

SECRET SHARING IN FAST FADING CHANNELS BASED ON RELIABILITY-BASED HYBRID ARQ

Chan Wong Wong, John M. Shea, and Tan F. Wong
Wireless Information Networking Group (WING)
Department of Electrical and Computer Engineering
University of Florida, Gainesville, FL 32611

{cwwong@ufl.edu, jshea@ece.ufl.edu, twong@ece.ufl.edu}

Abstract

Consider a wireless transmission from Alice to Bob in the presence of an eavesdropper, Eve. We propose a technique to allow Alice to send a message such that Bob can decode it but Eve can get little information about the message. This scenario is a classic example of the wiretap channel, for which several researchers have begun to develop practical schemes. However, we consider a challenging version in which the channel from Alice to Eve may be as good or better than the channel from Alice to Bob. There have been no practical secrecy coding techniques that have been developed for this scenario. The key to allow secret communication in such a scenario is feedback from Bob to Alice (which Eve can also observe). The scheme we develop uses reliability-based hybrid automatic-repeat-request (RB-HARQ) over a fast fading channel to provide a decoding advantage at Bob. Bob requests information about received symbols that suffer from deep fades. The retransmitted symbols improve Bob's ability to decode the message faster than at Eve, who sees retransmission of bits with random reliabilities. We evaluate the proposed scheme by performance measures such as the probability of successful decoding and the equivocation rate at Eve.

I. INTRODUCTION

Privacy and security are important considerations in the design of wireless communication systems. One aspect of security is to provide secure communication among trusted users. For instance, in a wireless network, a user (Alice) may want to transmit a message to a trusted receiver (Bob) across a public channel¹ in such a way that it is impossible for an adversary (Eve) to retrieve any useful information about the message. This

This work was supported by the National Science Foundation under grant number CNS-0626863 and by the Air Force Office of Scientific Research under grant number FA9550-07-10456.

¹The public channel is not encrypted, but it must be authenticated. Such authentication can be made unconditionally secure provided Alice and Bob share a short initial unconditionally secure secret key.

is the notion of *perfect secrecy*, which was first defined in an information-theoretic sense by Shannon [1]. Wyner [2] introduced the wiretap channel in which the Alice-to-Eve channel is a degraded version of the Alice-to-Bob channel. Wyner defined the secrecy rate as the maximum rate at which information can be sent from Alice to Bob while keeping the equivocation rate of Eve about Alice's messages the same as the information rate from Alice to Bob. For the wiretap channel, Wyner showed that positive secrecy rate from Alice to Bob is possible. Csiszár and Körner [3] extended Wyner's result to the more general situation in which the Alice-to-Bob channel is more capable than the Alice-to-Eve channel. In Wyner's original paper, he described a code design based on group codes for the wiretap channel. In [4], a code design based on coset codes was suggested for the special case in which the Alice-to-Bob channel is error-free. More practical designs were also proposed for the same type of wiretap channels based on low density parity check (LDPC) codes [5] and nested codes [6].

In practical wireless communication scenarios, the condition that the Alice-to-Bob channel is more capable than the Alice-to-Eve channel cannot be guaranteed. Maurer [7] first demonstrated that the availability of a public feedback channel from Bob to Alice could make secure communications possible even if the Alice-to-Bob channel is less capable than the Alice-to-Eve channel. Ahlswede and Csiszár [8] elegantly introduced the concept of secret sharing based on *common randomness* between Alice and Bob via a public channel between them. Bennett *et al.* [9] suggested a four-step process of achieving secret sharing over a wiretap channel with an additional public channel between Alice and Bob. The four steps are advantage distillation, information reconciliation, privacy amplification, and secret communication, in that order.

Common randomness can be provided in practical scenarios by noise and channel fading in a wireless

communication system. Most previous work has focused on the reconciliation protocols for systems in which the Alice-to-Eve channel is more noisy than the Alice-to-Bob channel (cf. [10], [11], [12] and references). We consider forward reconciliation, in which the goal is to make Bob have the same information as Alice, while limiting the amount of information disclosed to Eve. (In reverse reconciliation, the goal is to make Alice know what Bob received.) Previous works focus on reconciliation of the binary information, which limits their ability to identify which information is likely to be incorrect. They use reconciliation strategies based either on interactive error-correction coding [10] or Slepian-Wolf coding [11], [12] to correct errors introduced by the Alice-to-Bob channel.

