Oto Strauch

On distribution functions of sequences generated by scalar and mixed product

Mathematica Slovaca, Vol. 53 (2003), No. 5, 467--478

Persistent URL: http://dml.cz/dmlcz/136893

Mathematica Slovaca
© 2003 Mathematical Institute Slovak Academy of Sciences

Math. Slovaca, **53** (2003), No. 5, 467–478

ON DISTRIBUTION FUNCTIONS OF SEQUENCES GENERATED BY SCALAR AND MIXED PRODUCT

OTO STRAUCH

(*Communicated by Stanislav Jakubec*)

ABSTRACT. We study two types of real sequences: Firstly, the sequence of scalar products $\boldsymbol{b}_n \cdot \boldsymbol{x}_n$, $n = 1, 2, \ldots$, where $\boldsymbol{b}_n$, $\boldsymbol{x}_n$ are statistically independent and uniformly distributed in $[0,1]^3$. Secondly, the sequence of absolute values of mixed products $|(\boldsymbol{b}_n^{(1)} \times \boldsymbol{b}_n^{(2)}) \cdot \boldsymbol{x}_n|$, where $\boldsymbol{b}_n^{(1)}$, $\boldsymbol{b}_n^{(2)}$, $\boldsymbol{x}_n$, are statistically independent and uniformly distributed in the 3-dimensional ball $B(r)$ with the center $(0,0,0)$ and radius r. We compute their asymptotic distribution functions and then we modify one-time pad cipher by using these distribution functions. All basic problems are formulated for s-dimensional sequences.

1. Introduction

For a given continuous real function $f(\boldsymbol{b}, \boldsymbol{x})$, we can study a real sequence of the form $f(\boldsymbol{b}_n, \boldsymbol{x}_n)$, $n = 1, 2, \ldots$, where $\boldsymbol{b}_n$ and $\boldsymbol{x}_n$ are statistically independent and uniformly distributed (briefly u.d.) sequences of s-dimensional vectors in a Jordan-measurable bounded subset K of $\mathbb{R}^s$ with positive Lebesgue measure $|K|$. Its asymptotic distribution function (briefly a.d.f.) is defined by

$$g(t) = \lim_{N\to\infty} \frac{\#\{n \le N : \ f(\boldsymbol{b}_n, \boldsymbol{x}_n) < t\}}{N},$$

where $t \in [A_0, B_0]$, and $A_0 = \min\limits_{(\boldsymbol{b},\boldsymbol{x})\in K^2} f(\boldsymbol{b}, \boldsymbol{x})$ and $B_0 = \max\limits_{(\boldsymbol{b},\boldsymbol{x})\in K^2} f(\boldsymbol{b}, \boldsymbol{x})$. This distribution function (briefly d.f.) can be computed using relation

$$g(t) = \frac{\left|\{(\boldsymbol{b}, \boldsymbol{x}) \in K^2 : \ f(\boldsymbol{b}, \boldsymbol{x}) < t\}\right|}{|K|^2}.$$

2000 Mathematics Subject Classification: Primary 11K31, 94A60.
Keywords: sequence, uniform distribution, statistically independent sequences, distribution function, cipher, scalar product, mixed product.

This research was supported by INNA, Ltd. (Prague) and by the Slovak Academy of Sciences Grant 2/1130/21.

We can express the a.d.f. of a sequence $f\left(\boldsymbol{b}_n^{(1)}, \boldsymbol{b}_n^{(2)}, \ldots, \boldsymbol{b}_n^{(s-1)}, \boldsymbol{x}_n\right)$, $n = 1, 2, \ldots$, with statistically independent and u.d. sequences $\boldsymbol{b}_n^{(1)}, \boldsymbol{b}_n^{(2)}, \ldots, \boldsymbol{b}_n^{(s-1)}, \boldsymbol{x}_n$ in K in a similar way. Note that u.d. and statistical independence of $\boldsymbol{b}_n^{(1)}, \boldsymbol{b}_n^{(2)}, \ldots, \boldsymbol{b}_n^{(s-1)}, \boldsymbol{x}_n$ in K is equivalent to the u.d. of $\left(\boldsymbol{b}_n^{(1)}, \boldsymbol{b}_n^{(2)}, \ldots, \boldsymbol{b}_n^{(s-1)}, \boldsymbol{x}_n\right)$ in K^s. For exact definitions and basic properties of u.d. sequences and a.d.f.'s, see the monograph [DT].

