Mathematical Problems of Computer Science 35, 70–76, 2011.

The Shannon Cipher System With a Guessing Wiretapper Eavesdroping Through a Noisy Channel

Evgueni A. Haroutunian and Tigran M. Margaryan

Institute for Informatics and Automation Problems of NAS of RA
e-mail: eghishe@sci.am

Abstract

In this paper we study the processes in the Shannon cipher system with discrete memoryless source and a guessing wiretapper. The wiretapper observes a cryptogram of M-vector ciphered messages passed through the noisy channel and tries to guess the secret plaintext with length N. The security of encryption system is measured by the average number of guesses needed for the wiretapper to uncover the plaintext. The problem was suggested by Arikan and Merhav as a generalization of their result for noiseless channel to wairtapper.

References

[1] E. Arikan, "An inequality on guessing and its application to sequential decoding", *IEEE Trans. Inform. Theory*, vol. 42, no. 1, pp. 99-105, 1996.

[2] E. Arikan a "On the Average Nuber of Guesses Required to Determine the Value of a Random variable", *Transactions of the 12th Prague Conference on Information Theory, Statistical Decision Function and Random Processes*, pp. 20-23, 1994.

[3] E. Arikan and N. Merhav, "Guessing subject to distortion", *IEEE Trans. Inform. Theory*, vol. 44, no. 3, pp. 1041-1056, 1998.

[4] E. Arikan and N. Merhav,"Joint source-channel coding and guessing with application to sequential decoding", *IEEE Trans. Inform. Theory*, vol. 44, no. 5, pp. 1756-1769, 1998.

[5] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, New York: Academic, 1981.

[6] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, New York: Wiley, 2006.

[7] E. A. Haroutunian and A. R. Ghazaryan, "On cipher system with a wiretapper guessing with respect to fidelity and reliability criteria", *Proceedings of the Third Conference on Computer Science and Information Technologies* (Yerevan, Armenia, 2001), pp. 215-219.

[8] E. A. Haroutunian and A. R. Ghazaryan, "On the Shannon cipher system with a wiretapper guessing subject to distortion and reliability requirements", *Proceedings of the 2002 IEEE Int. Symp. Inform. Theory* (Lausanna, Switzerland), p. 324.

[9] E. A. Haroutunian, “Realibility approach in wiretapper guessing theory”, in “Aspects of Network and Information Security”, NATO Science for Peace and Security, series D: Information and Communication Security, vol. 17, pp. 248–260, IOS Press, 2008.

[10] Y. Hayashi and H. Yamamoto, “Coding theorems for the Shannon cipher with a guessing wiretapper and correlated source outputs”, *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2808-2817, June 2008.

[11] M. E. Hellman, “An extention of the Shannon theory approach to cryptography”, *IEEE Trans. on Inform. Theory*, vol. 23, no. 3, pp. 289-299, 1977.

[12] D. Malone and W. G. Sullivan, “Guesswork and entropy”, *IEEE Trans. Inform. Theory*, vol. 50, no. 3, pp. 525-526, 2004.

[13] J. L. Massey, ”Guessing and entropy”, *Proceedings of the 1994 IEEE International Symp. Inform. Theory* (Trondheim, Norway, 1994), p. 204.

[14] N. Merhav and E. Arikan, ”The Shannon cipher system with a guessing wiretapper”, *IEEE Trans. Inform. Theory*, vol. 45, no. 6, pp. 1860-1866, 1999.

[15] A. Sgarro, ”Error Probabilities for Simple Substitution Ciphers”, *IEEE Trans. Inform. Theory*, vol. 29, no. 2, pp. 190-197, 1983.

[16] A. Sgarro, “Exponential-type parameters and Substitution Ciphers”, *Problems of Control and Inform. Theory*, vol. 14(5), pp. 393-403, 1985.

Շենոնյան ծածկագրման համակարգում գաղտնագողի գուշակումը աղմկոտ կապուղով

Ե. Հարությունյան և Տ. Մարգարյան

Ամփոփում

Հոդվածում լուծված է Մերհավի և Արիկանի կողմից առաջադրված խնդիրը: Դիտարկված է հատնյալ համակարգը. ծանիչը բանալու օգնությամբ ծածկագրում է հաղորդագրությունը և անաղմուկ կապուղով ուղարկում է օրինական հասեատիրոջը, որին ուղարկում է նաև բանալին մեկ այլ անաղմուկ, պաշտպանված կապուղով: Գաղտնագողը, օգտվելով աղմկոտ կապուղուց, ստանալով ծածկագիրը, ձգտում է վերծանել հաղորդագրությունը հաջորդական գուշակումների միջոցով:

Հոդվածում ստացված է կռահման արագության գնահատականները: