} = 2^{-k} + 2^{-k}\sum_{i=1}^{n} A_i'(\mathbf{w})(1-2p)^i. \quad (13)$$

From (12), we see that $|A_i'(\mathbf{w})| \le A_i'$.

We now state the main security criterion as a theorem without proof.

Theorem 4: If

$$\sum_{i=1}^{n} A_i'(1-2p)^i \approx 0, \quad (14)$$

then Prob$\{e \in \mathbf{w} + C\} \approx 2^{-k}$ for all n-tuples $\mathbf{w}$.

We now provide some examples that satisfy the requirement of (14).

Example 4: (Single parity check codes) The dual of a $(n, n-1, 2)$ single parity check code is the $(n, 1, n)$ repetition code with weight distribution $A'_0 = 1$ and $A'_n = 1$. Hence,

$$\sum_{i=1}^{n} A'_i(1-2p)^i = (1-2p)^n \approx 0$$

for large n. However, the secrecy rate $1/n \to 0$ for large n. This is an example that was first used by Wyner in [2] to motivate coding over a wire tap channel system.

Example 5: (Hamming codes) The weight distribution of the dual of the $[n = 2^m - 1, n-m, 3]$ Hamming code $\mathcal{H}_m$ is $A'_0 = 1$ and $A'_{(n+1)/2} = n$. Hence,

$$\sum_{i=1}^{n} A'_i(1-2p)^i = n(1-2p)^{(n+1)/2} \approx 0$$

for large n. As in the previous example, the secrecy rate tends to zero for large n.

We now state the following theorem without proof that generalizes the above construction method.

Theorem 5: Let $\{C_{(n)}\}$ be a sequence of $(n, n-k_n)$ codes such that Prob{Detection Error}$\leq 2^{-k_n}$ over a BSC with error probability p, $0 \leq p \leq 1/2$ and $\lim_{n\to\infty}\{k_n/n\} < \log_2(1/(1-p))$. Let A'_i be the number of codewords of weight i in the dual code $C^{\perp}_{(n)}$. Then for any n-tuple $\mathbf{w}$, as $n \to \infty$,

$$\sum_{i=1}^{n} A'_i(1-2p)^i \to 0.$$

The existence of $(n, n-k_n)$ linear codes with probability of detection error less than 2^{-k_n} is well known [11, Section 3.6]. Suppose we find a class of such error detecting codes such that

$$R = \lim_{n\to\infty} \frac{k_n}{n}.$$

Then, for large n, the code $C_{(n)}$, when used as the code C over a wire tap channel system with a BSC (with error probability p) as the wiretapper's channel, provides perfect security whenever $R < -\log_2(1-p)$, or $p > 1 - 2^{-R}$. The maximum possible secrecy rate that can be achieved by this construction is therefore $-\log_2(1-p)$.

Codes such as Hamming codes and double error-correcting BCH codes are examples of such error-detecting codes. However, most known class of such codes have $R = 0$, asymptotically.

V. Conclusion

When the wiretapper's channel is a BEC and the main channel is noiseless, we have presented codes that approach secrecy capacity. To our knowledge these are the first and only such codes. However, we have shown that capacity-achieving codes are not necessary in this case. If a code exhibits a threshold behavior across a BEC (codes such as regular LDPC codes), its dual can be used effectively over a wire tap channel system with a BEC as the wiretapper's channel. This result enables the use of codes that can be more easily constructed.

For the case where both the main channel and the wiretapper's channel are BECs, we have studied two approaches for code design. The optimality and secrecy capacity of the constructions need to be studied and explored.

For the case where the wiretapper's channel is a BSC (with error probability p) and the main channel is noiseless, we have shown that codes with good error-detecting properties provide security. The capacity of this construction is $-\log_2(1-p)$, which is less than the secrecy capacity $h(p)$. Capacity-approaching codes will probably be graph-based. Use of graph-based codes for the BSC wiretapper's channel is a subject for future study.

References

[1] C. E. Shannon, "Communication Theory of Secrecy Systems", Bell Syst. Tech. J., vol. 28, pp. 656-715, Oct. 1949.

[2] A. D. Wyner, "The Wire-tap Channel", Bell Syst. Tech. J., vol. 54, no. 8, pp. 1355-1387, 1975.

[3] L. H. Ozarow and A. D. Wyner, "Wire-Tap Channel II", Bell Syst. Tech. J., vol. 63, pp. 2135-2157, Dec. 1984.

[4] I. Csiszar and J. Korner, "Broadcast Channels with Confi dential Messages", IEEE Trans. Inform. Theory, vol. IT-24, pp. 339-348, May, 1978.

[5] U. Maurer, "Secret Key Agreement by Public Discussion from Common Information", IEEE Trans. Info. Theory, vol. 39, no. 3, pp. 733-742, 1993.

[6] U. Maurer, "Unconditionally Secure KEy Agreement and the Intrinsic Conditional Information", IEEE Trans. Info. Theory, vol. 45, no. 2, pp. 499-514, 1999.

[7] D. Mackay, G. Mitchison, and P. McFadden, "Sparse Graph Codes for Quantum Error-correction", quant-ph/0304161, Submitted to IEEE Transactions on Information Theory.

[8] F. J. MacWilliams and N. J. Sloane, The Theory of Error-correcting Codes, Amsterdam, The Netherlands: North-Holland, 1977.

[9] J. Muramatsu, "Secret Key Agreement from Correlated Source Outputs using Low Density Parity Check Matrices", IEICE Trans. Fundamentals, vol. E87-A, no. 0, pp. 1-10, 2004.

[10] P. Oswald and A. Shokrollahi, "Capacity Achieving Sequnces for the Erasure Channel", IEEE Trans. Info. Theory, vol. 48, pp. 3017-3028, Dec. 2002.

[11] S. Lin and D. J. Costello Jr., Error-control Coding: Fundamentals and Applications, Englewood Cliffs, NJ: Prentice Hall Inc., 1983.

[12] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. McLaughlin, and J. M. Merolla, "Capacity Achieving Codes for the Wire Tap Channel with Applications to Quantum Key Distribution", Submitted to IEEE Transactions on Information Theory, preprint available at http://www.arxiv.org/abs/cs.IT/0411003.