ISSN 2186-6570

On Constructive Codes for Wiretap Channels

Mitsuru Hamada

Quantum ICT Research Institute, Tamagawa University
6-1-1 Tamagawa-gakuen, Machida, Tokyo 194-8610, Japan

Tamagawa University Quantum ICT Research Institute Bulletin, Vol.1, No.1, 21-24, 2011

Tamagawa University Quantum ICT Research Institute Bulletin
Vol.1 No.1 : 21-24 (2011)

On Constructive Codes for Wiretap Channels

Mitsuru Hamada
Quantum Information Science Research Center
Quantum ICT Research Institute
Tamagawa University
6-1-1 Tamagawa-gakuen, Machida, Tokyo 194-8610, Japan

***Abstract*—The wiretap channel (Wyner, 1975) is a model for communication subject to eavesdropping in information theory. Recently, the author obtained asymptotically optimal explicit codes for communication over the wiretap channel. Here, the explicitness means that the codes are constructible in polynomial time in their code-lengths. This result is briefly reviewed and it is described how the result was obtained.**

I. Introduction

The wiretap channel [1] is an information-theoretic model for communication subject to eavesdropping. In some rough usage of the term 'wiretap channel,' it also means the problem formulation of secure and reliable information transmission through such leaky channels due to [1], or the now standard generalized problem formulation in [2].

Recently, the author obtained a constructive solution to the problem of the wiretap channel [3], [4]. In the simplest case where the wiretap channel consist of a pair of binary symmetric channels (BSCs), the result can be stated as follows. It has been shown that for any pair (W_1, W_2) of binary symmetric channels, there exists a sequence of encoder-decoder pairs (ϕ_i, ψ_i) that achieves any rate below the secrecy capacity $C_{\rm s} = C_{\rm s}(W_1, W_2)$ while each encoder ϕ_i is constructible in polynomial time in its block length. Here, a BSC means a channel that flips an input symbol 0 into 1, and 1 into 0 with probability p for some $0 \le p \le 1$, 'achieves a rate R' means the information rate of the encoder approaches R as the block length grows large while the encoder-decoder pair fulfills the requirement that the following two quantities should go to zero asymptotically: (i) the decoding error probability for the information transmission through W_1, (ii) the amount of 'information leakage' to the eavesdropper through W_2. These are measures on reliability and security, respectively, and are quantified in standard information-theoretic manners. The number $C_{\rm s}$ has been known as the maximum rate at which information can be sent reliably and securely, but earlier results on achievability are existential.

In this article, the result is briefly reviewed and it is described how the result was obtained.

II. The Result to Be Explained

A. Compact Form of the Result

The author obtained several proofs for the constructive result described in the previous section. In fact, the version published by IEEE [4] of this statement is more general, as described below.

As usual, $\mathbb{F}_q$ denotes the finite field consisting of q elements.

Theorem 1: [4]. Let $P_{\rm unif}$ be the uniform distribution on $\mathbb{F}_q$. For any pair of discrete memoryless channels (W_1, W_2) with input alphabet $\mathbb{F}_q$ (often called wiretap channel), there exists a sequence of encoder-decoder pairs (ϕ_i, ψ_i) such that the sequence achieves any rate below $C' = I(P_{\rm unif}, W_1) - I(P_{\rm unif}, W_2)$, provided $C' > 0$, and each encoder ϕ_i is constructible in polynomial time in its block length.

Here, we have adopted Csiszár and Körner's alternative way of writing $I(P, W)$ in place of the mutual information $I(\mathsf{X};\mathsf{Y})$ for random variables X, Y with $\Pr\{\mathsf{X} = x, \mathsf{Y} = y\} = P(x)W(y|x)$.[1] Note if W_1 is less noisy than W_2 (see [2, Theorem 3] and [6]) and $I(P_{\rm unif}, W_j)$ is the capacity of W_j for $j = 1, 2$, the theorem says that the constructible codes achieve the secrecy capacity of (W_1, W_2). (This is the case if $q = 2$ and W_1, W_2 are BSCs with $C' > 0$ as can be checked elementarily [5]; the statement in Introduction indicates this case.)

