2014 IEEE International Conference on Cloud Engineering

Wiretap Channel with Correlated Sources

Yanling Chen*, Ning Cai†, Aydin Sezgin*
* Chair of Communication Systems, Ruhr University Bochum, Germany. Email: {yanling.chen-q5g, aydin.sezgin}@rub.de
† The State Key Lab. of ISN, Xidian University, Xi'an, China. Email: caining@mail.edu.cn

***Abstract*—This paper studies the problem of secret-message transmission over a wiretap channel with correlated sources in the presence of an eavesdropper who has no source observation. A coding scheme is proposed based on a careful combination of 1)** *Wyner-Ziv's source coding* **to generate secret key from correlated sources based on a certain cost on the channel; 2)** *one-time pad* **to secure messages without additional cost; and 3)** *Wyner's secrecy coding* **to achieve secrecy based on the advantage of legitimate receiver's channel over the eavesdropper's. The work sheds light on optimal strategies for practical code design for secure communication/storage systems.**

I. Introduction

The availability and processing of massive amounts of data, nicknamed *big data*, is a challenge faced by researchers and companies alike. In particular, as new technologies like cloud computing, smart grid, and biometrics mature, security and privacy issues have attracted global attention. How to deal with the big data in a smart way that utilizes the available resources efficiently while keeping the sensitive information protected, is of growing concern.

Cryptography serves as an effective and essential tool to protect data. However, cryptographic schemes usually involve a computational burden and a problematic issue of efficient key management. The security of those techniques is breached if there exists an efficient algorithm or if the attacker holds sufficient computational power. *Information theoretic secrecy*, on the other hand, offers a stronger security by requiring that the eavesdropper is clueless no matter the computational power he/she holds (i.e., *perfect secrecy*). The concept was introduced by Shannon [1], who considered a cipher system where both the intended receiver and the eavesdropper have direct access to the cipher-text. Under this setting, he showed that perfect secrecy can *only* be achieved when $H(K) \geq H(M)$, where $H(K)$ and $H(M)$ are the entropies of the secret key K and the message M, respectively. Note that K is shared by the transmitter and the intended receiver beforehand.

Wyner, in his seminal paper [2], introduced the wiretap channel, where he addressed the problem of secret-message transmission from a transmitter to a legitimate receiver (without sharing keys beforehand) over a degraded broadcast channel in the presence of an eavesdropper. It is shown that the secure communication is still possible by assuming that the eavesdropper always observes a *degraded* version of the legitimate receiver's observation. The fundamental limit of the secure communication, called *secrecy capacity*, is defined to be the maximum rate at perfect secrecy. Later on, Csiszár and Körner [3] extended Wyner's work by considering a general setup of transmitting secret- and common-message over a general broadcast channel, and provided a single-letter characterization of the secrecy capacity region.

For those wiretap channels which have a zero secrecy capacity, interestingly, Maurer [4] demonstrated that it is still possible to achieve a positive secret rate if a public feedback channel is made available. In parallel, Csiszár and Ahlswede [5] recognized that correlated sources observations could be explored for generating secret-key that could be used further for secret-message transmission via one-time pad. These offer alternative solutions to achieve information theoretic secrecy especially in cases that it is hopeless via the wiretap channel only (i.e., without key, feedback, side information, etc).

There has been a body of literature studying the problem of either secrecy-massage transmission or secret-key generation in different settings and extensions of wiretap channels and source models. Recently, a combined approach is taken by Prabhakaran *et al.* in [6], which aimed to characterize the trade-off of the secret-message and secret-key rates for the wiretap channel with correlated sources (where the channel is state-independent). They provided an achievable rate region, whilst the secrecy capacity region still remains open. Their result follows by considering a more general setup (where the channel is state-dependent, and the state is the source available at the transmitter).

In contrast to the approach taken in [6], here we provide an achievability scheme by directly considering a simple model of the wiretap channel with correlated sources where the eavesdropper has no source observation. We only focus on the secret-message problem, whilst the same coding scheme can be employed to derive achievable region for secret-key or the trade-off of secret-message and secret-key rates. The purpose of this work is to gain insights into the code design strategies that could fully exploit the advantages of both channel and sources. Our coding scheme follows by applying the classical methods of Wyner-Ziv source coding, one-time pad, and Wyner's secrecy coding. Information theoretic secrecy is achieved in the manner of crypto-coding in one step.

978-1-4799-3766-0/14 $31.00 © 2014 IEEE
DOI 10.1109/IC2E.2014.80

The rest of the paper is organized as follows: In Section II, we give the system model. In Section III, we briefly describe our main result. In Section IV, we establish an achievability scheme. Proofs of two lemmas are present in Section V. Finally, we conclude in Section VI.

II. Preliminaries

In this paper, we will denote the discrete random variables U, V, X, etc. by upper case letters; their realizations by corresponding lower case cases; and, the finite sets by script letters.