For communication over fading channels, the magnitude of the demodulator output indicates the reliability of that symbol. Since the fading processes at geographically separated receivers will generally be independent, fading can thus act as a source of common randomness and can be directly utilized to aid in reconciliation. The use of fading to provide common randomness has been previously proposed in the opportunistic transmission protocol of [12], in which Alice only transmits when the fading conditions assure a positive secrecy capacity from Alice to Bob. However, this scheme requires that Alice know the channel conditions to both Bob and Eve, which is not very practical.

In this paper, we show how reliability-based hybrid automatic-repeat-request (RB-HARQ) can be used in the advantage distillation and information reconciliation steps of [9]. We design a protocol in which Bob uses a (public) feedback channel to request additional information from Alice to allow him to decode a message from Alice, while keeping the information learned by Eve as ambiguous as possible². We assume independent fast fading on the Alice-to-Bob and Alice-to-Eve channels. The basic idea of our approach is for Alice to send a coded message at a power level that is so low that neither Bob nor Eve can correctly decode the message after the original transmission. Bob takes advantage of the presence of the feedback channel to increase his ability to decode the message at a faster rate than Eve.

II. CHANNEL MODEL AND KEY CAPACITY

Consider the fast fading wiretap channel depicted in Fig. 1, in which Eve tries to recover messages sent

²Although it is not generally possible to completely secure the data at its transmitted rate, *privacy amplification* techniques can be used to provide completely secure information at a lower rate.

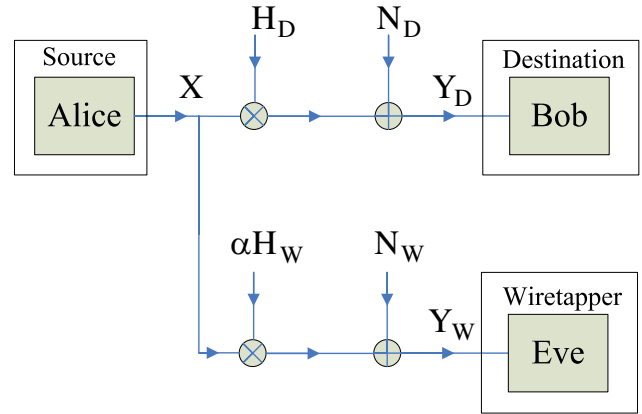


Fig. 1. The fast fading wiretap channel.

from Alice to Bob. Assume that Alice sends the symbol X with average power P , i.e., $E[X^2] = P$. For the coding schemes and their performance evaluation discussed in Sections III and IV, it is assumed that $X \in \{+\sqrt{P}, -\sqrt{P}\}$ corresponding to the use of binary phase-shift keying (BPSK). Bob and Eve observe the output of two independent fast Rayleigh fading channels given, respectively, by

$$\begin{aligned} Y_D &= H_D X + N_D \\ Y_W &= \alpha H_W X + N_W, \end{aligned} \quad (1)$$

where H_D and H_W are Rayleigh distributed random variables with unit variance, N_D and N_W are zero-mean Gaussian random variables with variance σ^2 , and α is a real positive constant. We assume that H_D , H_W , N_D , and N_W are all independent among themselves and over time. Although not shown in Fig. 1, we also assume that there is an error-free, unlimited-rate feedback channel from Bob to Alice. The average received signal-to-noise ratios (SNRs) at Bob and Eve are P/σ^2 and $\alpha^2 P/\sigma^2$, respectively. Hence the parameter α^2 can be interpreted as the SNR advantage of Eve over Bob. In addition, we assume that Bob and Eve have perfect causal channel state information (CSI) of their respective channels. That is, Bob and Eve respectively know the fading gains H_D and H_W up to the present moment. Because of the causality of CSI, Alice's transmit symbol X must be independent of H_D , H_W , N_D , and N_W .

The key capacity C_s [8] is the maximum possible rate at which secret information can be shared between Alice and Bob such that Eve is kept totally ignorant; i.e., the rate of the information that Eve can extract from her observation of the Alice-to-Eve and public channels is negligibly small. For the channel model considered in

(1), the results in [8] can be extended to give

$$C_s = \frac{1}{2} E \left[\log_2 \left(1 + \frac{H_D^2 P / \sigma^2}{1 + \alpha^2 H_W^2 P / \sigma^2} \right) \right], \quad (2)$$

where C_s is in the unit of bits per channel use (bpcu).