B. Remark

We remark that the author has already strengthened the above theorem to the statement that says the secrecy capacity of an arbitrary wiretap channel consisting of discrete memoryless channels is achievable with codes constructible in polynomial time. (The encoders in the above theorem can be tailored to such general wiretap channels.)

For those who have mastered information theory and have read [4], the following remarks on Theorem 1 would be enough to see this strengthening, where $V \cdot W$ denotes the cascade of channels V and W:

- Theorem 1 implies the achievability of $C'' = I(P_{\rm unif}, W_{\rm pre} \cdot W_1) - I(P_{\rm unif}, W_{\rm pre} \cdot W_2)$ with poly-

[1] Definitions of the mutual information can be found in most textbooks of information theory, or in [5].

nomially constructible encoders readily and obviously.

- The achievability of $C''' = I(P, W_{\rm pre} \cdot W_1) - I(P, W_{\rm pre} \cdot W_2)$ for an arbitrary P is still a corollary to Theorem 1 [by a technique of Gallagar's (1968)].

III. Definitions

A. Basics

To go into details, we need definitions. Throughout, n, m, N are positive integers, and logarithms are to base q. We denote by $[vw]$ the juxtaposition (concatenation) of vectors or sequences v and w, e.g., $[(0,1,0)(1,0)] = (0,1,0,1,0)$; the juxtaposition extends naturally to more vectors, e.g., $[uvw] = [[uv]w] = [u[vw]]$.

In this work, as usual, a channel means a stochastic matrix $[W(b|a)]_{(a,b)\in\mathcal{X}\times\mathcal{Y}}$, where $\mathcal{X}, \mathcal{Y}$ are finite or countable sets. We will also refer to such a matrix W as a stochastic map $W : \mathcal{X} \stackrel{\rm stch}{\to} \mathcal{Y}$. The product of matrices $[W(b|a)]_{(a,b)\in\mathcal{X}\times\mathcal{Y}}$ and $[V(c|b)]_{(b,c)\in\mathcal{Y}\times\mathcal{Z}}$ is written as WV or $W \cdot V$ so that the resulting matrix $U = WV$ is given by $U(c|a) = \sum_{b\in\mathcal{Y}} W(b|a)V(c|b)$. This represents the cascade of W and V.

Definition 1: For any function $f : \mathcal{X} \to \mathcal{Y}$, $f^{\rm stch}$ denotes the unique stochastic map $f^{\rm stch} : \mathcal{X} \stackrel{\rm stch}{\to} \mathcal{Y}$ satisfying $f^{\rm stch}(f(x)|x) = 1$ for any $x \in \mathcal{X}$.

B. Structured Encoders for Wiretap Channels

Consider the following simple process for encoding:

> We generate a string w of κ_2 digits uniformly randomly; then, we encode the secret data $v \in \mathbb{F}_q^k$ into $x = [vw]G+t$, where G is a $(k+\kappa_2)\times n$ full-rank matrix and $t \in \mathbb{F}_q^n$.

It has been turned out that this type of encoders or compositions (concatenations) of them are powerful. We also use the following notation.

Definition 2: For k, κ_1, κ_2 with $k = \kappa_1 - \kappa_2$ ($0 \le \kappa_2 \le \kappa_1 \le n$) and a function $f : \mathbb{F}_q^{\kappa_1} \to \mathbb{F}_q^n$, we define a stochastic map (encoder) $[f]_{\kappa_2}^{\rm stch} : \mathbb{F}_q^k \stackrel{\rm stch}{\to} \mathbb{F}_q^n$ by $[f]_{\kappa_2}^{\rm stch} = \mathcal{I}_{k,\kappa_2} \cdot f^{\rm stch}$, where $\mathcal{I}_{k,\kappa_2} : \mathbb{F}_q^k \stackrel{\rm stch}{\to} \mathbb{F}_q^{\kappa_1}$ is defined by

$$\mathcal{I}_{k,\kappa_2}(x|v) = \begin{cases} 1/q^{\kappa_2} & \text{if } \exists w \in \mathbb{F}_q^{\kappa_2}, x = [vw] \\ 0 & \text{otherwise.} \end{cases}$$

The encoder is called an $[[n,k]]$ encoder (over $\mathbb{F}_q$) if f is one-to-one whereas f is called an $[n,\kappa_1]$ encoder.

