Math-Net.Ru

Общероссийский математический портал

I. M. Arbekov, Нижние оценки для практической секретности ключа, *Матем. вопр. криптогр.*, 2017, том 8, выпуск 2, 29–38

DOI: <https://doi.org/10.4213/mvk221>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением

<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 3.95.254.165

26 апреля 2023 г., 16:01:00

Lower bounds for the practical secrecy of a key

I. M. Arbekov

JSC “InfoTeCS”, Moscow

Получено 17.III.2016

Abstract. We obtain lower bounds for the *practical secrecy* of a key. *Practical secrecy* is defined as the average amount of keys tested before the *encryption* key is determined. To find the *encryption* key we use truncated key search algorithms having some *success* probabilities. The lower bounds of the *practical secrecy* are expressed in terms of limiting values of success probabilities and of total variation distance between the key probability distribution and the uniform distribution.

Key words: practical secrecy of a key, truncated key search, symmetric cryptography

Нижние оценки для практической секретности ключа

И. М. Арбеков

ОАО «ИнфоТеКС», Москва

Аннотация. В работе получены нижние оценки *практической секретности* ключа. *Практическая секретность* определяется как среднее число опробованных ключей до определения ключа *шифрования*. Для определения ключа *шифрования* мы используем усеченные алгоритма поиска ключа, имеющие некоторые вероятности *успеха*. Нижняя оценка *практической секретности* выражается через предельное значение вероятности *успеха* и расстояние по вариации между распределением ключей и равномерным распределением.

Ключевые слова: практическая секретность ключа, усеченный поиск ключа, симметричная криптография

1. Practical secrecy of a key

1.1. Preliminaries

In [1] we have introduced the concept of the *practical secrecy* of a key as the average amount of work to determine the *encryption* key. In this section we will repeat some of the main provisions of [1].

In order to find the *encryption* key we use truncated key search algorithms with a check for readability of decrypted messages. If M keys have been tested, we say that the amount of work R is equal to $M : R = M$.

Let $K = \{1, 2, \dots, N\}$ be a key set and the selection of *encryption* keys in symmetric cryptography be defined by an *unobservable* random sample

$$k_1, k_2, \dots, k_i, \dots, k_N \in \{1, 2, \dots, N\}, \quad i = 1, 2, \dots, \quad (1)$$

where independent random variables $k_i, i = 1, 2, \dots$, have the common probability distribution $P = (p_1, p_2, \dots, p_N)$,

$$p_1 \geq p_2 \geq \dots \geq p_N. \quad (2)$$

Suppose that the testing of keys is in the order specified by (2). In the case of *exhaustive* key search we determine the *encryption* key in each experiment in the sample (1) with *success* probability equal to *unity* and with the average amount (the expectation) of work equal to

$$\bar{R} = \sum_{m=1}^N m p_m.$$

The maximum value of $\bar{R}$ corresponds to the uniform distribution $P = P_0 = (N^{-1}, \dots, N^{-1})$ [1]:

$$\bar{R}^{(max)} = \sum_{m=1}^N m \frac{1}{N} = \frac{N+1}{2}.$$

Consider a specific example of key distribution. Let

$$P = (p_1, p_2, \dots, p_N), \quad p_1 = \frac{1}{2}, \quad p_2 = \dots = p_N = \frac{1}{2(N-1)}. \quad (3)$$

The average amount of work for the *exhaustive* key search algorithm is

$$\bar{R} = \frac{1}{2} + \frac{1}{2(N-1)} \sum_{m=2}^N m = \frac{1}{2} + \frac{(2+N)(N-1)}{4(N-1)} > \frac{N}{4} \approx \frac{1}{2} \bar{R}^{(max)}$$

and we can say that from the viewpoint of the average amount of work the key distribution (3) is not very “bad”.

Consider the algorithm A where only the key having number 1 is being tested for each experiment in the sample (1). As $\mathbf{P}(k_i = 1) = 1/2$, each *encryption* key in the sample (1) is determined with the *success* probability equal to $1/2$. The number ξ of experiments (*steps*) before the *first success* has a geometric distribution with expectation $\mathbf{E} \xi = 1$.