Our study is motivated by a new application of the theory of u.d. in cryptology,[1] which is based on the following method for computing of the key sequence in a one-time pad type cipher:

$$x_n = \begin{cases} 1 & \text{for } f(\boldsymbol{b}_n, \boldsymbol{x}_n) \in [A, B)\,, \\ 0 & \text{for } f(\boldsymbol{b}_n, \boldsymbol{x}_n) \notin [A, B)\,, \end{cases}$$

where $\boldsymbol{b}_n$ is the secret, $\boldsymbol{x}_n$ is random and the interval $[A, B)$ satisfies $g(B) - g(A) = \frac{1}{2}$.

Part 2 of this paper is devoted to the study of a.d.f. $g(t)$ of the sequence $f(\boldsymbol{b}_n, \boldsymbol{x}_n)$, where f is defined by the scalar product $f(\boldsymbol{b}, \boldsymbol{x}) = \boldsymbol{b} \cdot \boldsymbol{x}$ and $K = [0, 1]^s$. For $s = 1, 2, 3$ and $t \in [0, 1]$ we will compute $g(t)$ explicitly.

In Part 3 we study a.d.f. $g(t)$ of the sequence $f\left(\boldsymbol{b}_n^{(1)}, \boldsymbol{b}_n^{(2)}, \ldots, \boldsymbol{b}_n^{(s-1)}, \boldsymbol{x}_n\right)$, $n = 1, 2, \ldots$, where f is defined by absolute value of the mixed product (i.e. the determinant)

$$f\left(\boldsymbol{b}^{(1)}, \ldots, \boldsymbol{b}^{(s-1)}, \boldsymbol{x}\right) = \left|\det\left(\boldsymbol{b}^{(1)}, \ldots, \boldsymbol{b}^{(s-1)}, \boldsymbol{x}\right)\right|,$$

where the vectors belong to the ball $K = B(r)$ in $\mathbb{R}^s$ with center $(0, \ldots, 0)$ and radius r. We give $g(t)$ explicitly, for $s = 1, 2, 3$.

In Part 4 we describe a modification of one-time pad cipher, having private vector sequence $\boldsymbol{b}_n$ and matrix sequence $\mathbf{A}_n$. Contrary to the classical one-time pad, in this case, $\boldsymbol{b}_n$, $\mathbf{A}_n$ can be securely applied many times. In Part 5 some other modifications are also given. A cryptanalysis of such modifications will be discussed in a forthcoming paper.

2. Sequence of scalar products of vectors in cubes

Define

$$g_s(t) = \left|\left\{(\boldsymbol{b}, \boldsymbol{x}) \in [0, 1]^{2s} : \ \boldsymbol{b} \cdot \boldsymbol{x} < t\right\}\right|, \qquad t \in [0, s]\,.$$

For $s = 1$ we have

$$g_1(t) = t - t \log t\,, \qquad t \in [0, 1]\,,$$

[1] This paper has been presented during Journées Tchéco-Slovaco-Francaises, Saint-Etienne, April 4–5, 2002; and TATRACRYPT 2003, Bratislava, June 26–28, 2003.

with the density $g_1'(t) = -\log t$. The $g_s(t)$ is an a.d.f. of the sequence

$$\boldsymbol{b}_n \cdot \boldsymbol{x}_n = \sum_{i=1}^{s} b_{n,i} x_{n,i}, \qquad n = 1, 2, \dots,$$

where $\boldsymbol{b}_n = (b_{n,1}, \dots, b_{n,s})$ and $\boldsymbol{x}_n = (x_{n,1}, \dots, x_{n,s})$ are statistically independent and u.d. in $[0,1]^s$. Since the s-dimensional sequence

$$(b_{n,1}x_{n,1}, \dots, b_{n,s}x_{n,s})$$

also has statistically independent coordinates, it has a.d.f. $g(\boldsymbol{t})$, $\boldsymbol{t} = (t_1, \dots, t_s)$, of the form

$$g(\boldsymbol{t}) = (t_1 - t_1 \log t_1) \cdots (t_s - t_s \log t_s)$$

which gives

$$g_s(t) = (-1)^s \int\limits_{\substack{t_1+\cdots+t_s<t \\ 0\le t_1\le 1, \dots, 0\le t_s\le 1}} 1 \cdot \log t_1 \cdots \log t_s \, \mathrm{d}t_1 \cdots \mathrm{d}t_s .$$