III. RELIABILITY-BASED HYBRID ARQ PROTOCOL

In this section, we describe a practical coding protocol that combines advantage distillation and information reconciliation for the fast fading wiretap channel. In our secrecy coding scheme, the message is coded and transmitted at a power level that is too low for correct decoding. Then Bob and Alice use RB-HARQ [13] to allow Bob to increase his ability to decode the message faster than Eve. RB-HARQ is an incremental ARQ scheme that utilizes reliability estimates generated either by the demodulator or soft-input soft-output (SISO) decoder to determine the incremental retransmission information. In RB-HARQ, symbols that are deemed to be unreliable at the destination are requested to be retransmitted. The retransmitted symbols improve the ability of the destination to decode the message.

The proposed joint advantage distillation and information reconciliation scheme is based on the aforementioned property of RB-HARQ. Consider the flow chart in Fig. 2. For the time being, assume that a standard rate-1/3 turbo code obtained from the parallel concatenation of two recursive systematic convolutional (RSC) encoders is employed. Alice transmits a turbo-encoded message through the fading channel to Bob. Eve observes the transmission through her own independent fading channel. Bob tries to decode the message and uses the embedded cyclic-redundancy-check (CRC) code to check for correct decoding of the message. We note that the use of CRC may be avoided by deciding on correct decoding when the minimum reliability of the information bits exceeds a threshold.

If decoding is unsuccessful, Bob ranks the received symbols at the output of demodulator according to absolute values of their channel log-likelihood ratios (LLRs). The symbols with the smallest absolute LLR values are considered unreliable, and the symbols with the largest LLR values are considered more reliable. Bob then determines the K least reliable symbols and asks Alice to retransmit those symbols. The retransmission request is made through the public feedback channel. The public feedback channel is required to be an authenticated reverse channel and authentication can be done using conventional cryptography. In other words, all the information sent over the public feedback channel

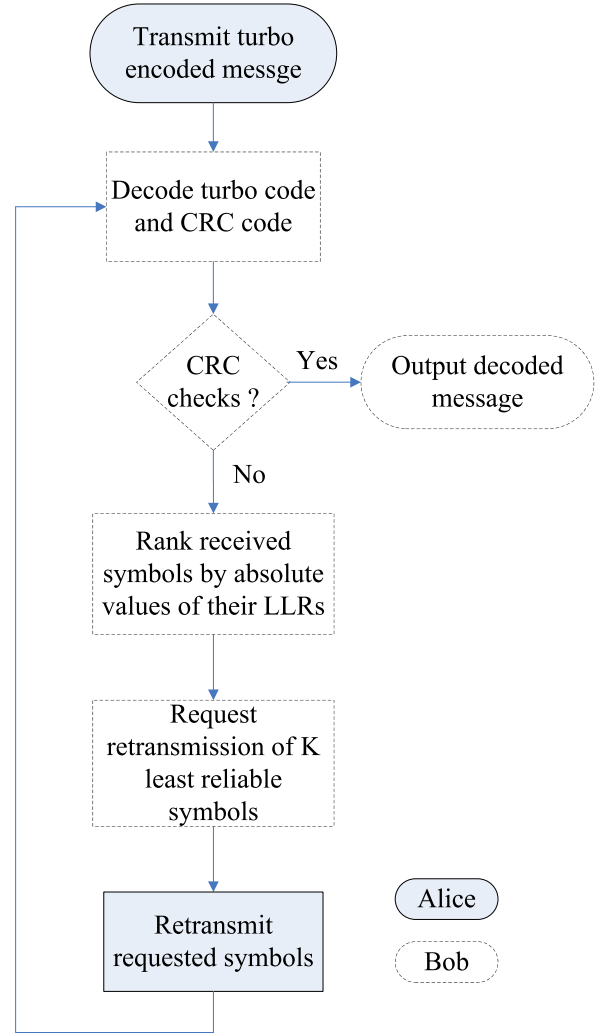


Fig. 2. Flow Chart of the proposed RB-HARQ coding protocol for advantage distillation and information reconciliation.

is received by Eve, but she cannot corrupt or introduce fake information. Hence Eve knows exactly which set of symbols Alice is going to retransmit. However, this set of additional symbols would not provide as much decoding benefit for her as they would for Bob, since the reliability of these symbols in the original transmission may not be low as seen by Eve. On the other hand, the retransmitted symbols can significantly improve Bob's decoding performance, as they correspond to the least reliable ones in the original transmission as seen by Bob.