Then the average amount of work to determine the *encryption* key for the *first time* in the sample (1) is, obviously, $\bar{R}_A = 2$. In other words, the average amount of additional work sufficient to reveal one more *encryption* key is equal to $\bar{R}_A = 2$. From this viewpoint the key with distribution (3) is very “bad”.

In this context, it is advisable to consider a *truncated* algorithm U , such that a search is performed only on the initial part of key set $\tilde{K} \subseteq K, |\tilde{K}| = M \leq N$. Let us find the average amount of work needed to reveal the *encryption* key for the *first time* in the sample (1) by means of truncated algorithm. Notice that if $M = N$ then we have the *exhaustive* key search algorithm.

For a *truncated* algorithm U each *encryption* key in the sample (1) is revealed with the success probability

$$\pi_U(M) = \sum_{m=1}^M p_m, \quad 0 < \pi_U(M) \leq 1, \quad p_1 \geq p_2 \geq \dots \geq p_N.$$

The number ξ of experiments before the first *success* (before the *encryption* key hits $\tilde{K}$) has a geometric distribution

$$\mathbf{P}(\xi = j) = (1 - \pi_U(M))^j \pi_U(M), \quad \sum_{j=0}^{\infty} \mathbf{P}(\xi = j) = 1,$$

and expectation

$$\mathbf{E} \xi = \frac{1 - \pi_U(M)}{\pi_U(M)}. \quad (4)$$

Let $\xi = j$, then in the sample (1) $k_1 \notin \tilde{K}, \dots, k_j \notin \tilde{K}, k_{j+1} \in \tilde{K}$. Conditionally on $k_{j+1} \in \tilde{K}$ the key distribution of k_{j+1} takes the form

$$\left(\frac{p_1}{\pi_U(M)}, \dots, \frac{p_M}{\pi_U(M)} \right).$$

Using (4) we find that the average amount $\bar{R}_U(M)$ of work to reveal the *encryption* key with truncated search algorithm U is

$$\begin{aligned} \bar{R}_U(M) &= \frac{(1 - \pi_U(M)) M}{\pi_U(M)} + \sum_{m=1}^M m \frac{p_m}{\pi_U(M)} = \\ &= \frac{(1 - \sum_{m=1}^M p_m) M + \sum_{m=1}^M m p_m}{\sum_{m=1}^M p_m}. \end{aligned} \quad (5)$$

We can minimize $\bar{R}_U(M)$ over the parameter M . For small $\pi_U(M)$ the value $(\pi_U(M))^{-1}$ represents the average number of experiments before the first success:

$$\mathbf{E} \xi = \frac{1 - \pi_U(M)}{\pi_U(M)} \approx \frac{1}{\pi_U(M)}$$

and cannot be *too* small.

Therefore, when we consider the truncated algorithms U with an average amount of work (5) it is advisable to restrict ourselves to algorithms with

$$\pi_U(M) = \sum_{m=1}^M p_m \geq \pi_0,$$

for some reasonable choice of π_0 .

Thus in [1] we have defined the notion of *practical secrecy* of a key with the ordered probability distribution $p_1 \geq p_2 \geq \dots \geq p_N$ as

$$Q = \min_{M: \pi_U(M) \geq \pi_0} \bar{R}_U(M). \quad (6)$$

For the uniform distribution $P = P_0 = (N^{-1}, \dots, N^{-1})$ we get from (5)

$$\bar{R}_U(M) = \frac{2N - M + 1}{2}$$

and

$$Q = \min_{M: \pi_U(M) \geq \pi_0} \bar{R}_U(M) = \frac{N+1}{2}.$$

Thus, *truncated* key search algorithms does not give any advantages over *exhaustive* key search algorithm in the case of the uniform probability distribution of *encryption* key.

1.2. The lower bound for the practical secrecy of a key

Now we consider a key set $K = \{1, 2, \dots, N\}$ with a probability distribution

$$P = (p_1, p_2, \dots, p_N), \quad p_1 \geq p_2 \geq \dots \geq p_N.$$

Let

$$\delta = \frac{1}{2} \sum_{m=1}^N \left| p_m - \frac{1}{N} \right|$$

be the *total variation distance*. We have find that an average amount of work needed to reveal one *encryption* key by the truncated key search algorithm is given by (5) and defined the *practical secrecy* of a key by the formula (6).