In particular, for any decomposition $S_1 \cup S_2 = \{1, \dots, s\}$, the coordinates of the sequence

$$\left(\sum_{i \in S_1} b_{n,i} x_{n,i}, \sum_{i \in S_2} b_{n,i} x_{n,i} \right)$$

are also statistically independent. Thus

$$g_s(t) = \int\limits_{x+y<t} 1 \cdot \mathrm{d}g_j(x) \, \mathrm{d}g_{s-j}(y)$$

and the Fig. 1

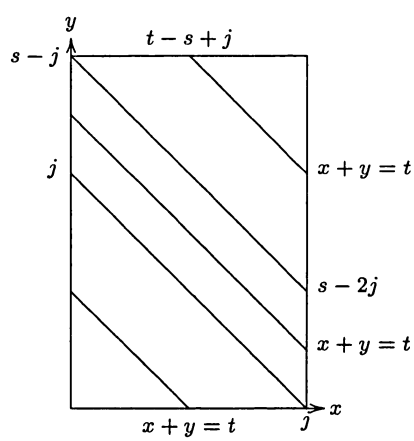

FIGURE 1.

implies that

$$g_s(t) = \begin{cases} \int\limits_0^t \mathrm{d}g_j(x) \int\limits_0^{t-x} \mathrm{d}g_{s-j}(y) & \text{for } t \in [0,j]\,, \\ \int\limits_0^j \mathrm{d}g_j(x) \int\limits_0^{t-x} \mathrm{d}g_{s-j}(y) & \text{for } t \in [j,s-j]\,, \\ \int\limits_0^{t-s+j} \mathrm{d}g_j(x) + \int\limits_{t-s+j}^j \mathrm{d}g_j(x) \int\limits_0^{t-x} \mathrm{d}g_{s-j}(y) & \text{for } t \in [s-j,s] \end{cases}$$

for $j \le s-j$. Its densities are

$$g_s'(t) = \begin{cases} \int\limits_0^t g_j'(x) g_{s-j}'(t-x)\,\mathrm{d}x & \text{for } t \in [0,j]\,, \\ \int\limits_0^j g_j'(x) g_{s-j}'(t-x)\,\mathrm{d}x & \text{for } t \in [j,s-j]\,, \\ \int\limits_{t-s+j}^j g_j'(x) g_{s-j}'(t-x)\,\mathrm{d}x & \text{for } t \in [s-j,s]\,. \end{cases} \tag{1}$$

Applying (1) we find:

THEOREM 1. *For $t \in [0,1]$,*

$g_2(t) = \frac{t^2}{2}\left((\log t)^2 - 3\log t + \frac{7}{2} - \frac{1}{6}\pi^2\right)$,

$g_3(t) = \frac{t^3}{27}\left(-\frac{9}{2}(\log t)^3 + \frac{99}{4}(\log t)^2 + \left(-\frac{255}{4} + \frac{9}{4}\pi^2\right)\log t + \frac{575}{8} - \frac{33}{8}\pi^2 - 9\zeta(3)\right)$,

where $\zeta(s)$ is the classical Riemann's zeta function.

Applying substitution $x_i = \frac{t_i}{t}$, $i = 1,2,\ldots,s$, for $t \in (0,1)$, L. Habsieger (Bordeaux) found (personal communication) that

$$\begin{aligned} g_s(t) &= (-1)^s t^s \int\limits_{\substack{x_1+\cdots+x_s<1 \\ 0\le x_1<1,\ldots,0\le x_s<1}} (\log t + \log x_1)\cdots(\log t + \log x_s)\,\mathrm{d}x_1\cdots\mathrm{d}x_s \\ &= (-1)^s t^s \sum_{j=0}^{s} \binom{s}{j} (\log t)^{s-j} \tilde{g}_j\,, \end{aligned}$$

and then using substitution $x_1 + \cdots + x_j = 1 - y_1 \cdots y_j$, he found

$$\begin{aligned} \tilde{g}_j &= \int\limits_{\substack{x_1+\cdots+x_s<1 \\ 0\le x_1<1,\ldots,0\le x_s<1}} \log x_1 \cdots \log x_j\,\mathrm{d}x_1\cdots\mathrm{d}x_j \\ &= \frac{1}{(s-j)!} \int\limits_{[0,1]^j} \prod_{i=1}^{j} \left(\log y_1 + \cdots + \log y_{j-1} + \log(1-y_j)\right) y_1^{s-1}\cdots y_j^{s-j}\,\mathrm{d}y_1\cdots\mathrm{d}y_j\,. \end{aligned}$$

He also observed that $\tilde{g}_j$ is a composition of integrals

$$\int_0^1 (\log x)^m x^n \,\mathrm{d}x = \frac{(-1)^m m!}{(n+1)^{m+1}},$$

$$\int_0^1 (\log x)^m x^n \log(1-x)\,\mathrm{d}x = (-1)^{m+1} m! \sum_{k=1}^{\infty} \frac{1}{k(k+n+1)^{m+1}}$$

$$= a_0 + a_1\zeta(2) + \cdots + a_m\zeta(m+1) \quad \text{for some } a_i \in \mathbb{Q}.$$

Remark 1. The explicit form of $g_s(t)$, for $t \in [1, s]$, is open even for $s = 2, 3$.