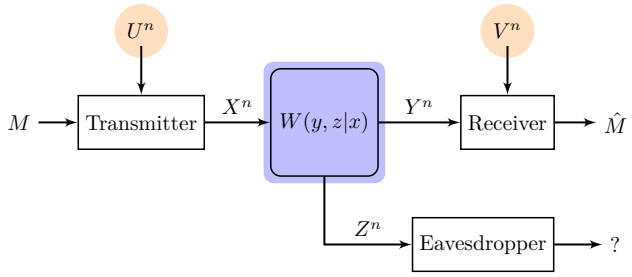

Fig. 1: Wiretap channel with correlated sources at the transmitter and the legitimate receiver in presence of an eavesdropper.

Our system model is given in Fig. 1. It consists of

- 3 terminals: a *transmitter*, a legitimate *receiver* and an *eavesdropper*;
- a discrete memoryless broadcast *channel* defined by $W(y, z|x)$;
- correlated *sources*, U^N and V^N, which are discrete memoryless, and non-causally known at the transmitter and the legitimate receiver, respectively.

Assume that the sources are independent of the channel. The objective is to achieve secret-message transmission over the noisy channel to the legitimate receiver in the presence of the eavesdropper. In particular, to transmit a message $M \in \mathcal{M}$ to the legitimate receiver in n uses of the channel,

- the transmitter, based on the knowledge of M and U^n, sends a codeword X^n to the channel;
- the legitimate receiver, upon receipt of Y^n and source observation V^n, makes an estimate $\hat{M}$ of the message M, such that it satisfies the *reliability* condition:

$$P_e = \Pr\{\hat{M} \neq M\} \leq \epsilon_n; \tag{1}$$

- whilst the eavesdropper observes Z^n and the information leakage $I(M; Z^n)$ shall satisfy the *secrecy* condition:

$$I(M; Z^n) \leq n\epsilon_n. \tag{2}$$

Define the transmission *rate* to be

$$R = \frac{1}{n} \log |\mathcal{M}|.$$

We say that rate R is *achievable* if there exist a sequence of encoding-decoding schemes with rate $R - \epsilon_n$, such that both conditions (1)-(2) are fulfilled, for ϵ_n such that $\epsilon_n \to 0$ as $n \to \infty$.

The maximum achievable rate, i.e., *secrecy capacity,* subject to both constraints on reliability and secrecy, is of our interest. The solution to this problem provides a fundamental limit for a reliable and secure communication between the transmitter and the legitimate receiver, while keeping the eavesdropper completely ignorant of the transmitted information.

III. Main Results

In this section, we summarize the main result of the paper, which proof is given in the following sections.

Theorem 1. *The secrecy capacity of the discrete memoryless wiretap channel with correlated sources available non-causally at the transmitter and the legitimate receiver is lower bounded by*

$$\max_{p(w|u)p(t)} \{|I(T;Y) - \max\{I(T;Z), I(W;U)\}|^+ + I(W;V)\}, \tag{3}$$

where $|a|^+ = \max(a, 0)$ *and*

$$I(T;Y) \geq I(W;U) \tag{4}$$

for a given distribution:

$$p(u, v, w, t, x, y, z) = p(u, v)p(w|u)p(t)p(x|t)W(y, z|x).$$

Easily, we have the following observations:

1): In the case of $U = V = \emptyset$, the above lower bound reduces to the secrecy capacity for the wiretap channel as established by Csiszár and Körner in [3]:

$$C_s^1 = \max_{p(t,x)} |I(T;Y) - I(T;Z)|^+.$$

2): In the case of $V = \emptyset$, the above lower bound reduces to the secrecy capacity for the wiretap channel with side information non-causally known at the transmitter, where, however, the side information is independent of the channel since $p(y, z|x, u) = p(y, z|x)$:

$$C_s^2 = \max_{p(t,x)} |I(T;Y) - I(T;Z)|^+.$$

3): In the case of $U = V$, the above lower bound reduces to the secrecy capacity for the wiretap channel with shared key as stated in [7, (22.7)]:

$$C_s^3 = \max_{p(t,x)} \min\{|I(T;Y) - I(T;Z)|^+ + R_K, I(T;Y)\},$$

where $T \to X \to (Y, Z)$ forms a Markov chain; and $R_K = \max_{p(w|u)} I(W;U) = H(U)$.
In particular, when Z is a *degraded* version of Y, then we have the secrecy capacity

$$C_{s1}^3 = \max_{p(x)} \min\{I(X;Y) - I(X;Z) + H(U), I(X;Y)\},$$

which is the same as shown in [8]; Moreover, when Z is *less noisy* than Y, then we have the secrecy capacity

$$C_{s2}^3 = \max_{p(x)} \min\{H(U), I(X;Y)\},$$

which coincides with the result in [8, Sec. III-C-2)].

IV. Coding Scheme

For a given distribution $p(w|u)p(t)p(x|t)$, we provide the coding scheme in two cases 1). $I(T;Y) > I(T;Z)$ and 2). $I(T;Y) \leq I(T;Z)$, respectively. We note that Markov chains $W \to U \to V$ and $T \to X \to (Y,Z)$ hold.