What is the relation between δ and Q ?

Proposition 1. *If $2\delta < \pi_0$, then*

$$Q \geq \left(1 - \frac{2\delta}{\pi_0}\right) \left(\frac{N(1-8\delta)+1}{2}\right). \quad (7)$$

Proof. Obviously,

$$\pi_U(M) = \sum_{m=1}^M p_m = \frac{M}{N} + \sum_{m=1}^M \left(p_m - \frac{1}{N}\right) \leq \frac{M}{N} + 2\delta \quad (8)$$

and if $2\delta < \pi_0$, then

$$\{M : \pi_U(M) \geq \pi_0\} \subseteq \left\{M : \frac{M}{N} \geq \pi_0 - 2\delta\right\} = \left\{M : \frac{N}{M} \leq \frac{1}{\pi_0 - 2\delta}\right\}. \quad (9)$$

Then, using (8), (9) we get:

$$\begin{aligned} \frac{1}{\pi_U(M)} &\geq \frac{1}{(M/N)+2\delta} = \frac{N}{M} \frac{1}{1+2\delta(N/M)} \geq \\ &\geq \frac{N}{M} \frac{1}{1+2\delta(\pi_0-2\delta)^{-1}} = \left(1 - \frac{2\delta}{\pi_0}\right) \frac{N}{M}, \end{aligned} \quad (10)$$

$$\begin{aligned} \sum_{m=1}^M m p_m &= \frac{M(M+1)}{2N} + \sum_{m=1}^M m \left(p_m - \frac{1}{N}\right) \geq \\ &\geq \frac{M(M+1)}{2N} - \sum_{m=1}^M m \left|p_m - \frac{1}{N}\right| \geq \frac{M(M+1)}{2N} - M 2\delta. \end{aligned} \quad (11)$$

Bringing together (8)–(11) we get

$$\begin{aligned} Q &= \min_{M: \pi_U(M) \geq \pi_0} \bar{R}_U(M) \geq \min_{M: \frac{M}{N} \geq \pi_0 - 2\delta} \frac{(1 - \pi_U(M))M + \sum_{m=1}^M m p_m}{\pi_U(M)} \geq \\ &\geq \min_{M: \frac{M}{N} \geq \pi_0 - 2\delta} \left(1 - \frac{2\delta}{\pi_0}\right) \frac{2N - M - 8N\delta + 1}{2} = \\ &= \left(1 - \frac{2\delta}{\pi_0}\right) \frac{N(1-8\delta)+1}{2}. \quad \square \end{aligned}$$

The inequality (7) is nontrivial if $\delta < \min\{1/8, \pi_0/2\}$. If $\delta \ll 1$, $\pi_0 \ll 1$, then the asymptotical lower bound for the *practical secrecy* Q takes the form

$$\left(1 - \frac{2\delta}{\pi_0}\right) \bar{R}^{(max)}.$$

2. Practical secrecy of a key under observations

2.1. The average amount of work

Under observations we have a key set $K = \{1, 2, \dots, N\}$ and a random sample

$$(k_1, z_1), (k_2, z_2), \dots, (k_i, z_i), \dots \quad (12)$$

$$k_i \in \{1, 2, \dots, N\}, \quad z_i \in Z, \quad i = 1, 2, \dots,$$

where independent random vectors (k_i, z_i) , $i = 1, 2, \dots$, have the common joint probability distribution $\mathbf{P}(k_i = m, z_i = z) = P(m, z)$; here k_i is an *unobserved* component (*encryption* key) and z_i is an *observed* component from some space of observations Z .

When observing z_i the posterior probability distribution

$$P(1|z_i), \dots, P(m|z_i), \dots, P(N|z_i),$$

of keys may be calculated:

$$P(m|z_i) = \frac{P(m, z_i)}{P(z_i)}, \quad P(z_i) = \sum_{s=1}^N P(s, z_i),$$

and ordered:

$$P(i_1|z_i) \geq P(i_2|z_i) \geq \dots \geq P(i_N|z_i). \quad (13)$$

If for some $\alpha, \beta, \dots, \gamma$ we have $P(i_\alpha|z_i) = P(i_\beta|z_i) = \dots = P(i_\gamma|z_i)$, then the posterior probabilities are ordered in accordance with the $\{1, 2, \dots, N\}$.