Example 1: Given a $\kappa_1 \times n$ matrix G and a vector $t \in \mathbb{F}_q^n$, let us define a function $\mathcal{F}_{G,t} : \mathbb{F}_q^{\kappa_1} \to \mathbb{F}_q^n$ by

$$\mathcal{F}_{G,t}(u) = uG + t. \tag{1}$$

Then, $[\mathcal{F}_{G,t}]_{\kappa_2}^{\rm stch}$ stands for the aforementioned simple process for encoding. (It is a convention to call the range of $\mathcal{F}_{G,t}$ an $[n,\kappa_1]$ code when G is of full rank.) Sometimes, G will be called a generator matrix of $[\mathcal{F}_{G,t}]_{\kappa_2}^{\rm stch}$.

In this example, if we divide G into two submatrices as

$$G = \begin{bmatrix} G_1 \\ G_2 \end{bmatrix} \tag{2}$$

where G_1 and G_2 have $\kappa_1 - \kappa_2$ and κ_2 rows, respectively, the role of G_2 may be understood as a kind of scrambler. The encoder $[\mathcal{F}_{G,t}]_{\kappa_2}^{\rm stch}$ has appeared as the encoder of the quotient code C/B in [7], where G_2 and G generate B and C, respectively, and t is the zero vector. We remark that the way to produce the stochastic map $[\mathcal{F}_{G,t}]_{\kappa_2}^{\rm stch}$ described in [7] is different from the above.[2]

Definition 3: A product $[\phi^{(1)}|\cdots|\phi^{(N)}]$ of stochastic maps $\phi^{(i)} : \mathcal{V}^m \stackrel{\rm stch}{\to} \mathcal{W}^n$, $i \in \{1,\dots,N\}$, is defined by

$$[\phi^{(1)}|\cdots|\phi^{(N)}]([x^{(1)}\cdots x^{(N)}]\,|\,[v^{(1)}\cdots v^{(N)}]) = \prod_{i=1}^{N} \phi^{(i)}(x^{(i)}\,|\,v^{(i)}) \tag{3}$$

where $v^{(i)} \in \mathcal{V}^m, x^{(i)} \in \mathcal{W}^n$, $i \in \{1,\dots,N\}$.

C. Wiretap Channels

As usual, a channel $W : \mathcal{X} \stackrel{\rm stch}{\to} \mathcal{Y}$ is called a *memoryless channel* in the situation where a transmitted word $x \in \mathcal{X}^\nu$ is changed by (ν uses of) the channel W into $y \in \mathcal{Y}^\nu$ with probability $W^\nu(y|x)$. Here, W^ν is the νth extension of W:

$$W^\nu = \underbrace{[W|\cdots|W]}_{\nu}. \tag{4}$$

A broadcast channel with confidential messages (BCC) [2] is a pair of channels (W_1, W_2) consisting of memoryless channels $W_1 : \mathcal{X} \stackrel{\rm stch}{\to} \mathcal{Y}$ and $W_2 : \mathcal{X} \stackrel{\rm stch}{\to} \mathcal{Z}$, where $\mathcal{X}, \mathcal{Y}, \mathcal{Z}$ are finite sets. The outputs of W_1 are received by the legitimate user, and those of W_2 by the eavesdropper. We sometimes call a BCC (W_1, W_2) a wiretap channel as in Theorem 1 when no common message is wanted to be broadcast (but only confidential messages) while originally, the part W' of a BCC (W_1, W_1W') was called a wire-tap channel [1].

