A Generalization of Hellman's Extension of Shannon's Approach to Cryptography

(Abstract)

Pierre Beauchemin
Gilles Brassard

Département d'informatique et de recherche opérationnelle
Université de Montréal
C.P. 6128, Succursale "A"
Montréal, Québec
Canada H3C 3J7

In his landmark 1977 paper [Hell77], Hellman extends the Shannon theory approach to cryptography [Shan49]. In particular, he shows that the expected number of spurious key decipherements on length n messages is at least $2^{H(K)-nD} - 1$ for *any* uniquely encipherable, uniquely decipherable cipher, as long as each key is equally likely and the set of meaningful cleartext messages follows a uniform distribution (where $H(K)$ is the key entropy and D is the redundancy of the source language). In this paper, we show that Hellman's result holds with no restrictions on the distribution of keys and messages. We also bound from above and below the key equivocation upon seeing the ciphertext. Sufficient conditions for these bounds to be tight are given. The results are obtained through very simple purely information theoretic arguments, with no needs for (explicit) counting arguments.

The formal statements and proofs will be provided in the final paper, to appear in the *Journal of Cryptology* [BB88].

Bibliography

[BB88] Beauchemin, P. and G. Brassard, "A generalization of Hellman's extension of Shannon's approach to cryptography", to appear in *Journal of Cryptology*, 1988.

[Hell77] Hellman, M. E., "An extension of the Shannon theory approach to cryptography", *IEEE Transactions on Information Theory*, vol. IT-23, 1977, pp. 289-294.

[Shan49] Shannon, C. E., "Communication theory of secrecy systems", *Bell System Technical Journal*, vol. 28, 1949, pp. 656-715.

C. Pomerance (Ed.): Advances in Cryptology - CRYPTO '87, LNCS 293, p. 461, 1988.