A. $I(T;Y) > I(T;Z)$

Choose $R_1, R_2 \geq 0$ such that

$$\begin{aligned} R_2 &\leq I(W;V) - \epsilon; &(5)\\ R_1 &\leq I(T;Y) - \max\{I(T;Z), I(W;U)\} - \epsilon. &(6)\end{aligned}$$

Additionally, we let

$$\begin{aligned} R_0 &= I(W;U) - R_2 + \epsilon; &(7)\\ R_3 &= |I(T;Z) - I(W,U) - 2\epsilon|^+. &(8)\end{aligned}$$

Note that the secret-message rate R_2 will be achieved via one-time pad; whilst R_1 will be achieved via Wyner's secrecy coding.

Codebook generation:

First, randomly and independently generate $2^{n(R_0+R_2)} = 2^{n(I(W;U)+\epsilon)}$ sequences $w^n(s,k)$ with $(s,k) \in [1 : 2^{nR_0}] \times [1 : 2^{nR_2}]$ according to $p(w)$. For W^n, we use S to denote the random variable representing the bin index of W^n; and K the index in the bin. The source codebook is denoted to be $\mathcal{C}_k$; and, the sub-codebook for bin s to be $\mathcal{C}_k(s)$.

Besides, randomly and independently generate $2^{n(R_1+R_2+R_0+R_3)} \leq 2^{n(I(T;Y)-\epsilon)}$ codewords $t^n(m_1,i,s,r)$, with $(m_1,i,s,r) \in [1 : 2^{nR_1}] \times [1 : 2^{nR_2}] \times [1 : 2^{nR_0}] \times [1 : 2^{nR_3}]$. The codebook is denoted to be $\mathcal{C}$.

Encoding at the transmitter:

Rate splitting: Assume M has a uniform distribution. Split M of nR bits into two parts, i.e., $M = (M_1, M_2)$, where M_1 is of nR_1 bits, M_2 of nR_2 bits, and $R = R_1 + R_2$.

Let $m = (m_1, m_2) \in [1 : 2^{nR_1}] \times [1 : 2^{nR_2}]$ be the message to be sent. The encoder has access to U^n. Assume the sender receives u^n and further assume that $u^n \in \mathcal{T}_U^n$ since it will hold with probability $\to 1$ as n increases. (In fact, an error event $\mathcal{E}_1$ is declared if $(u^n, v^n) \notin \mathcal{T}_{U,V}^n$.)

By the source codebook construction of $\mathcal{C}_k$, with a high probability there is at least one w^n which is jointly typical with u^n. In the case that w^n is not unique, one can choose w^n randomly and uniformly. If no such sequence exists, then an error event $\mathcal{E}_2$ is declared. Otherwise, we denote the sequence accordingly chosen to be $w^n(s,k)$.

Furthermore, the sender calculates $i = m_2 \oplus k$, randomly chooses an $r \in [1 : 2^{nR_3}]$ and finds $t^n(m_1,i,s,r)$ in the codebook $\mathcal{C}$ (An error event $\mathcal{E}_3$ is declared if $t^n(m_1,i,s,r) \notin \mathcal{T}_{W|U}^n$). Conditioned on $t^n(m_1,i,s,r)$, a codeword x^n is randomly generated according to $p(x|t)$ and sent through the channel. Note that we denote I to be the random variable representing $I = M_2 \oplus K$.

Decoding at the legitimate receiver:

Upon receiving y^n, the legitimate receiver searches for a unique t^n such that (t^n, y^n) are jointly typical, and accordingly recovers (m_1, i, s, r) from t^n. Error event $\mathcal{E}_4$ is declared if $y^n \notin T_Y^n$; $\mathcal{E}_5$ is declared if no such t^n is found such that $(t^n, y^n) \in T_{T,Y}^n$; or $\mathcal{E}_6$ is declared in case of another t^n or more than one are found.

With the source observation of v^n and the knowledge of s, the legitimate receiver can recover w^n by searching for, in source sub-codebook $\mathcal{C}_k(s)$, a sequence which is jointly typical with v^n. If a unique sequence $w^n(s,\hat{k})$ is found, m_2 will be decoded to be $\hat{m}_2 = i \oplus \hat{k}$. An error event $\mathcal{E}_7$ is declared if no such w^n is found; and an error event $\mathcal{E}_8$ is declared if another w^n or more than one are found.

Analysis of the probability of error:

There are following possible errors that might happen in the encoding and decoding procedure:

$$\begin{aligned}
&\mathcal{E}_1 = \{(u^n, v^n) \notin \mathcal{T}_{U,V}^n\};\\
&\mathcal{E}_2 = \{(u^n, w_*^n) \notin \mathcal{T}_{U,W}^n \text{ for all } w_*^n \in \mathcal{C}_k\};\\
&\mathcal{E}_3 = \{t^n \notin \mathcal{T}_T^n\};\\
&\mathcal{E}_4 = \{y^n \notin \mathcal{T}_Y^n\};\\
&\mathcal{E}_5 = \{(t_*^n, y^n) \notin \mathcal{T}_{T,Y}^n \text{ for all } t_*^n \in \mathcal{C}\};\\
&\mathcal{E}_6 = \{\exists t_*^n \text{ s.t. } (t_*^n, y^n) \in \mathcal{T}_{T,Y}^n \text{ where } t_*^n \neq t^n\};\\
&\mathcal{E}_7 = \{(v^n, w_*^n) \notin \mathcal{T}_{V,W}^n \text{ for all } w_*^n \in \mathcal{C}_k(s)\};\\
&\mathcal{E}_8 = \{\exists w_*^n \text{ s.t. } (v^n, w_*^n) \in \mathcal{T}_{V,W}^n \text{ for } w_*^n \neq w^n, w_*^n \in \mathcal{C}_k(s)\}.
\end{aligned}$$