3. Sequences of mixed products of vectors in balls

Let $K = B(r)$ be the s-dimensional ball with center $(0, \ldots, 0)$ and radius r. Consider the d.f.

$$g_s(r,t) = \frac{\left|\{(\boldsymbol{b}^{(1)}, \ldots, \boldsymbol{b}^{(s-1)}, \boldsymbol{x}) \in B^s(r) : \ |\det(\boldsymbol{b}^{(1)}, \ldots, \boldsymbol{b}^{(s-1)}, \boldsymbol{x})| < t\}\right|}{|B(r)|^s}$$

for $t \in [0, r^s]$. It can be seen that for

$$\lambda = \frac{t}{r^s}$$

there exists d.f. $\tilde{g}_s(\lambda)$ such that

$$g_s(r,t) = \tilde{g}_s(\lambda), \qquad \lambda \in [0,1].$$

The d.f. $\tilde{g}_s(\lambda)$ can be found directly from the definition and also via the following application of Crofton's theorem (cf. [KM; pp. 25–27]): Let

$$g_s^*(r,t) =$$
$$= \frac{\left|\{(\boldsymbol{b}^{(1)}, \ldots, \boldsymbol{b}^{(s-1)}) \in B^{s-1}(r) : \ |\boldsymbol{x}| = r, \ \boldsymbol{x} \text{ — fixed}, |\det(\boldsymbol{b}^{(1)}, \ldots, \boldsymbol{b}^{(s-1)}, \boldsymbol{x})| < t\}\right|}{|B(r)|^{s-1}},$$

where $|\boldsymbol{x}|$ is the norm of $\boldsymbol{x}$. Then the d.f. $g_s(r,t)$ and $g_s^*(r,t)$ satisfy

$$\frac{\mathrm{d}g_s(r,t)}{\mathrm{d}r} = s\big(g_s^*(r,t) - g_s(r,t)\big)\frac{\mathrm{d}|B(r)|}{\mathrm{d}r}\frac{1}{|B(r)|}. \tag{2}$$

Using these two methods we find:

THEOREM 2. *For $\lambda \in [0,1]$ we have*

$$\tilde{g}_2(\lambda) = \frac{2}{\pi}\left(1+2\lambda^2\right)\arcsin\lambda + \frac{6}{\pi}\lambda\sqrt{1-\lambda^2} - 2\lambda^2\,,$$

$$\tilde{g}_3(\lambda) = 1 + \frac{9}{4}\lambda\int_{\lambda}^{1}\frac{\arccos x}{x}\,\mathrm{d}x - \frac{3}{4}\lambda^3\arccos\lambda - \sqrt{1-\lambda^2} + \frac{7}{4}\lambda^2\sqrt{1-\lambda^2}\,,$$

where the final integral cannot be expressed in the form of a finite combination of elementary functions.[2]

P r o o f .

For $\tilde{g}_2(\lambda)$: Put

$$\boldsymbol{b} = (b\cos\beta, b\sin\beta) = (b_1, b_2)\,,$$
$$\boldsymbol{x} = (x\cos\alpha, x\sin\alpha)\,.$$

Then

$$|\det(\boldsymbol{b},\boldsymbol{x})| = |bx\sin(\alpha-\beta)|\,.$$

Putting $x = r$ and $\alpha = 0$ we have

$$|\det(\boldsymbol{b},\boldsymbol{x})| < t \iff |b_2| < \frac{t}{r}\,.$$

Thus

$$g_2^*(r,t) = \frac{\left|\{\boldsymbol{b}\in B(r):\ |b_2| < t/r\}\right|}{\pi r^2}$$

which gives

$$g_2^*(r,t) = \frac{2}{\pi}\arcsin\Big(\frac{t}{r^2}\Big) + \frac{2}{\pi}\Big(\frac{t}{r^2}\Big)\sqrt{1-\Big(\frac{t}{r^2}\Big)^2}\,.$$

Solving the differential equation (2) we find the desired d.f. $\tilde{g}_2(\lambda)$.

