Tatra Mt. Math. Publ. **25** (2002), 81–89

TATRA MOUNTAINS
Mathematical Publications

A SHARP PROOF OF UNICITY DISTANCE FOR MARKOFF SOURCES

Otokar Grošek* — Sergio A. Herrera-Garcia† — Karol Nemoga‡ — Ladislav Satko*

ABSTRACT. The *unicity distance* of a symmetric cryptosystem, denoted by n_0, is defined to be the value, at which the expected number of spurious keys becomes zero. In words of entropy, if we have at least n_0 ciphertexts $Y_1, Y_2, \dots, Y_{n_0}$ then there is no uncertainty about the used key, i.e., $H(K/Y_1, Y_2, \dots, Y_n) \approx 0$ for all $n \geq n_0$. Standard approach to estimate such an n_0 can be found in [D. Konheim: *Cryptograpy.* A primer, J. Wiley & Sons, New York, 1981], [D. Stinson: *Cryptography.* Theory and Practice, CRC Press, Boca Raton, Florida, 1995]. Unfortunately, in this kind of proof there is no specification of the used source, and this bound is not valid in general.

It is shown that for a cryptosystem with the key-space $\mathcal{K}$, and plaintext alphabet $\mathcal{P}$, the following is valid:

$$n_0 \geq \frac{\log_2 |\mathcal{K}|}{\mathcal{R} \log_2 |P|} - r\left(\frac{1}{\mathcal{R}} - 1\right)$$

for a stationary Markoff source of the rth order with the redundancy $\mathcal{R}$.

For a general case

$$n_0 \geq \max\left\{ n(\varepsilon), \frac{\log_2 |\mathcal{K}|}{\mathcal{R} \log_2 |P| + \varepsilon} \right\},$$

where $n(\varepsilon)$ is determined by the well known relation (see, e.g., [R. G. Galager: *Information Theory and Reliable Communication*, J. Wiley, New Yor, 1968])

$$\left| \frac{1}{n} H(A_1, A_2, \dots, A_n) - \mathcal{H} \right| < \varepsilon .$$

2000 Mathematics Subject Classification: 94A60, 60J22.
Keywords: unicity distance, Markoff sources.

* This work was supported by VEGA grant 1/7611/20.

† The author wants to express thanks to CITEDI–IPN Research Center and CONACYT MEXICO for supporting this work.

‡ This work was supported by VEGA grant 2/1130/21.

1. Some basic facts

The *unicity distance* of a symmetric cryptosystem, denoted by n_0, is defined to be the value, at which the expected number of spurious keys becomes zero. In words of entropy, if we have at least n_0 ciphertexts $Y_1, Y_2, \dots, Y_{n_0}$ then there is no uncertainty about the used key, i.e., $H(K/Y_1, Y_2, \dots, Y_n) \approx 0$ for all $n \geq n_0$. Standard approach to estimate such an n_0 can be found in [4, 8]. Unfortunately, in this kind of proof there is no specification of the used source, and this bound is not valid in general.

It is shown that for a cryptosystem with the key-space $\mathcal{K}$, and plaintext alphabet $\mathcal{P}$, the following is valid:

$$n_0 \geq \frac{\log_2 |\mathcal{K}|}{\mathcal{R} \log_2 |P|} - r\left(\frac{1}{\mathcal{R}} - 1\right)$$

for a stationary Markoff source of the rth order with the redundancy $\mathcal{R}$.

For a general case

$$n_0 \geq \max\left\{ n(\varepsilon),\, \frac{\log_2 |\mathcal{K}|}{\mathcal{R} \log_2 |P| + \varepsilon} \right\},$$

where $n(\varepsilon)$ is determined by the well known relation (see e.g., [3])

$$\left| \frac{1}{n} H(A_1, A_2, \dots, A_n) - \mathcal{H} \right| < \varepsilon . \tag{1}$$

Definition 1. Entropy $\mathcal{H}$ of a source is known to be the number (if there exists)

$$\mathcal{H} = \lim_{k \to \infty} \frac{1}{k} H(A_1, A_2, \dots, A_k) . \tag{2}$$