By the union bound, we can bound the probability of error to be

$$\begin{aligned}
P_e \leq\, &\Pr(\mathcal{E}_1) + \Pr(\mathcal{E}_2|\mathcal{E}_1^c) + \Pr(\mathcal{E}_3|\mathcal{E}_1^c, \mathcal{E}_2^c) + \Pr(\mathcal{E}_4|\mathcal{E}_3^c)\\
&+ \Pr(\mathcal{E}_5|\mathcal{E}_1^c, \mathcal{E}_2^c, \mathcal{E}_3^c, \mathcal{E}_4^c) + \Pr(\mathcal{E}_6|\mathcal{E}_1^c, \mathcal{E}_2^c, \mathcal{E}_3^c, \mathcal{E}_4^c)\\
&+ \Pr(\mathcal{E}_7|\mathcal{E}_1^c, \mathcal{E}_2^c) + \Pr(\mathcal{E}_8|\mathcal{E}_2^c).
\end{aligned}$$

We obtain $P_e \to 0$ as $n \to \infty$ as a result of the following arguments.

- $\Pr(\mathcal{E}_1) \to 0$ as $n \to \infty$: this is due to the fact that (u^n, v^n) are discrete memoryless sources generated according to $p(u,v)$; and as $n \to \infty$, (u^n, v^n) are jointly typical with probability $\to 1$.
- $\Pr(\mathcal{E}_2|\mathcal{E}_1^c) \to 0$ as $n \to \infty$: this is due to the covering lemma [7]; and the fact that by the source codebook generation, there are $2^{n(I(W;U)+\epsilon)}$ sequences w_*^n in $\mathcal{C}_k$.
- $\Pr(\mathcal{E}_3|\mathcal{E}_1^c, \mathcal{E}_2^c) \to 0$ as $n \to \infty$: this is due to the fact that t^n is generated according to $p(t)$; and as $n \to \infty$, t^n belongs to the typical set $\mathcal{T}_T^n$ with probability $\to 1$.
- $\Pr(\mathcal{E}_4|\mathcal{E}_3^c) \to 0$ and $\Pr(\mathcal{E}_5|\mathcal{E}_1^c, \mathcal{E}_2^c, \mathcal{E}_3^c, \mathcal{E}_4^c) \to 0$ as $n \to \infty$: this is due to the conditional typicality lemma [7]; and the fact that given $t^n \in \mathcal{T}_T^n$, y^n is output through the discrete memoryless channel $p(x|t)p(y|x)$.
- $\Pr(\mathcal{E}_6|\mathcal{E}_1^c, \mathcal{E}_2^c, \mathcal{E}_3^c, \mathcal{E}_4^c)$ as $n \to \infty$: this is due to the packing lemma [7]; and by the codebook generation of $\mathcal{C}$, there are $2^{n(I(T;Y)-\epsilon)}$ sequences t_*^n in $\mathcal{C}$.

- $\Pr(\mathcal{E}_7|\mathcal{E}_1^c,\mathcal{E}_2^c) \to 0$ as $n \to \infty$: this is due to the Markov lemma [7]; and the fact that given $(u^n,v^n) \in \mathcal{T}^n_{U,V}$ and $(u^n,w^n) \in \mathcal{T}^n_{U,W}$, and the Markov Chain $W \to U \to V$ (i.e., $p(v|u,w)=p(v|u)$), (u^n,v^n,w^n) are jointly typical with probability $\to 1$.
- $\Pr(\mathcal{E}_8|\mathcal{E}_2^c) \to 0$ as $n \to \infty$: this is due to the packing lemma [7]; and the fact that by the source codebook generation, there are 2^{nR_2} sequences w_*^n in sub-codebook $\mathcal{C}_k(s)$ with $R_2 \le I(W;V)-\epsilon$.

Analysis of equivocation at the eavesdropper:

To show the secrecy of the message from the eavesdropper, we need the following two lemmas. Lemma 2 shows the uniformity of the key generated from correlated sources; whilst Lemma 3 gives an upper bound on the eavesdropper's equivocation on the codeword T^n with his observation Z^n and the knowledge of M_1, M_2. Their proofs are provided in Section V.

Lemma 2. *For K,S as defined in codebook generation,*
1) $H(K) \ge n(R_2-\epsilon')$;
2) $H(K,S) \ge n(R_0+R_2-\epsilon'')$.