After the first retransmission by Alice, Bob adds the LLR of each of the K newly received symbols to that of the corresponding symbol for further decoding. If Bob still cannot correctly decode the message, Bob ranks the received symbols according to the updated LLRs

and asks Alice for another retransmission. The set of requested symbols is likely to be different from the set at the first retransmission. Bob continues the RB-HARQ process until he can successfully decode the message.

In summary, we use RB-HARQ to retransmit the unreliable symbols, which contribute most to decoding failure at Bob, thus quickly improving his ability to decode the message. Although Eve still benefits through these retransmissions, the contribution to Eve's decoding is much less significant than to Bob's. This is due to the independence of the fading processes of the Alice-to-Bob and Alice-to-Eve channels. RB-HARQ serves as the coding protocol that helps to exploit the common randomness shared by Alice and Bob through the fading process of the Alice-to-Bob channel.

One possible way to enhance the advantage distillation performance of the RB-HARQ coding protocol is by puncturing the original rate-1/3 turbo code. Traditionally, puncturing is achieved by removing some of the parity symbols. However, we observe that weakening the code by traditional puncturing has the same effect on both decoders of Bob and Eve. As a result, there is no gain in the advantage distillation performance. The challenge is to design a puncturing scheme such that Bob can overcome the loss of decoding performance due to puncturing through RB-HARQ faster than Eve can. Toward this end, we employ non-systematic turbo codes (NSTCs) (cf. [14]), in which all the systematic bits of the turbo code are punctured.

IV. PERFORMANCE EVALUATION

In this section, we present simulation results to evaluate the performance of the proposed RB-HARQ based protocol for advantage distillation and information reconciliation. We assume the system model described in Section II with the following simulation setting:

- The basic turbo code comprises two 8-state RSC encoders with the same generator polynomial (13, 15). Random interleaving is applied to the data bits before they are encoded by one of the RSC encoders.
- We consider the use of the following three turbo codes:
 - TC1: The rate-1/3 basic turbo code.
 - TC2: The rate-1/2 NSTC obtained by puncturing all the systematic bits in the basic turbo code.
 - TC3: The rate-3/5 NSTC obtained by puncturing all the systematic bits and some parity bits of one of the component RSC codes in the basic turbo code.

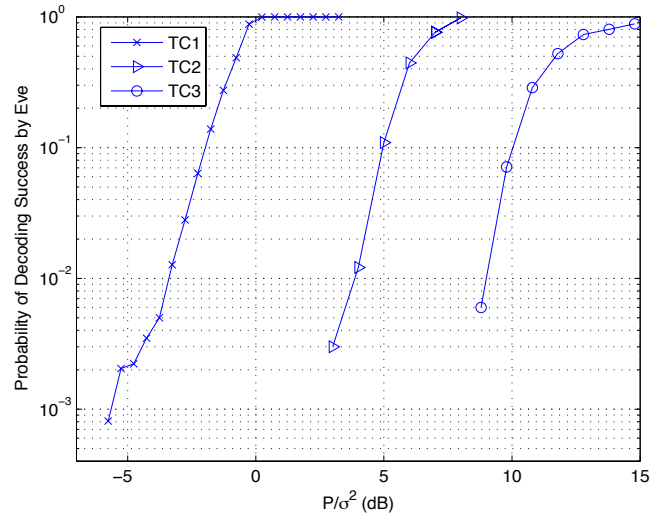


Fig. 3. Probability of successful decoding by Eve when $\alpha^2 = 0$ dB.