Especially, for a stationary Markoff source of order r, and $k > r$ we have

$$\begin{aligned}
\frac{1}{k} H(A_1, A_2, \dots, A_k) &= \frac{1}{k} H(A_1, A_2, \dots, A_r) + \frac{1}{k} H(A_{r+1}/A_1, A_2, \dots, A_r) \\
&\quad + \ \cdots + \frac{1}{k} H(A_k/A_1, A_2, \dots, A_{k-1}) \\
&= \frac{1}{k} H(A_1, A_2, \dots, A_r) + \frac{1}{k} H(A_{r+1}/A_1, A_2, \dots, A_r) \\
&\quad + \ \cdots + \frac{1}{k} H(A_{r+1}/A_1, A_2, \dots, A_r) \\
&= \frac{1}{k} H(A_1, A_2, \dots, A_r) + \frac{k-r}{k} H(A_{r+1}/A_1, A_2, \dots, A_r) .
\end{aligned} \tag{3}$$

This yields

Theorem 1. *For a stationary Markoff source of order r the following is valid*

(1) $\mathcal{H} = H(A_{r+1}/A_1, A_2, \ldots, A_r)$;

(2) $\frac{1}{k} H(A_1, A_2, \ldots, A_k) \geq \frac{k-r}{k}\,\mathcal{H}$.

Entropy of a source is closely related to the notion of so called *source redundancy.*

Definition 2. *Redundancy* $\mathcal{R}$ of a source working on an alphabet $\mathcal{P}$ and having entropy $\mathcal{H}$ is the number defined by[1]

$$\mathcal{R} = 1 - \frac{\mathcal{H}}{\log_2 |\mathcal{P}|}\,.$$

Almost all formulas valid for stationary sources are also valid for non-stationary ergodic sources too. Unfortunately this is not true in general. As an example we present Item 2 of Theorem 1.

2. Spurious keys and unicity distance

A. Kerckhoffs[2], a German teacher at Ecole des Etudies Commerciales, and at Ecole Arago in Paris, was dealing with ciphering. He was the first who clearly stated in his book *La Cryptographie militaire* the fact that a security of a (symmetric) algorithm must depend on a secret key only. Hence it makes sense to deal with a function

$$\jmath(n) = \begin{cases} H(K) & \text{if } n = 0\,, \\ H(K/Y_1, Y_2, \ldots, Y_n) & \text{if } n > 0\,, \end{cases}$$

where K is an unknown key, and $Y_1, Y_2, \ldots, Y_n$ are observable ciphertexts. This function is decreasing. To find its values is not an easy task even for a simple algorithm, like Caesar cipher. In practice we use a vocabulary and estimate these values with respect to the words listed there.

The following theorem is known [4, 8]:

Theorem 2. *Let X, $e(X,k) = Y$ be plaintext and ciphertext, respectively, obtained by a random key $K = k$, and an encryption function $e(\cdot, k)$. Then*

$$H(K/Y) = H(K) + H(X) - H(Y)\,. \tag{4}$$

[1] Some authors use for redundancy $\mathcal{D} = \mathcal{R}\log_2|\mathcal{P}| = \log_2|\mathcal{P}| - \mathcal{H}$ (see [6, 2]).

[2] Auguste Kerckhoffs (1835–1903), born in Netherlands.

COROLLARY 1. *Theorem 2 is valid for random vectors* $X = (X_1, X_2, \dots, X_n)$ *and* $Y = (Y_1, Y_2, \dots, Y_n)$ *too:*

$$H(K/Y_1, Y_2, \dots, Y_n) = H(K) + H(X_1, X_2, \dots, X_n) - H(Y_1, Y_2, \dots, Y_n). \quad (5)$$

In [2, 4, 6] an "ergodic" approach was used to estimate unicity distance. A different approach is shown in [8]. The following is a corrected version of Theorem 2.11 from the cited book.

THEOREM 3. *Assume a stationary Markoff source of the order* r, *and having a redundancy* $\mathcal{R}$. *Let possible plaintexts and ciphertexts be of the same cardinality, i.e.,* $|\mathcal{P}| = |\mathcal{C}|$. *Let probability distribution for key* $k \in \mathcal{K}$ *be uniform,* $\mathrm{Prob}(K = k) = 1/|\mathcal{K}|$. *Let* S_n *be a random variable counting the number of spurious keys if an opponent knows* n *ciphertexts* $Y_1, Y_2, \dots, Y_n$. *Then the mean value of* S_n, $n > r$ *is*

$$E(S_n) \geq \frac{|\mathcal{K}|}{|\mathcal{P}|^{n\mathcal{R}+r(1-\mathcal{R})}} - 1. \quad (6)$$