IV. The Concatenated Encoder

The codes, or encoders more precisely, that have been proved to be constructible in polynomial time and to achieve any rate below C' are concatenated encoders, which generalize Forney's concatenated codes. (Even though C' is not the secrecy capacity for some wiretap channels, the encoders in the above theorem can be modified to achieve the secrecy capacity of the general wiretap channel, as already explained.)

[2] In fact, the primary purpose of writing [7] was to explain the standard (symplectic) quantum error-correcting codes by relating their ability of error correction with that of the corresponding quotient codes. For this purpose, the author did not care for the efficiency of encoding but explaining the relation.

The concatenated encoder proposed by this author [8], [4] is an encoder of the form

$$\tilde{\phi} = \phi_{\text{out}} \cdot [\phi^{(1)}| \cdots |\phi^{(N)}] \tag{5}$$

where ϕ_{out} is an $[[kN, K_{\text{o}}]]$ encoder and $\phi^{(i)}$ are $[[n, k]]$ encoders.[3]

V. Security of the Concatenated Encoder

A lemma on the security of the concatenated encoder $\tilde{\phi}$ (Section IV), used on a BCC (W_1, W_2) as described in Section III-C, was presented in [4]. With this lemma, the achievability of any rate below the secrecy capacity was proved. (The lemma is essentially the same as the security lemma in [3]. Theorem 2 of [4] is a refinement of the lemma, i.e., Lemma 1 thereof.)

VI. How the Codes Were Obtained

A. How the Codes Were Obtained

In 2006, a method for concatenating codes that can be used both for quantum error correction and for communication over wiretap channel was proposed by the author [9]. This has been presented in [9], [10] as a method for creating a pair of linear codes (L_1, L_2) with $L_2^{\perp} \subseteq L_1$ from a pair of q^k-ary codes (D_1, D_2) with $D_2^{\perp} \subseteq D_1$ (outer codes) and pairs of q-ary codes $(C_1^{(i)}, C_2^{(i)})$ with $C_2^{(i)\perp} \subseteq C_1^{(i)}$ and $|C_1^{(i)}/C_2^{(i)\perp}| = q^k$ (inner codes) to encode the ith symbol of D_1 or D_2.[4] [5]

When this author wrote the initial version of [10], the author thought the primary application of this method would be cryptographic protocols. In fact, the motivation for the investigation in [10] was quantum key distribution (QKD) since concrete constructions of (L_1, L_2) were awaited as the heart of QKD protocols, which have been claimed to be information-theoretically (unconditionally [12]) secure. On the other hand, in the community of information theory, interest in another related issue has been revived. The issue is that of wiretap channels. Such situation of communication as described with wiretap channels is the one the author thought most important, and he applied for a patent [8] for the invention of the encoder in Section III-B and the concatenated encoder $\tilde{\phi}$.

It should be explained how such a code pair (L_1, L_2) can be used to transmit secret information. Some analysis of QKD protocols using code pairs (L_1, L_2) with $L_2^{\perp} \subseteq L_1$ is directly applicable to analysis of $L_1/L_2^{\perp}$ used for wiretap channels. This may be expected if one notice that the secret information (key) is encoded into $L_1/L_2^{\perp}$ in such QKD protocols, and we can use $L_1/L_2^{\perp}$ to encode a secret message into $L_1/L_2^{\perp}$ directly for communication over wiretap channels. A code of the form $L_1/L_2^{\perp}$ had been named a quotient code [7].

Thus, the author expected that the concatenated code pairs (L_1, L_2) would be useful for communication over channels subject to eavesdropping in the converted form $L_1/L_2^{\perp}$ and wrote [8] after he had wrote a manuscript arXiv:quant-ph/0610194 (the initial version of [10], submitted in Aug. 2006). Then, he presented security analysis of $L_1/L_2^{\perp}$ used on classical and quantum wiretap channels in [13], [14] invoking to techniques from quantum information theory.