Lemma 3. *Equivocation on T^n given Z^n, M_1 and M_2 :*

$$H(T^n|M_1,M_2,Z^n) \le n|I(W;U)-I(T;Z)+2\epsilon|^+ + n\delta'.$$

Secrecy of M_2 given Z^n at the eavesdropper:

$$\begin{aligned}
H(M_2|Z^n) &\ge H(M_2|Z^n,I,S) && (9)\\
&\ge H(M_2|I,S) - I(M_2;Z^n|I,S) && (10)\\
&\overset{(a)}{=} H(M_2|I,S) && (11)\\
&= H(M_2,I,S) - H(I,S) && (12)\\
&\overset{(b)}{=} H(M_2)+H(K,S)-H(I,S) && (13)\\
&\overset{(c)}{\ge} n(R_2-\epsilon''), && (14)
\end{aligned}$$

where I is the random variable representing $I = M_2 \oplus K$;
And,
(a) is due to the Markov chain $(M_2,U^n) \to (I,S) \to Z^n$;
(b) is due to the fact that $H(M_2,I,S) = H(M_2,K,S) = H(M_2)+H(K,S)$ since M_2 is independent of K,S;
(c) is due to the fact that $H(M_2) = nR_2$; $H(K,S) \ge n(R_0+R_2-\epsilon'')$ by Lemma 2-2); and $H(I,S) \le n(R_0+R_2)$ by the source codebook construction.

Note that above proof implies also $I(M_2;I) \le I(M_2;I,S) \le n\epsilon''$. Therefore, our coding scheme transmits M_2 via I in a manner of one-time pad.

Secrecy of M_1 given Z^n, M_2 at the eavesdropper:

$$\begin{aligned}
&H(M_1|M_2,Z^n) = H(M_1,M_2,Z^n) - H(M_2,Z^n)\\
&= H(T^n,M_1,M_2,Z^n) - H(T^n|M_1,M_2,Z^n) - H(M_2,Z^n)\\
&\overset{(d)}{=} H(T^n)+H(M_2|T^n)+H(Z^n|T^n)\\
&\quad - H(T^n|M_1,M_2,Z^n) - H(M_2,Z^n)\\
&\overset{(e)}{\ge} H(T^n)+H(M_2|T^n)+nH(Z|T)\\
&\quad - H(T^n|M_1,M_2,Z^n) - H(M_2) - H(Z^n)\\
&\overset{(f)}{\ge} H(T^n)+H(M_2|T^n)-nI(T;Z)\\
&\quad - H(T^n|M_1,M_2,Z^n) - H(M_2)\\
&\overset{(g)}{\ge} n(R_1+R_2+R_0+R_3)+H(M_2|T^n)-nI(T;Z)\\
&\quad - H(T^n|M_1,M_2,Z^n) - H(M_2) - n\epsilon''\\
&\overset{(h)}{=} n(R_1+R_2+R_0+R_3)+H(M_2|I,S)-nI(T;Z)\\
&\quad - H(T^n|M_1,M_2,Z^n) - H(M_2) - n\epsilon''\\
&\overset{(i)}{\ge} n(R_1+R_2+R_0+R_3)-nI(T;Z)\\
&\quad - H(T^n|M_1,M_2,Z^n) - 2n\epsilon''\\
&\overset{(j)}{\ge} n(R_1+R_2+R_0+R_3)-nI(T;Z)\\
&\quad - n|I(W;U)-I(T;Z)+2\epsilon|^+ - n\delta' - 2n\epsilon''\\
&\overset{(k)}{\ge} n(R_1-\delta''),
\end{aligned}$$

where
(d) is due to the Markov chain $(M_1,M_2) \to T^n \to Z^n$; and that the realization of T^n indicates the value of M_1.
(e) is due to the fact $H(Z^n|T^n) = nH(Z|T)$ since the channel is discrete memoryless; and $H(M_2,Z^n) \le H(M_2)+H(Z^n)$;
(f) is due to the fact that $H(Z^n) = \sum_{i=1}^n H(Z_i|Z^{i-1}) \le \sum_{i=1}^n H(Z_i) = nH(Z)$;
(g) follows from the fact that $H(T^n) \ge n(R_1+R_2+R_0+R_3-\epsilon'')$ since there is a one-to-one mapping between $t^n \in \mathcal{C}$ and $(m_1,i,s,r) \in [1:2^{nR_1}] \times [1:2^{nR_2}] \times [1:2^{nR_0}] \times [1:2^{nR_3}]$. where m_1, r are chosen uniformly and independently of i,s; and $H(I,S) \ge H(I,S|M_2) = H(K,S) \ge n(R_0+R_2-\epsilon'')$ by Lemma 2-2);
(h) follows from the fact that $H(M_2|T^n) = H(M_2|I,S)$ since there is a one-to-one mapping between $t^n \in \mathcal{C}$ and $(m_1,i,s,r) \in [1:2^{nR_1}] \times [1:2^{nR_2}] \times [1:2^{nR_0}] \times [1:2^{nR_3}]$, and m_1, r are chosen independently of m_2 and i,s;
(i) is due to the fact that $H(M_2) - H(M_2|I,S) = I(M_2;I,S) = H(M_2)+H(I,S)-H(M_2,I,S) = H(I,S)-H(K,S) \le n\epsilon''$ since $H(K,S) \ge n(R_0+R_2-\epsilon'')$ by Lemma 2-2) and $H(I,S) \le n(R_0+R_2)$ by the source codebook construction; and the fact that $R_1+R_2+R_0+R_3 = I(T;Y)-\epsilon$;
(j) is due to Lemma 3;
(k) is by substituting R_0 and R_3 by their definitions in (7) and (8), respectively; and taking $\delta'' = \epsilon+\delta'+2\epsilon''$.