Proof. Let $x = (x_1, x_2, \dots, x_n)$, and let $y = (y_1, y_2, \dots, y_n)$ be fixed. Denote $U(y)$ the set of possible keys for the ciphertext y as

$$\begin{aligned} U(y) &= U(y_1, y_2, \dots, y_n) \\ &= \left\{ k \in \mathcal{K} \colon \text{ there exists } x \in \mathcal{P}^n \text{ such that } e_k(x_i) = y_i \right\}. \end{aligned}$$

Then clearly $S_n = |U(y)| - 1$ is the number of spurious keys. For its mean value we have

$$\begin{aligned} E(S_n) &= \sum_y P(Y_1 = y_1, Y_2 = y_2, \dots, Y_n = y_n)\big(|U(y)| - 1\big) \\ &= \sum_y P(Y_1 = y_1, Y_2 = y_2, \dots, Y_n = y_n)\big|U(y)\big| \\ &\quad - \sum_y P(Y_1 = y_1, Y_2 = y_2, \dots, Y_n = y_n) \\ &= \sum_y P(Y_1 = y_1, Y_2 = y_2, \dots, Y_n = y_n)\big|U(y)\big| - 1. \end{aligned}$$

From Definitions, (1), (2), and from Item 2 of Theorem 1 we have the estimation[3]

$$H(X) > (n - r)\mathcal{H} = (n - r)(1 - \mathcal{R}) \log_2 |\mathcal{P}|. \quad (7)$$

With respect to our assumption $|\mathcal{P}| = |\mathcal{C}|$

$$H(Y) = H(Y_1, Y_2, \dots, Y_n) \leq n \log_2 |\mathcal{C}| = n \log_2 |\mathcal{P}|$$

[3] In fact, this is the place where our proof is sharp contrary to [8].

and (5) can be written as

$$\begin{aligned} H(K/Y) &= H(K) + H(X) - H(Y) \\ &\geq H(K) + (n-r)(1-\mathcal{R})\log_2|\mathcal{P}| - n\log_2|\mathcal{P}|\,, \end{aligned} \tag{8}$$

and for $H(K) = \log_2|\mathcal{K}|$,

$$H(K/Y) \geq \log_2 \frac{|\mathcal{K}|}{|\mathcal{P}|^{n\mathcal{R}}|\mathcal{P}|^{r(1-\mathcal{R})}}\,. \tag{9}$$

On the other hand, using the well known Jensen's inequality [8]

$$\begin{aligned} H(K/Y) = &\sum_y P(Y_1 = y_1, Y_2 = y_2, \ldots, Y_n = y_n) \\ &\times H\big(K/Y_1 = y_1, Y_2 = y_2, \ldots, Y_n = y_n\big) \end{aligned}$$

$$\begin{aligned} &\leq \sum_y P\big(Y_1 = y_1, Y_2 = y_2, \ldots, Y_n = y_n\big)\log_2\big|U(y)\big| \\ &\leq \log_2\Big(\sum_y P\big(Y_1 = y_1, Y_2 = y_2, \ldots, Y_n = y_n\big)\big|U(y)\big|\Big) \\ &= \log_2\big(E(S_n) + 1\big)\,. \end{aligned} \tag{10}$$

If we compare estimations (9) and (10)

$$\log_2\big(E(S_n) + 1\big) \geq \log_2 \frac{|\mathcal{K}|}{|\mathcal{P}|^{n\mathcal{R}+r(1-\mathcal{R})}}\,,$$

and after a small manipulation we can conclude our proof. Moreover, the lower bound for $E(S_n)$ decreases with n exponentially to -1. □

As a corollary we have

Corollary 2. *Let n_0 be the smallest number of known ciphertexts such that $E(S_{n_0}) = 0$. Then the following is valid*

$$n_0 \geq \frac{\log_2|\mathcal{K}|}{\mathcal{R}\log_2|\mathcal{P}|} - r\left(\frac{1}{\mathcal{R}} - 1\right). \tag{11}$$

Example 1. Taking a simple substitution cipher on English as an example with typical parameters $\mathcal{H}_r$ bits/character, taken from [7], the new "correction terms" $d(r) = r\left(\frac{1}{\mathcal{R}} - 1\right)$ just involved are as follows:

r	0	1	2	3
$\mathcal{H}_r$	4.7	4.14	3.56	3.30
$\mathcal{R}_r$	0.0	0.12	0.24	0.30
$d(r)$	0.0	7.40	6.24	7.07