The analysis in [13], [14] is applicable to the polynomial-time constructions of quotient codes $L_1/L_2^{\perp}$ in [9], [15]. As an illustration of the result, an achievable rate of the polynomially constructible quotient codes $L_1/L_2^{\perp}$ was evaluated for the wiretap channel that consists of BSCs. For this specific wiretap channel, however, the result was not very satisfactory in that the obtained rate was suboptimal in this case. (This does not mean the analysis in [13], [14] is all obsolete since the codes are secure against a much wider class of classical channels to the eavesdroppers, not to mention quantum channels, than the class of BSCs.)

Thus, an improvement of this achievable rate were awaited, and the author accomplished this in [3]. Namely, in [3], it was shown that the polynomially constructible code $L_1/L_2^{\perp}$ in [9], [15] actually achieve the secrecy capacity.

The presentation of the code construction in [3], which depends on [9], [15], might look awkward for those interested only in the solution to the classical issue of wiretap channels and not in quantum error correction or QKD; they would prefer the presentation of the code construction in [4] since it is simple and direct. Besides this, the security analysis in [4] is strengthened as compared to that of [3].

B. Remarks

The publication of the solution seems exceptional in that it was first published in a specification of a patent [8], and later the asymptotic optimality (achievability of the secrecy capacity) was established [3], [4].

Note in information theory, it it customary to express an encoder for wiretap channels as a stochastic map following [2]. When the author wrote [8], the way of writing was subject to this convention. The author noticed that this might be confusing for the readers of [8], so that he amended [8]. Specifically, an 'encoder' usually means a device for encoding information (and an 'encoding' usually means a process to encode information verbatim) except in the literature on the wiretap channels in information theory. Whereas the terms 'encoder' and 'encoding' was used primarily in such usual sense in [8], the author called the two-step encoding that corresponds

[3] The concatenated encoder is an $[[nN, K_{\text{o}}]]$ encoder.

[4] A version (close to the original) of the first half of [10] is [11], which uses variable inner codes explicitly; the change of [10] is due to a reviewer's request to avoid the use of variable inner codes since it is not necessary for the main result of [10].

[5] Now the author would like to comment that calling this method concatenating in [10] may have caused some confusion. This is because the concatenated encoder in Section IV seems the legitimate generalization of Forney's concatenated codes whereas the concatenation of pairs of linear codes only generalize the concatenation of linear codes.

to $\tilde{\phi}$ in (5) an $[[nN, K_{\rm o}]]$ encoding in the initial version of [8].[6] But this would not be precise since in [8], an $[[n, k]]$ encoding was defined to be such process as described at the beginning of Section III-B of the present article. Thus, he noticed that the two-step encoding should have been referred to as *equivalent to* an $[[nN, K_{\rm o}]]$ encoding as in the amended version. (The footnote 2, which states that the concatenated encoder is an $[[nN, K_{\rm o}]]$ encoder, is correct since the present article defines an encoder as a stochastic map.)

For those who have read [4], the author would like to make another remark. He wrote in [4]:

> There are two ways to establish Theorem 1 or its analogues:
>
> 1) Find an ensemble of encoders that are good on average, and single out a good encoder from the ensemble. Use it as a fixed inner code in the concatenated encoder;
> 2) Find an ensemble of encoders that are good on average, and use all encoders in the ensemble as variable inner codes in the concatenated encoder.

Here, the inner codes or inner encoders mean the components $\phi^{(i)}$, $i = 1, \ldots, N$, of the concatenated encoder $\tilde{\phi}$ in Section IV. Both fixed and variable inner codes would be interesting. However, I emphasized in [9] a construction with variable inner codes.

In retrospect, the primary reason for this seems to be that at the time of writing [9],

> the author expected his polynomially constructible codes [9] using variable inner codes would be proved to achieve larger rates by some security analysis that was not yet obtained at that time.