For $\tilde{g}_3(\lambda)$: The direct proof is divided into the following steps.

(a) Let $|\boldsymbol{u}_0| = r^2$ (the Euclidean norm), then

$$|\boldsymbol{u}_0\cdot\boldsymbol{z}| = \Big||\boldsymbol{u}_0|\frac{\boldsymbol{u}_0}{|\boldsymbol{u}_0|}\cdot\boldsymbol{z}\Big| < t \iff \Big|\frac{\boldsymbol{u}_0}{|\boldsymbol{u}_0|}\cdot\boldsymbol{z}\Big| < \frac{t}{|\boldsymbol{u}_0|} = \frac{t}{r^2}$$

and for the measure we get

$$\left|\{|\boldsymbol{z}|\le r:\ |\boldsymbol{u}_0\cdot\boldsymbol{z}| < t\}\right| = \begin{cases} 2\pi r^2\left(\frac{t}{r^2}\right) - \frac{2}{3}\pi\left(\frac{t}{r^2}\right)^3 & \text{for } \frac{t}{r^2}\le r\,,\\ \frac{4}{3}\pi r^3 & \text{for } \frac{t}{r^2} > r\,.\end{cases}$$

[2] Cf. [RG; p. 122].

(b) Given vector $\boldsymbol{u}_0$, $|\boldsymbol{u}_0| = r^2$, and $\theta \in [0,1]$, define $\boldsymbol{u} = \theta \boldsymbol{u}_0$, then using (a) we get that the set $\{|\boldsymbol{z}| \leq r : \ |\boldsymbol{u} \cdot \boldsymbol{z}| < t\}$ has the measure

$$\left|\{|\boldsymbol{z}| \leq r : \ |\boldsymbol{u}_0 \cdot \boldsymbol{z}| < \tfrac{t}{\theta}\}\right| = \begin{cases} 2\pi r^2 \left(\frac{t}{\theta r^2}\right) - \frac{2}{3}\pi \left(\frac{t}{\theta r^2}\right)^3 & \text{for } \frac{t}{r^3} \leq \theta, \\ \frac{4}{3}\pi r^3 & \text{for } \frac{t}{r^3} > \theta. \end{cases}$$

(c) For vectors $\boldsymbol{u}_0$, $|\boldsymbol{u}_0| = r^2$, and $\boldsymbol{x}_0$, $|\boldsymbol{x}_0| = r$, $\boldsymbol{u}_0 \cdot \boldsymbol{x}_0 = 0$, define $\boldsymbol{u} = \theta \boldsymbol{u}_0$ for fixed $\theta \in [0,1]$ and $\boldsymbol{x} = \theta_1 \boldsymbol{x}_0$ with $\theta_1 \in [0,1]$. Every solution of the equation $\boldsymbol{u} = \boldsymbol{x} \times \boldsymbol{y}$ such that $|\boldsymbol{y}| \leq r$ has the form

$$\boldsymbol{y} = \frac{\boldsymbol{u} \times \boldsymbol{x}}{|\boldsymbol{x}|^2} + \alpha \boldsymbol{x},$$

where α is any real number for which $|\boldsymbol{y}| \leq r$. Since

$$\left|\frac{\boldsymbol{u} \times \boldsymbol{x}}{|\boldsymbol{x}|^2}\right| = \frac{|\boldsymbol{u}|}{|\boldsymbol{x}|} = \frac{\theta r^2}{\theta_1 r} = \frac{\theta}{\theta_1} r,$$

and the minimum of $(\theta r)/\theta_1$ is attained at $\theta_1 = 1$, it can be seen that all solutions $\boldsymbol{y}$, $|\boldsymbol{y}| \leq r$, form a circle segment with height $r - \theta r$ and thus

$$\left|\{|\boldsymbol{y}| \leq r : \ \boldsymbol{u} = \boldsymbol{x} \times \boldsymbol{y}, \ \boldsymbol{u} = \theta \boldsymbol{u}_0, \ \boldsymbol{x} = \theta_1 \boldsymbol{x}_0, \ \theta_1 \in [0,1]\}\right| = r^2 \left(\arccos\theta - \theta\sqrt{1-\theta^2}\right).$$