Then $\sigma(z_i) = (i_1, i_2, \dots, i_N)$ is some permutation of $(1, 2, \dots, N)$ depending on z_i .

Truncated algorithm U for each observation ($i = 1, 2, \dots$) tests M keys in the order $(i_1, i_2, \dots, i_M)$.

Let $\mathbf{z} = (z_1, z_2, \dots, z_i, \dots)$ be a fixed sequence of observations.

In the i th experiment the *encryption* key k_i is selected in accordance with the conditional distribution (13). The conditional probability that the key k_i belongs to the set $\tilde{K}(z_i) = (i_1, i_2, \dots, i_M)$ is

$$\pi_U^*(M, z_i) = \mathbf{P}(k_i \in \tilde{K}(z_i) | z_i) = \sum_{m=1}^M P(i_m | z_i).$$

The number ξ of experiments (*steps*) before the *first success* (before the *encryption* key k_{j+1} hits $\tilde{K}(z_{j+1})$) has a conditional distribution

$$\begin{aligned} \mathbf{P}(\xi = j | \mathbf{z}) &= \mathbf{P}(k_1 \notin \tilde{K}(z_1), \dots, k_j \notin \tilde{K}(z_j), k_{j+1} \in \tilde{K}(z_{j+1}) | \mathbf{z}) = \\ &= \pi_U^*(M, z_{j+1}) \prod_{s=0}^j (1 - \pi_U^*(M, z_s)), \quad j = 0, 1, \dots \end{aligned}$$

Then the *conditional* average amount $\bar{R}_U^*(M | \mathbf{z})$ of work needed to determine one *encryption* key in the sample (12) is

$$\begin{aligned} \bar{R}_U^*(M | \mathbf{z}) &= \sum_{j=0}^{\infty} \mathbf{E}(\bar{R}_U^*(M | \mathbf{z}, \xi = j) \mathbf{P}(\xi = j | \mathbf{z})) = \\ &= \sum_{j=0}^{\infty} \left(jM + \sum_{m=1}^M m \frac{P(i_m | z_{j+1})}{\pi_U^*(M, z_{j+1})} \right) \mathbf{P}(\xi = j | \mathbf{z}) = \\ &= M \sum_{j=0}^{\infty} \left(j \pi_U^*(M, z_{j+1}) \prod_{s=0}^j (1 - \pi_U^*(M, z_s)) \right) + \\ &\quad + \sum_{j=0}^{\infty} \sum_{m=1}^M \left(m \frac{P(i_m | z_{j+1})}{\pi_U^*(M, z_{j+1})} \pi_U^*(M, z_{j+1}) \prod_{s=0}^j (1 - \pi_U^*(M, z_s)) \right) = \\ &= M \sum_{j=0}^{\infty} \left(j \pi_U^*(M, z_{j+1}) \prod_{s=0}^j (1 - \pi_U^*(M, z_s)) \right) + \\ &\quad + \sum_{j=0}^{\infty} \sum_{m=1}^M \left(m P(i_m | z_{j+1}) \prod_{s=0}^j (1 - \pi_U^*(M, z_s)) \right). \end{aligned} \quad (14)$$

Let

$$\begin{aligned} p_m^* &= \mathbf{E}_z P(i_m | z) = \sum_{z \in Z} P(i_m | z) P(z), \\ \pi_U^*(M) &= \mathbf{E}_z \pi_U^*(M, z) = \sum_{z \in Z} \sum_{m=1}^M P(i_m | z) P(z) = \sum_{m=1}^M p_m^*. \end{aligned}$$

The following equations hold:

$$\begin{aligned} \sum_{m=1}^N p_m^* &= 1, \\ \sum_{j=0}^{\infty} j \pi_U^*(M) (1 - \pi_U^*(M))^j &= \frac{1 - \pi_U^*(M)}{\pi_U^*(M)}, \\ \sum_{j=0}^{\infty} \pi_U^*(M) (1 - \pi_U^*(M))^j &= 1. \end{aligned} \quad (15)$$