The work [4] or [3] has presented such security analysis and resulting achievable rates. The codes have turned out to be optimal for a wide class of wiretap channels in that they achieve the asymptotically optimum rate, the secrecy capacity, and can be used as the heart of secrecy-capacity-achieving codes for other wiretap channels. (This was presented in [3]; the work [4] covers most contents of [3] relevant to the achievability).

The author also suggested a construction with fixed inner codes in [9] implicitly. However, this construction needs to be modified to achieve the secrecy capacity. The modification is the first code construction in [4].

VII. Concluding Remarks

In view of the fact that Forney's concatenated codes have influenced subsequent researches and developments of the art of coding both theoretically and practically still after decades, the method for concatenating codes for the wiretap channel would also be worth further investigations. Thus, the author has been continuing the study on this method.

[6] In [8], the variables corresponding to $n, K_{\rm o}$ are slightly different from those of this article. Namely, the $[[nN, K_{\rm o}]]$ encoding has appeared as $[[N'', K']]$ encoding in [8]. In [8], the two-step encoding has been named so since the suggested process is the process corresponding to $\phi_{\rm out}$ followed by the process corresponding to $[\phi^{(1)}| \cdots |\phi^{(N)}]$.

References

[1] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, pp. 1355–1387, Oct. 1975.

[2] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Information Theory*, vol. IT-24, no. 3, pp. 339–348, May 1978.

[3] M. Hamada, "Constructive codes achieving the secrecy capacity of wiretap channels," *IEICE Tech. Report*, ISEC2009-73, pp. 15–22, Dec. 2009.

[4] ——, "Security of concatenated encoders for wiretap channels," *Proc. 2010 IEEE International Symposium on Information Theory (ISIT)*, pp. 2558–2562, Jun. 2010.

[5] ——, "Constructive codes for communication over channels subject to eavesdropping," *Tamagawa University Research Review*, no. 16, pp. 19–49, Dec. 2010.

[6] M. van Dijk, "On a special class of broadcast channels with confidential messages," *IEEE Trans. Information Theory*, vol. 43, no. 2, pp. 712–714, Mar. 1997.

[7] M. Hamada, "Quotient codes and their reliability," *IPSJ Digital Courier*, vol. 1, no. 0, pp. 450–460, Oct. 2005, available at `http://www.jstage.jst.go.jp/article/ipsjdc/1/0/1_450/_article`. Also appeared in *IPSJ Journal*, vol. 46, pp. 2428–2438, no. 10, Oct., 2005.

[8] M. Hamada, "Encoding device for error correction, encoding method for error correction and encoding program for error correction," Patent (Japan), no. 4756489, tokkai2011-172279, submitted Sep. 2006.

[9] ——, "Conjugate codes for secure and reliable information transmission," *Proceedings of IEEE Information Theory Workshop*, Chengdu, China, pp. 149–153, Oct. 2006. Corrections to typos, as well as an exposition of the results, can be found in arXiv:1001.1806 [cs.IT].

[10] ——, "Concatenated quantum codes constructible in polynomial time: Efficient decoding and error correction," *IEEE Trans. Information Theory*, vol. 54, no. 12, pp. 5689–5704, Dec. 2008.

[11] ——, "Efficient quotient codes decodable in polynomial time for quantum error correction and cryptography," *Proc. of the 2008 International Symposium on Information Theory and Its Applications, ISITA*, pp. 293–298, Dec. 2008.

[12] D. Mayers, "Unconditional security in quantum cryptography," *J. Assoc. Comp. Mach.*, vol. 48, pp. 351–406, 2001.

[13] ——, "Algebraic and quantum theoretical approach to coding on wiretap channels," *Proc. International Symposium on Communication, Control and Signal Processing*, Malta, pp. 520–525, Mar. 2008.

[14] ——, "Constructive codes for classical and quantum wiretap channels," in *Cryptographic Research Perspectives*, R. E. Chen, ed., pp. 1–48, 2009, ISBN 978-1-60456-492-1.

[15] ——, "Constructive conjugate codes for quantum error correction and cryptography," 2007, e-Print arXiv:cs/0703141v2 (cs.IT).