- Bob performs turbo decoding.
- Eve knows the exact coding scheme and the retransmission protocol. Since the complexity of a true maximum likelihood (ML) decoder for turbo code is exorbitant and no practical decoder that provides performance between the ML and turbo decoder has been published in the literature, we assume that Eve uses the same turbo decoder as Bob. However, in order to address the complexity issue, we also provide results in which Eve tries all possible values for 10, 20, or 30 of the least reliable bits and performs parallel turbo decoding; this is equivalent to allowing the complexity at Eve to be approximately 10^3 , 10^6 or 10^9 times that at Bob, respectively.
- The block size N of the turbo code is 1000, and Bob and Eve employ 10 decoding iterations after each transmission.
- For each retransmission, Bob requests the retransmission of the $K = 60$ least reliable symbols.

A. Probability of successful decoding by Eve

The first performance measure of interest is the probability that Eve can successfully decode the message by the time the RB-HARQ process ends. Let this probability be denoted by P_c . Figs. 3 and 4 show plots of P_c versus Bob's average SNR P/σ^2 for the three turbo codes when $\alpha^2 = 0$ dB and 3 dB, respectively. When Eve has the same average SNR as Bob (i.e., $\alpha^2 = 0$ dB), Bob can decode but Eve has minimal probability of successfully decoding the message provided the SNR is low enough,

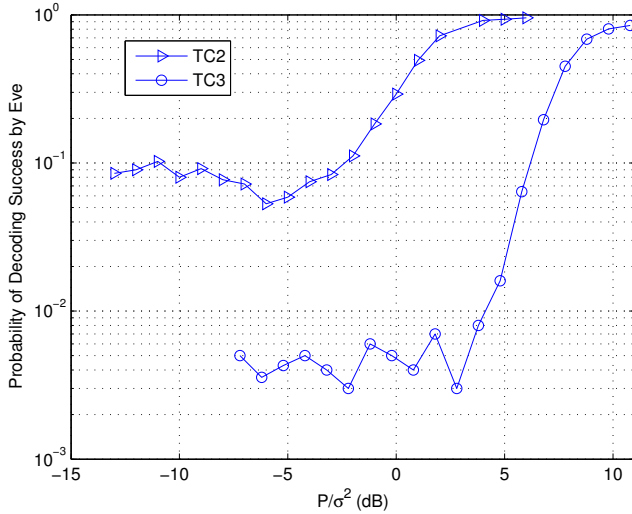


Fig. 4. Probability of successful decoding by Eve when $\alpha^2 = 3$ dB.

for all three turbo codes considered. When the Alice-to-Eve channel is more capable (i.e., $\alpha^2 = 3$ dB), leveling of P_c is observed when the SNR drops below some thresholds for both TC2 and TC3. With TC1, Eve can always decode the message correctly over the range of SNR shown in Fig. 4. Thus, TC1 is not suitable for use in this case.

The results above show that the RB-HARQ scheme with properly designed codes can effectively prevent Eve from decoding the message correctly. Nonetheless, the observed P_c -leveling behavior is undesirable. More effort is needed to design codes that do not have this behavior. In addition, we note that P_c is not a sufficient measure of the performance of advantage distillation, as Eve may still be able to learn much about the message even if she cannot successfully decode it.

B. Complexity-constrained equivocation rate

When the conditional entropy of the message given all observations that Eve can make over her channel and the public feedback channel, is the same as the entropy of the message, *perfect secrecy* is achieved [1]. A weaker, but more convenient, notion of secrecy is employed in [2], [3], [8], where the best objective of secrecy transmission is to have Eve's equivocation rate R_E to be as large as the information rate R_I from Alice to Bob. R_E is defined as

$$R_E = H(X|Y_W, H_W)R_I, \quad (3)$$

where $H(X|Y_W, H_W)$ is the conditional entropy of the message at Eve.

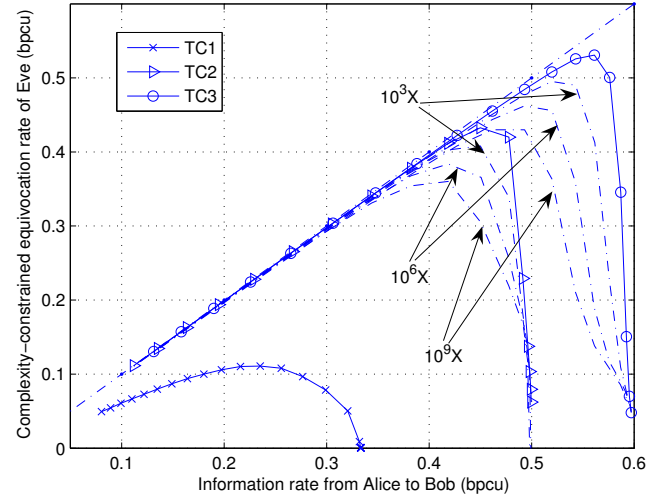


Fig. 5. Complexity-constrained equivocation rate of Eve versus information rate from Alice to Bob when $\alpha^2 = 0$ dB.