(d) Since $\left|\{|\boldsymbol{x}_0| = r : \ \boldsymbol{u}_0 \cdot \boldsymbol{x}_0 = 0, \ \boldsymbol{u}_0 \text{ — fixed}\}\right| = 2\pi r$, we have

$$\left|\{(\boldsymbol{x}, \boldsymbol{y}) \in B(r) : \ \boldsymbol{x} \times \boldsymbol{y} = \theta \boldsymbol{u}_0, \ \boldsymbol{u}_0 \text{ — fixed}\}\right| = 2\pi r^3 \left(\arccos\theta - \theta\sqrt{1-\theta^2}\right)$$

and putting $\left|\{|\boldsymbol{u}_0| = r^2\}\right| = M$ we find that

$$g_3(r,t) = \frac{M}{\left(\frac{4}{3}\pi r^3\right)^3} \left[\frac{4}{3}\pi r^3 \int_0^{\frac{t}{r^3}} 2\pi r^3 \left(\arccos\theta - \theta\sqrt{1-\theta^2}\right) \mathrm{d}\theta \right.$$
$$\left. + \int_{\frac{t}{r^3}}^{1} 2\pi r^3 \left(\arccos\theta - \theta\sqrt{1-\theta^2}\right) \left(2\pi r^2 \left(\frac{t}{\theta r^2}\right) - \frac{2}{3}\pi \left(\frac{t}{\theta r^2}\right)^3\right) \mathrm{d}\theta \right].$$

Norming $g_3(r,t) = 1$ for $t = r^3$ we find $M = \frac{4}{3}\pi r^3$ which gives the desired $\tilde{g}_3(\lambda)$. □

Remark 2. Note that in a direct proof for $\tilde{g}_2(\lambda)$ the fact can be used that if the sequence $(\boldsymbol{b}_n, \boldsymbol{x}_n)$ is u.d. in $B(r)^2$ and

$$\boldsymbol{b}_n = (b_n \cos\beta_n, b_n \sin\beta_n),$$
$$\boldsymbol{x}_n = (x_n \cos\alpha_n, x_n \sin\alpha_n),$$

then the coordinate sequence

$$(b_n, x_n, \beta_n, \alpha_n)$$

has a.d.f.

$$g(x,u,y,v) = \frac{x^2}{r^2}\frac{u^2}{r^2}\frac{y}{2\pi}\frac{v}{2\pi}$$

defined on $[0,r] \times [0,r] \times [0,2\pi] \times [0,2\pi]$.

Remark 3. For possible control of $g_3(r,t)$ via Crofton's theorem, we have

$$g_3^*(r,t) = 1 + \frac{3}{2}\lambda \int_{\lambda}^{1} \frac{\arccos x}{x}\,\mathrm{d}x + \frac{3}{4}\lambda^3 \arccos\lambda - \sqrt{1-\lambda^2} + \frac{1}{4}\lambda^2\sqrt{1-\lambda^2}\,,$$

where $\lambda = \frac{t}{r^3}$.

Remark 4. As mentioned, the explicit form of $\tilde{g}_s(\lambda)$ for $s > 3$ is unknown. Also the form of d.f. is open if we replace s-dimensional ball $K = B(r)$ by the unit cube $K = [0,1]^s$.

4. A modified one-time pad cipher

(I) Two users X and Y agree on the

- private vector sequence

$$\boldsymbol{b}_n\,, \qquad n = 1,2,\ldots,N\,,$$

in $K \subset \mathbb{R}^s$,

and

- private sequence of regular $(s+1) \times (s+1)$ real matrices

$$\mathbf{A}_n\,, \qquad n = 1,2,\ldots,N\,,$$

where N is sufficiently large,

and

- continuous function

$$f(\boldsymbol{b},\boldsymbol{x}) \qquad \text{for} \quad \boldsymbol{b},\boldsymbol{x} \in K\,,$$

where the values $f(\boldsymbol{b},\boldsymbol{x})$ form an interval $[A_0, B_0]$.

The users compute the d.f.

$$g(t) = \frac{\left|\{(\boldsymbol{b}, \boldsymbol{x}) \in K^2 : \ f(\boldsymbol{b}, \boldsymbol{x}) < t\}\right|}{|K|^2} \qquad \text{for} \quad t \in [A_0, B_0]$$

and select an interval $[A, B) \subset [A_0, B_0]$ such that

$$g(B) - g(A) = \frac{1}{2}.$$

The interval $[A, B)$ is also private.

