Mathematical Problems of Computer Science 37, 17–24, 2012.

On the Shannon Cipher System with Correlated Source Outputs and Guessing Wiretapper Eavesdroping through a Noisy Channel

Tigran Margaryan

Institute for Informatics and Automation Problems of NAS of RA
e-mail: martigranm@gmail.com

Abstract

In this paper the Shannon cipher system with discrete memoryless correlated sources is considered. The wiretapper gains the noisy version of the cryptogram through the memoryless noisy channel and tries to guess the secret information which is related to the encrypted plaintext. The security level of the encryption system is measured by the expected number of wiretapper's guesses. The upper and lower bounds are obtained for the guessing rate.

References

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

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

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

[5] 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.

[6] 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.

[7] E. Arikan, "Guessing and cryptology", in "Aspects of Network and Information Security", NATO Science for Peace and Security, series D: Information and Communication Security, IOS Press, vol. 17, pp. 211–217, 2008

[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, IOS Press, vol. 17, pp. 248–260, 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] D. Malone and W. G. Sullivan, "Guesswork and entropy", *IEEE Trans. Inform. Theory*, vol. 50, no. 3, pp. 525-526, 2004.

[12] E. A. Haroutunian and T. M. Margaryan, "The Shannon cipher system with a guessing wiretapper eavesdroping through a noisy channel", *Transactions of IIAP of NAS of RA , Mathematical Problems of Computer Science*, vol. 35, pp. 70-76, 2011.

[13] E. A. Haroutunian and T. M. Margaryan, "Wiretapper guessing by noisy channel for the Shannon cipher system with correlated source outputs", *Proceedings of International Conference CSIT 2011*, pp. 125–128, Yerevan 2011.

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

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

Գուշակող գաղտնագողի առկայությամբ աղմկոտ կապուղով և աղբյուրի հարաբերակցված հաղորդագրություններով Շենոնյան ծածկագրման համակարգի մասին

Տ. Մարգարյան

Ամփոփում

Հոդվածում դիտարկվել է ընդհատ, առանց հիշողության հարաբերակցված աղբյուրներով Շենոնյան ծածկագրման համակարգը: Գաղտնագողը ստանում է գաղտնագրի աղավաղված տարբերակը և ձգտում գուշակել գաղտնի տեղեկությունը, որը կապված է ծածկագրված այլ հաղորդագրության հետ: Ծածկագրման համակարգի գաղտնիության աստիճանը չափվում է գաղտնագողի գուշակումների քնակաի սպասելիով: Ստացվել են վերին և ստորին գնահատականներ կոռհման արագության համար:

О шенноновской секретной системе с коррелированными сообщениями источника и угадывающим нарушителем подслушивающим через канал с шумом

Т. Маргарян

Аннотация

В статье рассматривается шенноновская секретная система с дискретными источниками без памети. Нарушитель получает зашумленную версию криптограммы через канал без памяти и стремится угадать

секретную информацию, связанную с зашифрованым сообщением. Уровень секретности криптографической системы измеряется средним числом угадываний нарушителя. Получены верхняя и нижняя границы скорости угадывания.