For the case of RB-HARQ, the information rate R_I from Alice to Bob is the effective code rate of RB-HARQ, which is defined as the ratio of the number of data bits to the number of total transmitted (including the first transmission and all subsequent retransmissions) symbols. Note that we do not count the time when the channel is not used by Alice while she waits for Bob's retransmission requests. Eve's equivocation rate about the message is, on the other hand, very difficult to calculate because of the complexity of the RB-HARQ process with turbo decoding. Instead we employ the *a posteriori* probabilities of the data bits generated by Eve's decoder to estimate the conditional entropy $H(X|Y_W, H_W)$ and hence the equivocation rate R_E using (3). In order to do so, we adopt the approximation that the *a posteriori* distributions of the data bits are independent. This approximation is quite accurate with the use of random interleaving and large block size.

We refer to this equivocation rate estimated from the outputs of Eve's turbo decoder as the *complexity-constrained equivocation rate*. This is because it quantifies the amount of ambiguity left about the message after decoding what Eve observes, under the assumption that Eve can only use a decoder that is no more complex than (or a multiple of the complexity of) the one used by Bob. Obviously the complexity-constrained equivocation rate overestimates the true equivocation rate. Nevertheless, it still provides a reasonable measure on the advantage distillation performance of the proposed secrecy coding scheme.

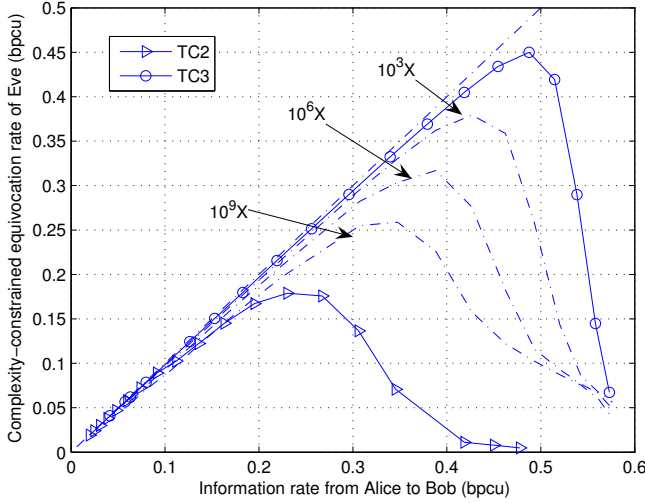


Fig. 6. Complexity-constrained equivocation rate of Eve versus information rate from Alice to Bob when $\alpha^2 = 3$ dB.

Figs. 5 and 6 show Eve's complexity-constrained equivocation rate versus information rate from Alice to Bob for the cases of $\alpha^2 = 0$ dB and 3 dB, respectively. To aid in interpreting the results, each figure includes a broken line that shows the maximum possible equivocation rate (which equals the information rate from Alice to Bob). For the case of $\alpha^2 = 0$ dB, TC2 and TC3 give equivocation rates close to the bound until the latter reaches 0.42 and 0.52 bpcu, respectively. On the other hand, the equivocation rate is never close to the bound with the use of TC1. This may be attributed to the direct leakage of information through the systematic bits that are transmitted in TC1. For TC2 and TC3, Fig. 5 also the equivocation rates achieved when Eve uses the previously-described reference decoders, which have complexity 10^3 , 10^6 or 10^9 times that of Bob's decoder. As expected, as the complexity of Eve's decoder increases, the information rate at which the equivocation rates turn away from the bound decreases. For example, for the decoder with 10^9 times complexity advantage, TC2 and TC3 give equivocation rates close to information rates only when the latter is less than 0.32 and 0.38 bpcu, respectively. For the case of $\alpha^2 = 3$ dB, similar observations can be made except that only TC3 provides good secrecy performance. TC2 does not give equivocation rates close to the bound except for low information rates. TC1 always gives small equivocation rates as expected since Eve can decode the message, as discussed before. The results imply that puncturing of the systematic and parity bits not only makes decoding