(II) If X wants to send a message written as 0–1 sequence (i.e. the plaintext digits)

$$u_n, \qquad n = 1, 2, \ldots, N,$$

to Y, he does the following steps:

- X selects a random (or pseudo-random) sequence of vectors $\boldsymbol{x}_n$, $n = 1, 2, \ldots, N$, in the region K.
- X computes enciphering sequence (the key digits)

$$x_n = \begin{cases} 1 & \text{for } f(\boldsymbol{b}_n, \boldsymbol{x}_n) \in [A, B), \\ 0 & \text{for } f(\boldsymbol{b}_n, \boldsymbol{x}_n) \notin [A, B). \end{cases} \tag{3}$$

- X enciphers u_n to the sequence (ciphertext digits)

$$y_n = u_n + x_n \pmod 2, \qquad n = 1, 2, \ldots, N.$$

- X mixes the sequence $(\boldsymbol{x}_n, y_n)$ of $s+1$-dimensional vectors by matrices $\mathbf{A}_n$ to

$$\boldsymbol{z}_n^T = \mathbf{A}_n \cdot (\boldsymbol{x}_n, y_n)^T,$$

and then sends $\boldsymbol{z}_n$ to Y through public line.

(III) Y decrypts the received ciphertext as follows:

- Y decomposes $\boldsymbol{z}_n$ applying formula

$$(\boldsymbol{x}_n, y_n) = \mathbf{A}_n^{-1} \cdot \boldsymbol{z}_n^T.$$

- Using $\boldsymbol{x}_n$ he computes x_n in the same manner as X.
- He finds the plaintext digits

$$u_n = y_n + x_n \pmod 2, \quad n = 1, 2, \ldots, N.$$

Remark 5. In the classical one-time pad cipher (i.e. Vernam cipher, cf. [MvV; Chap. 6]), two users X and Y have a common private 0–1 key sequence x_n, $n = 1, 2, \ldots, N$, and X sends the 0–1 plaintext sequence u_n, $n = 1, 2, \ldots, N$, to Y as cipertext sequence $y_n = u_n + x_n \pmod 2$. If u_n is disclosed, and since y_n through public line, the key sequence x_n is also disclosed. Thus a secure application of x_n is only one time. Now, assume that

- $\mathbf{A}_n$, $n = 1, 2, \ldots, N$,
- u_n, $n = 1, 2, \ldots, N$,
- $[A, B)$

are disclosed. Then (since $\boldsymbol{z}_n$, $n = 1, 2, \ldots, N$, through public line) $\boldsymbol{x}_n$ and x_n also are disclosed, and for secret $\boldsymbol{b}_n$, $n = 1, 2, \ldots$, we have only

$$\boldsymbol{b}_n \in f^{-1}([A, B), \boldsymbol{x}_n) \qquad \text{or} \qquad \boldsymbol{b}_n \notin f^{-1}([A, B), \boldsymbol{x}_n),$$

where $f^{-1}(I, \boldsymbol{x}) = \{\boldsymbol{b} \in K : f(\boldsymbol{b}, \boldsymbol{x}) \in I\}$. Therefore $\boldsymbol{b}_n$ can be used several times. The detail security analysis will be investigated in our forthcoming paper. For the quality of the key sequence x_n we only note that any given 0–1 u.d. sequence x_n can be constructed by (3) using suitable u.d. $\boldsymbol{b}_n$ and $\boldsymbol{x}_n$.

5. Other modifications

(A) The cryptosystem of Part 4 can be modified taking a function $f(\boldsymbol{b}^{(1)}, \ldots, \boldsymbol{b}^{(s-1)}, \boldsymbol{x})$ and vector sequence $(\boldsymbol{b}_n^{(1)}, \ldots, \boldsymbol{b}_n^{(s-1)}, \boldsymbol{x}_n)$ in K^s, where

- $(\boldsymbol{b}_n^{(1)}, \ldots, \boldsymbol{b}_n^{(s-1)})$ is a common secret sequence for both users X and Y;
- $\boldsymbol{x}_n$ is a random choice sequence for X;
- The enciphering sequence is computed by

$$x_n = \begin{cases} 1 & \text{for } f(\boldsymbol{b}_n^{(1)}, \ldots, \boldsymbol{b}_n^{(s-1)}, \boldsymbol{x}_n) \in [A, B), \\ 0 & \text{for } f(\boldsymbol{b}_n^{(1)}, \ldots, \boldsymbol{b}_n^{(s-1)}, \boldsymbol{x}_n) \notin [A, B), \end{cases}$$

where $g(B) - g(A) = \frac{1}{2}$ and

$$g(t) = \frac{\left|\{(\boldsymbol{b}^{(1)}, \ldots, \boldsymbol{b}^{(s-1)}, \boldsymbol{x}) \in K^s : f(\boldsymbol{b}^{(1)}, \ldots, \boldsymbol{b}^{(s-1)}, \boldsymbol{x}) < t\}\right|}{|K^s|}.$$

Note that the function f involving determinant as in Part 3, can be used.