If we omit in Theorem 3 the assumption about the type of source, namely that it is Markoff, then we cannot use Item 2 of Theorem 1. If this is the case, we may use (2). From the existence of this limit, for any $\varepsilon > 0$, there exists $n(\varepsilon)$ such that for all $n > n(\varepsilon)$

$$\left|\frac{1}{n}H(X) - \mathcal{H}\right| < \varepsilon$$

is valid. This yields a similar estimation as (7):

$$-\varepsilon n + n\mathcal{H} < H(X) < \varepsilon n + n\mathcal{H},$$

$$H(X) > -\varepsilon n + n(1-\mathcal{R})\log_2|\mathcal{P}|.$$

The same arguments then lead to

$$E(S_n) \geq \frac{|\mathcal{K}|}{2^{n\varepsilon}|\mathcal{P}|^{n\mathcal{R}}} - 1, \tag{12}$$

or to

$$n_0 \geq \max\left\{n(\varepsilon), \frac{\log_2|\mathcal{K}|}{\mathcal{R}\log_2|\mathcal{P}| + \varepsilon}\right\}.$$

We emphasize, that the smaller is ε, the greater is $n(\varepsilon)$. In such a case $n_0 = n(\varepsilon)$. This correction is important since in practice we are interested in estimations for a relatively small n.

EXAMPLE 2. For particular choices of $\mathcal{K}, \mathcal{P}$ and $\mathcal{R}$ of a Markoff source of order 0 we have:

- In the case of Caesar cipher $n_0 \geq \frac{1}{\mathcal{R}}$.
- In the case of Hill cipher[4], and $\mathcal{P} = \mathbb{F}_q$, the number of all regular matrices $h \times h$ is given by (see, e.g., [5])

$$q^{h^2}\prod_{i=1}^{h}\left(1 - \frac{1}{q^i}\right).$$

  Assuming choices of b we have

$$|\mathcal{K}| = q^{h^2+h}\prod_{i=1}^{h}\left(1 - \frac{1}{q^i}\right), \qquad |\mathcal{P}^h| = q^h,$$

  and thus $n_0 \geq \frac{h+1}{\mathcal{R}}$. Recall that here n_0 means the number of blocks, and $\mathcal{R}$ is the redundancy of blocks too.

[4] Hill cipher is defined to be an affine transformation $y = xA + b$.

- In the case of Hill cipher, and $\mathcal{P} = Z_{26}$, $h = 2$, and $b = (0,0)$, one can find the number of all 2×2 regular matrices, namely 157 248.[5]
  Hence $n_0 \geq \frac{1.836}{\mathcal{R}}$ which is slightly different from expected $n_0 \geq \frac{2}{\mathcal{R}}$. But the reason is clear: dependences between blocks of plaintexts and rows of regular matrices.

3. Estimation of the order r

It is readily seen from formula (11) that unicity distance is a function of order r. Hence one can study the following problem: Assume a stationary Markoff source of an unknown order r, and having a redundancy $\mathcal{R}$. Let possible plaintexts and ciphertexts be of the same cardinality, i.e., $|\mathcal{P}| = |\mathcal{C}|$. Let probability distribution for key $k \in \mathcal{K}$ be uniform, $\mathrm{Prob}(K = k) = 1/|\mathcal{K}|$. What is the smallest possible r such that the unicity distance of the source will be n_0? This is the same as to suppose that after having n_0 ciphertexts, one can uniquely identify the related plaintext.

An easy manipulation with (11) and Definition 2 yields

$$r \geq n_0 + \frac{1}{\mathcal{H}} \log_2 \frac{|\mathcal{K}|}{|\mathcal{P}|^{n_0}} . \tag{14}$$

Next we apply our result to Hill cipher defined to be an affine transformation $y \equiv x * A + b \pmod{m}$, where A is an $h \times h$ regular matrix over Z_m. We refer to the three particular cases, namely:

1. $h = 1$, $A = 1$, $b \in Z_m$, known as Caesar shift. For $m = 26$, $\log_2 |\mathcal{K}| = \log_2 26 = 4.70044$, and $\hat{r}_0 \approx n_0 + 4.7(1 - n_0)/\mathcal{H}_r$;
2. $h = 1$, $\gcd(A, m) = 1$, $b \in Z_m$, known as Affine cipher. For $m = 26$, $\log_2 |\mathcal{K}| = \log_2\bigl(m\varphi(m)\bigr) = \log_2 26 + \log_2 12 = 4.70044 + 3.58496$, and $\hat{r}_1 \approx n_0 + 4.7(1 - n_0)/\mathcal{H}_r + 3.6/\mathcal{H}_r$.