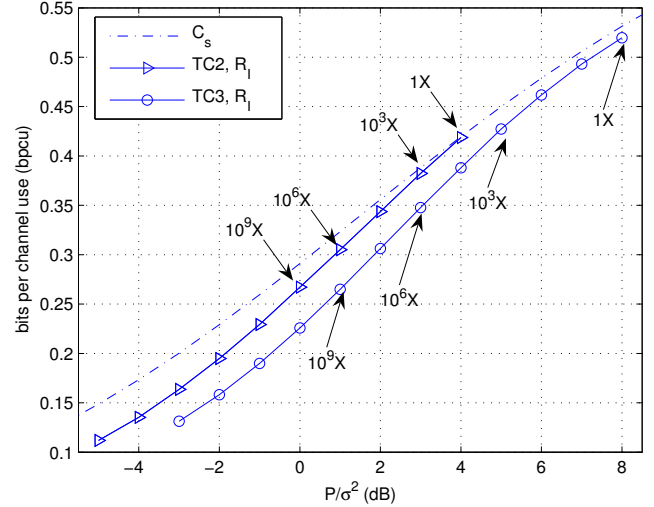


Fig. 7. Comparison of secret information rate achieved by RB-HARQ and key capacity when $\alpha^2 = 0$ dB.

more difficult for Eve, but also increases Eve's ambiguity about the message after decoding.

C. Comparison to key capacity

It is also illustrative to compare the amount of secret information sent by Alice to Bob through the proposed RB-HARQ protocol to the key capacity C_s introduced in Section II. For this comparison, we consider the RB-HARQ protocol operates only at the range of SNR over which the Eve's complexity-constrained equivocation rate is at least 98% of the information rate from Alice to Bob. This is to make sure that the information transferred from Alice to Bob is at a reasonable secrecy level.

Figs. 7 and 8. show the secret information rate from Alice to Bob achieved by RB-HARQ when $\alpha^2 = 0$ dB and 3 dB, respectively. The key capacity C_s is calculated by (2). Note that we only plot the points at which Eve's equivocation rate is at least 98% of the information rate. For the case of $\alpha^2 = 0$ dB, TC2 can give secret information rates close to the key capacity values until the key capacity reaches 0.42 bpcu. Beyond this rate, the 98% equivocation-rate-to-information-rate secrecy performance requirement is not met. TC3 gives poorer performance in terms of the information rate at about 1 to 3 dB away from the key capacity. However, the secrecy performance requirement is not violated until the information rate reaches 0.52 bpcu. As expected TC1 never satisfies the secrecy performance requirement. For three reference decoders, the rates at which the equivocation-rate-to-information-rate ratio is

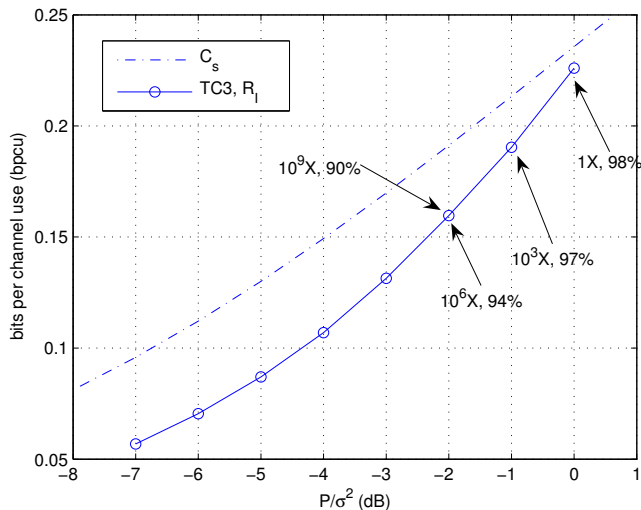


Fig. 8. Comparison of secret information rate achieved by RB-HARQ and key capacity when $\alpha^2 = 3$ dB.

at least 98% are also pointed out in Fig. 7. For example, the 98% equivocation-rate-to-information-rate secrecy performance requirement is met if the information rates is lower than 0.27 bpcu for the $10^9 X$ decoder.