Achievable secret rate at the legitimate receiver:

The achievable secret-message rate is R_1+R_2, where R_1, R_2 are specified in (5) and (6), respectively. Thus we obtain the following lower bound on the secrecy capacity:

$$C_s \ge \max_{p(w|u)p(t)} |I(T;Y)-\max\{I(T;Z),I(W;U)\}|^+ + I(W;V). \quad (15)$$

B. $I(T;Y) \le I(T;Z)$

In the case where $I(T;Y) \le I(T;Z)$, the secrecy capacity of the channel is zero without the help of correlated sources. So the correlated sources are the only advantage

that could be exploited in order to achieve a positive secret-message rate. Note surprisingly, this rate will be limited by the secret key rate $I(W;V)$ as employing the Wyner-Ziv source coding. This is feasible under the assumption (4): $I(W;U) \leq I(T;Y)$.

We choose

$$R_2 \leq I(W;V) - \epsilon, \quad (16)$$
$$R_0 = I(W;U) - R_2 + \epsilon. \quad (17)$$

Here the secret-message rate R_2 will be achieved via one-time pad.

Codebook generation:

First, we generate the source codebook which is the same as in subsection IV-A for case $I(T;Y) > I(T;Z)$. Randomly and independently generate $2^{n(R_0+R_2)}$ sequences $w^n(s,k)$ with $(s,k) \in [1:2^{nR_0}] \times [1:2^{nR_2}]$.

Besides, randomly and independently generate $2^{n(I(T;Y)-\epsilon)}$ codewords $t^n(s,i,r)$, with $(s,i,r) \in [1:2^{nR_0}] \times [1:2^{nR_2}] \times [1:2^{nR_3}]$. Here $R_3 = I(T;Y) - R_0 - R_2 - \epsilon \geq 0$.

Encoding at the transmitter:

Let $\{1,2,\cdots,2^{nR_2}\}$ be the message set. The sender receives u^n and wants to send message m_2. Then for $u^n \in \mathcal{T}_U^n$, the sender will find a sequence $w^n(s,k)$ which is jointly typical with u^n. Randomly choosing an r, the sender finds $t^n(s,i,r)$ with $i = k \oplus m_2$ in the channel codebook and accordingly sends codeword x^n.

Decoding at the legitimate receiver:

Upon receiving y^n, the legitimate decoder can recover $t^n(s,i,r)$ (thus s,i) correctly with a high probability. Then with his knowledge of v^n, he can recover w^n by searching for in bin s in the source codebook a $w^n(s,\hat{k})$ which is jointly typical with v^n. Then decode m to be $\hat{m}_2 = i \oplus \hat{k}$.

Analysis of the probability error:

This can be done in the same manner as in subsection IV-A for case $I(T;Y) > I(T;Z)$ and thus omitted here.

Analysis of equivocation at the eavesdropper:

In this case, we only need to prove the secrecy of M_2 given Z^n at the eavesdropper. The proof is the same as shown in (9)-(14) and omitted here.

Achievable secret rate at the legitimate receiver:

The achievable secret-message rate is R_2 as specified in (16). Thus, in the case where $I(T;Y) \leq I(T;Z)$, we have the following lower bound on the secrecy capacity

$$C_s \geq I(W;V). \quad (18)$$

Combining (15) and (18), we establish Theorem 1.

V. Proofs of Lemma 2 and Lemma 3

Lemma 2:For K,S as defined in codebook generation,

1) $H(K) \geq n(R_2 - \epsilon')$;
2) $H(K,S) \geq n(R_0 + R_2 - \epsilon'')$.

Proof: First we define $\mathcal{E}$ to be the event: $\mathcal{E} = \{U^n \in \mathcal{T}_U^n\}$; and, accordingly E to be an indicator random variable which takes value 1 if $u^n \in \mathcal{T}_U^n$; and 0 otherwise.

Recall the source codebook $\mathcal{C}_k$. Note that it contains $2^{n(I(W;U)+\epsilon)}$ sequences $w^n(s,k)$ with $(s,k) \in [1:2^{nR_0}] \times [1:2^{nR_2}]$, which are randomly and independently generated according to $p(w)$. For those codewords with a fixed index $k \in [1:2^{nR_2}]$, we denote them as a sub-codebook $\mathcal{C}_k(k)$. Note that there are 2^{nR_0} sequences w^n in $\mathcal{C}_k(k)$.