(B) A further modification of one-time pad is as follows:

- The users X and Y have a common secret sequence

$$(\boldsymbol{b}_n^{(1)}, \ldots, \boldsymbol{b}_n^{(s-2)}), \qquad n = 1, 2, \ldots.$$

Before the encryption of a message, users X and Y exchange through public line two sequences $\boldsymbol{x}_n$ and $\boldsymbol{y}_n$ computed as follows:

- X selects $\boldsymbol{x}_n^{(s-1)}$ randomly;
- Y selects $\boldsymbol{x}_n^{(s)}$ randomly;
- X sends to Y through public line a sequence of vectors

$$\boldsymbol{x}_n = \begin{vmatrix} \boldsymbol{i}_1 & \ldots & \boldsymbol{i}_s \\ b_{n,1}^{(1)} & \ldots & b_{n,s}^{(1)} \\ \vdots & \ddots & \vdots \\ b_{n,1}^{(s-2)} & \ldots & b_{n,s}^{(s-2)} \\ x_{n,1}^{(s-1)} & \ldots & x_{n,s}^{(s-1)} \end{vmatrix},$$

where $\boldsymbol{i}_1, \boldsymbol{i}_2, \ldots, \boldsymbol{i}_s$ are s-dimensional unit vectors and $\boldsymbol{b}_n^{(i)} = (b_{n,1}^{(i)}, b_{n,2}^{(i)}, \ldots, b_{n,s}^{(i)})$;

- Y sends to X through public line the sequence

$$\boldsymbol{y}_n = \begin{vmatrix} \boldsymbol{i}_1 & \ldots & \boldsymbol{i}_s \\ b_{n,1}^{(1)} & \ldots & b_{n,s}^{(1)} \\ \vdots & \ddots & \vdots \\ b_{n,1}^{(s-2)} & \ldots & b_{n,s}^{(s-2)} \\ x_{n,1}^{(s)} & \ldots & x_{n,s}^{(s)} \end{vmatrix};$$

- X and Y compute the common sequence of absolute values of scalar products

$$v_n = \left|\boldsymbol{x}_n \cdot \boldsymbol{x}_n^{(s)}\right| = \left|\boldsymbol{y}_n \cdot \boldsymbol{x}_n^{(s-1)}\right|;$$

- X and Y compute the key sequence x_n by

$$x_n = \begin{cases} 1 & \text{for } v_n \in [A, B), \\ 0 & \text{for } v_n \notin [A, B), \end{cases}$$

where $g(B) - g(A) = \frac{1}{2}$ and $g(t) = g_s(r, t)$ as in Part 3.

It can be proved that this method is equivalent to the method of Part 4 with scalar product, without scrambling matrices and having s^2-dimensional vectors.

(C) In all of the above modifications, the intervals $[A, B)$ can also be replaced by m non-overlapping intervals $[A_i, B_i)$, $i = 1, 2, \ldots, m$, satisfying

$$\sum_{i=1}^{m} g(B_i) - g(A_i) = \frac{1}{2}.$$

6. Acknowledgement

The author expresses many thanks INNA Ltd. (Prague), especially F. Krincvaj and I. Trtík, for their assistance at the implementation of the cryptosystem described in Part 4 and based on $g_3(t)$.

REFERENCES

[DT] DRMOTA, M.—TICHY, R. F.: *Sequences, Discrepancies and Applications.* Lecture Notes in Math. 1651, Springer-Verlag, Berlin-Heidelberg, 1997.

[KM] KENDALL, D. G.—MORAN, P. A. P.: *Geometrical Probabilities* (Russian translation), Izd. Nauka, Moscow, 1972.

[MvV] MENEZES, A.—OORSCHOT, P. van—VANSTONE, S.: *Handbook of Applied Cryptography*, CRC Press (electronic version), 1996.

[RG] RYSHIK, I. M.—GRADSTEIN, I. S.: *Tables of Series, Products, and Integrals* (Translation from the Russian, Moscow, 1951), VEB Deutscher Verlag der Wissenschaften, Berlin, 1957.

Received September 5, 2003
Revised October 2, 2003

Mathematical Institute
Slovak Academy of Sciences
Štefánikova 49
SK–814 73 Bratislava
SLOVAKIA

E-mail: strauch@mat.savba.sk