Then, averaging (14) over $\mathbf{z} = (z_1, z_2, \dots, z_i, \dots)$ and using (15) we get the average amount of work $\bar{R}_U^*(M)$ needed to determine one *encryption* key in the sample (12):

$$\begin{aligned} \bar{R}_U^*(M) &= M \sum_{j=0}^{\infty} \left(j (\mathbf{E}_z \pi_U^*(M, z_{j+1})) \prod_{s=0}^j (1 - \mathbf{E}_z \pi_U^*(M, z_s)) \right) + \\ &\quad + \sum_{j=0}^{\infty} \sum_{m=1}^M \left(m (\mathbf{E}_z P(i_m | z_{j+1})) \prod_{s=0}^j (1 - \mathbf{E}_z \pi_U^*(M, z_s)) \right) = \\ &= M \sum_{j=0}^{\infty} j \pi_U^*(M) (1 - \pi_U^*(M))^j + \sum_{j=0}^{\infty} \sum_{m=1}^M m p_m^* (1 - \pi_U^*(M))^j = \\ &= \frac{(1 - \pi_U^*(M)) M}{\pi_U^*(M)} + \sum_{m=1}^M m \frac{p_m^*}{\pi_U^*(M)} = \\ &= \frac{(1 - \sum_{m=1}^M p_m^*) M + \sum_{m=1}^M m p_m^*}{\sum_{m=1}^M p_m^*}. \end{aligned}$$

Notice that

$$p_m^* = \sum_{z \in Z} P(i_m | z) P(z)$$

is the average probability for the *encryption* key to be in the m th place for the Bayesian classification procedure.

We define the notion of *practical secrecy* of a key under observations as

$$Q^* = \min_{M: \pi_U^*(M) \geq \pi_0} \bar{R}_U^*(M).$$

2.2. The lower bound for the practical secrecy of a key under observations

Let

$$d = \frac{1}{2} \sum_{m,z} \left| P(m, z) - \frac{1}{N} P(z) \right|$$

be the *total variation distance* [2].

The average amount $\bar{R}_U^*(M)$ of work needed to determine one *encryption* key in the sample (12) is

$$\bar{R}_U^*(M) = \frac{(1 - \sum_{m=1}^M p_m^*) M + \sum_{m=1}^M m p_m^*}{\sum_{m=1}^M p_m^*},$$

the *practical secrecy* of a key under observations is

$$Q^* = \min_{M: \pi_U^*(M) \geq \pi_0} \bar{R}_U^*(M), \quad \pi_U^*(M) = \sum_{m=1}^M p_m^*.$$

Proposition 2. *If $2d < \pi_0$, then*

$$Q^* \geq \left(1 - \frac{2d}{\pi_0}\right) \frac{N(1-8d)+1}{2}.$$

Proof. Let

$$\delta^* = \frac{1}{2} \sum_{m=1}^N \left| p_m^* - \frac{1}{N} \right|.$$

As $\sigma(z) = (i_1, i_2, \dots, i_N)$ is some permutation of $(1, 2, \dots, N)$ then it is easy to get

$$\begin{aligned} \delta^* &= \frac{1}{2} \sum_{m=1}^N \left| p_m^* - \frac{1}{N} \right| = \frac{1}{2} \sum_{m=1}^N \left| \sum_{z \in Z} P(i_m | z) P(z) - \frac{1}{N} \right| = \\ &= \frac{1}{2} \sum_{m=1}^N \left| \sum_{z \in Z} \left(P(i_m, z) - \frac{1}{N} P(z) \right) \right| \leq \frac{1}{2} \sum_{m,z} \left| P(m, z) - \frac{1}{N} P(z) \right| = d. \end{aligned}$$

Then inequality $2d < \pi_0$ implies inequality $2\delta^* < \pi_0$ and using Proposition 1 we obtain:

$$Q^* \geq \left(1 - \frac{2\delta^*}{\pi_0}\right) \frac{N(1-8\delta^*)+1}{2} \geq \left(1 - \frac{2d}{\pi_0}\right) \frac{N(1-8d)+1}{2}. \quad \square$$

References

- [1] Arbekov I. M., “Criteria of key security”, *Mathematical Aspects of Cryptography*, **7**:1 (2016), 41–58 (in Russian).
- [2] Portmann C., Renner R., “Cryptographic security of quantum key distribution”, arXiv: 1409.3525v1 [quant-ph] 11 Sep 2014.