For $u^n \in \mathcal{T}_U^n$ (i.e., $E=1$), define $\mathcal{E}_k$ to be the event that $K=k$. That is,

$$\mathcal{E}_k = \{\exists w^n \in \mathcal{C}_k(k) \text{ s.t. } (u^n,w^n) \in \mathcal{T}_{U,W}^n | u^n \in \mathcal{T}_U^n\}.$$

Note that $\Pr(K=k|E=1) = \sum_{u^n \in \mathcal{T}_U^n} p(u^n) \Pr\{\mathcal{E}_k\}$; and

$$\begin{aligned}
\Pr\{\mathcal{E}_k\} &= 1 - \Pr\{\mathcal{E}_k^c\} \\
&= 1 - \Pr\{(u^n,w^n) \notin \mathcal{T}_{U,W}^n \text{ for all } w^n \in \mathcal{C}_k(k) | u^n \in \mathcal{T}_U^n\} \\
&\overset{(a)}{\leq} 1 - (1 - 2^{-n(I(W;U)-\epsilon_0)})^{2^{nR_0}} \\
&\overset{(b)}{\leq} 2^{nR_0} \cdot 2^{-n(I(W;U)-\epsilon_0)} \\
&\overset{(c)}{=} 2^{-n(R_2-\epsilon_1)},
\end{aligned}$$

where
(a) is due to the fact that for $u^n \in \mathcal{T}_U^n$, and W^n i.i.d drawn according to $p(w)$, we have

$$2^{-n(I(W;U)+\epsilon_0)} \leq \Pr\{(u^n,W^n) \in \mathcal{T}_{U,W}^n\} \leq 2^{-n(I(W;U)-\epsilon_0)}.$$

That is, $\Pr\{(u^n,W^n) \notin \mathcal{T}_{U,W}^n\} \geq 1 - 2^{-n(I(W;U)-\epsilon_0)}$.
(b) is due to the inequality $(1-y)^n \geq 1-ny$ for $0 < y < 1$.
(c) is by the fact that $R_0 + R_2 = I(W;U) + \epsilon$ and taking $\epsilon_1 = \epsilon + \epsilon_0$.

Therefore, we have

$$\Pr\{K=k|E=1\} = \sum_{u^n \in \mathcal{T}_U^n} p(u^n) \Pr\{\mathcal{E}_k\} \leq 2^{-n(R_2-\epsilon_1)}. \quad (19)$$

Furthermore,

$$\begin{aligned}
H(K) &\geq H(K|E) \geq \Pr(E=1) H(K|E=1) \\
&\overset{(d)}{\geq} (1-\delta_0) H(K|E=1) \\
&\geq (1-\delta_0) \sum_{k=1}^{2^{nR_2}} \Pr\{K=k|E=1\} \log \frac{1}{\Pr\{K=k|E=1\}} \\
&\overset{(e)}{\geq} (1-\delta_0)(1-\delta_1) \min_k \log \frac{1}{\Pr\{K=k|E=1\}} \\
&\overset{(f)}{\geq} (1-\delta_2) \log \frac{1}{\max_k \Pr\{K=k|E=1\}} \\
&\overset{(g)}{\geq} n(1-\delta_2)(R_2-\epsilon_1) \\
&\overset{(h)}{\geq} n(R_2-\epsilon').
\end{aligned}$$

where
(d) is due to the fact that for an arbitrary small $\delta_0 > 0$, $\Pr(E=1) \geq 1-\delta_0$ as n is sufficiently large;
(e) is due to the fact that for an arbitrary small $\delta_1 > 0$,

$\sum_{k=1}^{2^{nR_2}} \Pr\{K=k|E=1\} \geq 1-\delta_1$ as n is sufficiently large. The reason is that by covering lemma [7], the probability that there is no $k \in [1:2^{nR_2}]$ such that $w^n \in \mathcal{C}_k$ which is jointly typical with $u^n \in \mathcal{T}_U^n$, goes to 0 as $n \to \infty$.
(f) is by taking $\delta_2 = \delta_0 + \delta_1$;
(g) is by (19); and
(h) is by taking $\epsilon' = R_2\delta_2 + \epsilon_1$.

Applying a similar proof, one can establish $H(K,S) \geq n(R_0+R_2-\epsilon'')$. ■

Lemma 3: Equivocation on T^n given Z^n, M_1 and M_2 :

$$H(T^n|M_1,M_2,Z^n) \leq n|I(W;U)-I(T;Z)+2\epsilon|^+ + n\delta'.$$

Proof: We prove the bound on $H(T^n|M_1,M_2,Z^n)$ by considering the following two cases:

- Case $I(W;U)+\epsilon < I(T;Z)-\epsilon$:
  Recall (8) and we have in this case $R_3 = n(I(T;Z)-I(W;U)-2\epsilon)$. Thus $R_2+R_0+R_3 = I(T;Z)-\epsilon$ by definition. Note that the channel codebook $\mathcal{C}$ consists of codewords $t^n(m_1,i,s,r)$ with $(m_1,i,s,r) \in [1:2^{nR_1}] \times [1:2^{nR_2}] \times [1:2^{nR_0}] \times [1:2^{nR_3}]$. For each fixed m_1, we take the $2^{n(R_2+R_0+R_3)} = 2^{n(I(T;Z)-\epsilon)}$ codewodes as a sub-codebook $\mathcal{C}(m_1)$. Then we have

  $$H(T^n|M_1,M_2,Z^n) \leq H(T^n|M_1,Z^n) \overset{(a)}{\leq} n\delta', \quad (20)$$