[5] We recall the formula for the number of $h \times h$ regular matrices over Z_m due to [1]: Let $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s}$ be a prime factorization of a modulus m, and

$$\rho(p, h) = \prod_{j=1}^{h} \left(1 - p^{-j}\right) .$$

Then the number $g(m, h)$ of all $h \times h$ regular matrices over Z_m is given by

$$g(m, h) = m^{h^2} \prod_{j=1}^{s} \rho(p_j, h) . \tag{13}$$

3. $\gcd(\det(A), m) = 1$, $b = 0$, known as linear Hill cipher. For $m = 26$, and large h, $\log_2 |\mathcal{K}| = \log_2 g(m,h) \approx h^2 \log_2 m$, and $\hat{r}_2 \approx n_0 + 4.7(h^2 - 2n_0)/\mathcal{H}_r$.

Our experimental results are as follows:

- In order to have an estimation for entropies $\mathcal{H}_r$ we processed randomly selected plaintexts taken from one Slovak newspaper (PRÁCA), and simplified to the alphabet $\mathcal{P} = Z_{26}$. Finally we got a 35 412 kB file, and from our previous experiments we already know that a good estimation of unicity distance for Caesar and Affine cipher is $\hat{n}_0 = 4$, and for Hill cipher and $h = 2$ is $\hat{n}_0 = 2$.
- Calculated entropies $H(A_1) = 4.19939$, $H(A_1, A_2) = 7.72769$, $H(A_1, A_2, A_3) = 10.77093$.
- By Theorem 1 we have estimations $\mathcal{H}_0 = 4.19939$, $\mathcal{H}_1 = 3.528299$, $\mathcal{H}_2 = 3.04324$.
- Final estimations for orders are arranged in the table below, where for $g(26, 2)$ we use the exact number 157 248.

r	0	1	2
$\mathcal{H}_r$	4.19939	3.528299	3.04324
$\hat{r}_0$	0.64	1.50	−0.63
$\hat{r}_1$	0.00	1.02	0.54
$\hat{r}_2$	3.87	4.23	4.58

- From these results we conclude (in the case of the newspaper style in the Slovak language...), that in the case of Caesar and Affine cipher we recommend $\hat{r} = 2$, and for Hill cipher for blocks of the length 2, $\hat{r} = 5$.

REFERENCES

[1] BAUER, F. L.: *Entzifferte Geheimnisse*, Springer-Verlag, Berlin, 1995.

[2] HELLMAN, M. E.: *An Extension of the Shannon Theory Approach to Cryptography*, IEEE Trans. Inform. Theory IT-23 (1977), 289–294.

[3] GALAGER, R. G.: *Information Theory and Reliable Communication*, J. Wiley, New York, 1968.

[4] KONHEIM, D.: *Cryptography. A Primer*, J. Wiley & Sons, New York, 1981.

[5] LIDL, R.—NIEDERREITER, H.: *Finite Fields*, Encyclopedia Math. Appl., Vol. 20, Addison–Wesley, Reading Mass., 1983.

[6] SHANNON, C. E.: *Communication theory of secrecy systems*, Bell System Tech. J. **28** (1949), 656–715.

[7] SHANNON, C. E.: *Prediction and entropy of printed English*, Bell System Tech. J. **30** (1951), 50–64.

[8] STINSON, D. R.: *Cryptography. Theory and Practice*, CRC Press. Boca Raton, Florida, 1995 (2nd edition 2002).

Received April 2, 2002

Otokar Grošek, Ladislav Satko
Department of Mathematics
Faculty of Electrical Engineering
and Informatin Technology
Slovak University of Technology
Ilkovičova 3
SK–812 19 Bratislava
SLOVAKIA
E-mail: grosek@elf.stuba.sk
satko@elf.stuba.sk

Sergio A. Herrera-Garcia
CITEDI–IPN Research Center
Tijuana, 22310
MEXICO
E-mail: sherrera@telnor.net

Karol Nemoga
Institute of Mathematics
Slovak Academy of Sciences
SK–814 73 Bratislava
SLOVAKIA
E-mail: nemoga@mat.savba.sk