For the case of $\alpha^2 = 3$ dB, only TC3 can satisfy the secrecy performance requirement, and it does so only when the information rate is lower than 0.22 bpcu. Also, the 98% equivocation-rate-to-information-rate secrecy performance requirement is not met for the three reference decoders. However, as indicated in Fig. 8, a 97%, 94% and 90% equivocation-rate-to-information-rate ratio is guaranteed when the information rate is lower than 0.19, 0.16 and 0.16 bpcu respectively. In summary, as the SNR advantage of Eve increases, the design of secret sharing coding schemes becomes much more difficult.

V. CONCLUSION

We have developed a practical secrecy-sharing scheme that achieves advantage distillation and information reconciliation through error-control coding and reliability-based hybrid ARQ. In our design, Alice (source) transmits the information to Bob (destination) over a fast fading channel at an SNR that is lower than the required level for correct decoding. RB-HARQ is used to retransmit the symbols that experience deep fades over the Alice-to-Bob channel. We demonstrate that with properly designed codes, Bob can quickly improve his decoding ability through RB-HARQ, while Eve (the adversary) gets little benefits out of the retransmissions. With the

restriction that Eve cannot use a more complex decoder than Bob's, we show that the RB-HARQ scheme can achieve information rate that is close to the key capacity while keeping Eve's equivocation rate at 98% of the information rate. When Eve has a decoder that is 10^3 to 10^9 times more complex than Bob's, performance close to the key capacity is still obtained for a wide range of SNRs, although at an equivocation rate that is somewhat smaller (90% of the information rate for 10^9 complexity). Our results show that the RB-HARQ design is a promising candidate for secret sharing between two trusted terminals. Nevertheless, more effort is still needed to design codes that can give better secret sharing performance, in particular when Eve has a significant SNR advantage over Bob.

REFERENCES

- [1] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, pp. 656–715, Oct. 1949.
- [2] A. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, pp. 1355–1387, Oct. 1975.
- [3] I. Csiszar and J. Korner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.
- [4] L. Ozarow and A. D. Wyner, "Wire-tap channel II," *Bell Syst. Tech. J.*, vol. 63, no. 10, pp. 2135–2157, Dec. 1984.
- [5] A. Thangaraj, S. Dihidar, A. R. Calderbank, S. McLaughlin, and J.-M. Merolla, "Applications of LDPC codes to the wiretap channel," Nov. 2004. [Online]. Available: arXiv:cs/0411003
- [6] R. Liu, Y. Liang, H. Poor, and P. Spasojevic, "Secure nested codes for type II wiretap channels," *Proc. IEEE 2007 Inform. Theory Workshop*, pp. 337–342, Sept. 2007.
- [7] U. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inform. Theory*, vol. 39, no. 3, pp. 733–742, May 1993.
- [8] R. Ahlswede and I. Csiszar, "Common randomness in information theory and cryptography - Part I: Secret sharing," *IEEE Trans. Inform. Theory*, vol. 39, no. 4, pp. 1121–1132, Jul. 1993.
- [9] C. Bennett, G. Brassard, C. Crepeau, and U. Maurer, "Generalized privacy amplification," *IEEE Trans. Inform. Theory*, vol. 41, no. 6, pp. 1915–1923, Nov. 1995.
- [10] G. Brassard and L. Salvail, "Secret-key reconciliation by public discussion," *Advances in Cryptology - Eurocrypt'93*, pp. 410–423, 1994.
- [11] K.-C. Nguyen, G. Van Assche, and N. J. Cerf, "Side-information coding with turbo codes and its application to quantum key distribution," in *Proc. 2004 IEEE Int. Symp. Inform. Theory and Applicat.*, Param, Italy, Oct. 2004.
- [12] M. Bloch, J. Barros, M. Rodrigues, and S. McLaughlin, "Wireless information theoretic security - Part II: Practical implementation," Nov. 2006. [Online]. Available: http://arxiv.org/PS.cache/cs/pdf/0611/0611121v1.pdf
- [13] J. M. Shea, "Reliability-based hybrid ARQ," *IEE Electronics Letters*, vol. 38, no. 13, pp. 644–645, June 2002.
- [14] A. Banerjee, F. Vatta, B. Scanavino, and D. J. Costello, Jr., "Nonsystematic turbo codes," *IEEE Trans. Commun.*, vol. 53, no. 11, pp. 1841–1849, Nov. 2005.