  where (a) is due to the Fano's inequality since the eavesdropper could decode T^n reliably given m_1, z^n, by using jointly typical decoding (i.e., searching for a unique $t^n \in \mathcal{C}(m_1)$ which is jointly typical with z^n).
- Case $I(W;U)+\epsilon \geq I(T;Z)-\epsilon$:
  Recall (8) and we have in this case $R_3 = 0$. That is, the codebook $\mathcal{C}$ consists of codewords $t^n(m_1,i,s)$ with $(m_1,i,s) \in [1:2^{nR_1}] \times [1:2^{nR_2}] \times [1:2^{nR_0}]$ (since $R_3 = 0$ and r thus becomes a constant, we omit r here for simplicity). For each fixed m_1, we take the $2^{n(R_2+R_0)} = 2^{n(I(W;U)+\epsilon)}$ codewords as a sub-codebook $\mathcal{C}(m_1)$.
  Equally partition the codewords in $\mathcal{C}(m_1)$ into $2^{n(I(W;U)-I(T;Z)+2\epsilon)}$ parts such that each part consists of $2^{n(I(T;Z)-\epsilon)}$ codewords. We use P to denote the index of the parts. Clearly P can be considered as a function of (I,S). Given a $p \in [1:2^{n(I(W;U)-I(T;Z)+2\epsilon)}]$, it indicates $2^{n(I(T;Z)-\epsilon)}$ realizations of (I,S).
  Assume that the eavesdropper was given the side information P regarding the possible choices of i,s (further with m_1 to obtain t^n). Then, for each fixed m_1 and p, the corresponding $2^{n(I(T;Z)-\epsilon)}$ codewords could be taken as a sub-codebook $\mathcal{C}(m_1,p)$. Therefore,

  $$\begin{aligned} H(T^n|M_1,M_2,Z^n) &\overset{(b)}{=} H(I,S|M_1,M_2,Z^n) \\ &\overset{(c)}{=} H(I,S,P|M_1,M_2,Z^n) \\ &\overset{(d)}{\leq} H(P) + H(I,S|M_1,P,M_2,Z^n) \\ &\overset{(e)}{\leq} n(I(W;U)-I(T;Z)+2\epsilon) + H(T^n|M_1,P,Z^n) \\ &\overset{(f)}{\leq} n(I(W;U)-I(T;Z)+2\epsilon) + n\delta', \end{aligned} \quad (21)$$

  where
  (b) is due to the one-to-one mapping between T^n and M_1,I,S in this case;
  (c) is due to the fact that P is a function of I,S;
  (d) is since $H(P|M_1,M_2,Z^n) \leq H(P)$;
  (e) is due to the fact that $H(I,S|M_1,P,M_2,Z^n) = H(T^n|M_1,P,M_2,Z^n) \leq H(T^n|M_1,P,Z^n)$;
  (f) is due to the fact that the eavesdropper could decode T^n reliably given m_1,p,z^n, by using jointly typical decoding (i.e., searching for a unique $t^n \in \mathcal{C}(m_1,p)$ which is jointly typical with z^n).

Summarizing (20) and (21), we conclude the proof. ■

VI. conclusion

In this paper, we address the problem of secure communication over a wiretap channel with correlated source in presence of an eavesdropper. We focus on the secret-message problem under the assumptions that 1) the eavesdropper has no source observation; 2) the channel is independent of the correlated sources.

The purpose of this work is to gain insight into the code design strategies that could fully exploit the advantages of both channel and sources. We provide a direct coding scheme by incorporating the classical methods of 1) *Wyner-Ziv source coding*, which takes advantage of corrected sources to generate secret key shared by the transmitter and the legitimate receiver, but imposes a certain cost on the channel transmission; 2) *one-time pad* to secure message in an economic manner; and 3) *Wyner's secrecy coding* which takes advantage of the legitimate receiver's channel over the eavesdropper's (additional randomness on the cost of the channel is needed to confuse the eavesdropper). Information theoretic secrecy is achieved in a manner of crypto-coding.

References

[1] C. E. Shannon, "Communication Theory of Secrecy Systems," *Bell Systems Technical Journal*, vol. 28, pp. 656–715, 1949.
[2] A. D. Wyner, "The wire-tap channel," *Bell Systems Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Jan. 1975.
[3] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Transactions on Information Theory*, vol. 24, no. 3, pp. 339–348, May 1978.
[4] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733–742, 1993.
[5] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography. i. secret sharing," *IEEE Transactions on Information Theory*, vol. 39, no. 4, pp. 1121–1132, 1993.
[6] V. M. Prabhakaran, K. Eswaran, and K. Ramchandran, "Secrecy via sources and channels," *IEEE Transactions on Information Theory*, vol. 58, no. 11, pp. 6747–6765, 2012.
[7] A. E. Gamal and Y.-H. Kim, *Network Information Theory*. New York, NY, USA: Cambridge University Press, 2012.
[8] Y.-K. Chia and A. El Gamal, "Wiretap channel with causal state information," *IEEE Transactions on Information Theory*, vol. 58, no. 5, pp. 2838–2849, 2012.