ON ROTATION GROUP AND ENCRYPTION OF ANALOG SIGNALS

Su-shing Chen

University of Florida
Gainesville, Florida 32611, U.S.A.

INTRODUCTION

The problem of generating random elements in groups has direct application to cryptography. For instance, we like to know whether the DES permutations are random permutations of the 2^{64} possible 64-bit words. The whole symmetric group is known to be generated by certain k-functions (7). Another example is the Wyner voice encryption scheme (12) which requires the production of large numbers of random real orthogonal matrices. N. J. A. Sloane has given a survey on this problem (11) which has led to the following questions for a given group G:

1. How does one generate elements of G at random ?
2. How can one test if certain given elements of G really are random ?
3. Does a given subset H generate the whole group G ?
4. If so, how long does it take ?

In this paper, we consider these questions for the orthogonal group O(d) for any positive integer d. By looking at the Lie algebra o(d) of O(d) and one-parameter subgroups of O(d), we can find the generation of an arbitrary element in terms of one-parameter rotation groups in uniform fashion. The length of generation can be determined. Random elements are generated using random number generator on the real parameter space of each one-parameter subgroup.

The structural theory of Lie groups and other groups seems to be useful to cryptography. For groups which are not Lie, one may try to embed them into Lie groups. The transformation group theory and ergodic theory emerge to be also very useful. Ergodic theory can be considered to be a generalization of

G.R. Blakley and D. Chaum (Eds.): Advances in Cryptology - CRYPTO '84, LNCS 196, pp. 95-100, 1985.

the existing probabilistic and statistical methods. We certainly owe the idea to Shannon in his classic paper in 1949 (11) on the mixing property of two non-commuting operations on some space. We only have to find an operation which is the iteration of these two operations to a certain high degree to achieve relatively mixing situation in the space. We may point out that a quite simple group, such as the real numbers, can act on a space in a very complicated way to yield a good cryptosystem. RSA system can be considered in this manner (4) as a transformation semigroup.

ENCRYPTION OF ANALOG SIGNALS

Wyner's voice encryption scheme offers high fidelity and high security to encrypting voice signals over telephone lines. The technique is applicable to other analog signals. For the space of approximately bandlimited sequences $(a(1),\ldots,a(N))$, there is known basis $x_1,\ldots,x_d$, $d \approx 2WN$, where $W < 1/2$ is the bandwidth, called discrete prolate spheroidal sequences (11). Each waveform is sampled every T seconds, where T is less than the Nyquist rate. We take a finite segment $a = (a(1),\ldots,a(N))$ of the sampled sequence and express it by

$$a = \sum_{j=1}^{d} a_j x_j,$$

where the coefficients are determined in the standard way and N is large enough to contain most of the energy in the given waveform.

The scrambling or encrypting is performed by multiplying the coefficient vector $(a_1,\ldots,a_d)$ by a secret d by d orthogonal matrix Q, obtaining

$$(b_1,\ldots,b_d) = (a_1,\ldots,a_d)Q.$$

The encrypted sequence is

$$b = \sum_{j=1}^{d} b_j x_j,$$

from which the encrypted waveform can be formed. The encrypted waveform has the

same bandwidth and approximately the same energy as the original waveform. Wyner has shown that if N and d are large enough and matrices Q are chosen independently and uniformly from the orthogonal group, then his scheme offers essentially perfect security (11), (12).

THE ORTHOGONAL GROUP

The orthogonal group O(d) acting on the d-dimensional Euclidean vector space can be characterized by the preservation of the Euclidean inner product. The group O(d) is a Lie group and a Lie subgroup of the general linear group GL(d) of all nonsingular matrices. The manifold (Lie group) structure of GL(d) comes from the Euclidean vector space R^{2d} as an open subset. For each Lie group G, there is a Lie algebra $\underline{g}$ which is a vector space together with a Lie product $[\ ,\ ]$. For matrix Lie groups, the Lie product is the commutator $[X,Y] = XY - YX$, where X and Y are just matrices in R^{2d}. It is easy to see that the Lie algebra of GL(d) is R^{2d}. The key point is that the exponential mapping exp(tX) brings an element X in the Lie algebra $\underline{g}$ to an element exp(tX) in the Lie group G. For matrix Lie groups,

$$\exp(tX) = 1 + (tX) + (t^2X^2)/2! + \ldots,$$

where X is any element of in $\underline{g}$. The set of exp(tX) for all t in R is a one-parameter subgroup in G and the derivative of exp(tX) at t=0 is X. Thus X is the velocity at t=0 of the group exp(tX).

The orthogonal group O(d) and its Lie algebra o(d) are well known including their complete structures and associated mathematical invariants. The group O(d) is not connected and has two connected components; those having determinant +1 form SO(d), while those having determinant -1 form the other component which is not a group because the identity matrix is not in it. The dimension of SO(d) as well as O(d) is d(d-1)/2. The dimension of the Lie algebra o(d) is that of O(d). Indeed, the Lie algebra o(d) is also the Lie algebra of SO(d). The classification of Lie subgroups of a simple Lie group is important to our consideration (3).

RANDOM GENERATION

If we take a set of one-parameter groups $\exp(tX_1),\ldots,\exp(tX_m)$, all the finite products of elements from these groups generate an arcwise connected subgroup of SO(d). By Yamabe's theorem, it is a Lie subgroup. For m large enough, it contains a maximal subgroup and has to be the whole group SO(d). For example, SO(3) has no 2-dimensional Lie subgroup and m = 2 will be sufficient. Thus up to one-parameter subgroups, question 3. of Sloane is answered. Question 4. is answered by finding a positive integer n such that every element of SO(d) can be expressed as a product of elements selected from the given set of one-parameter subgroups and the length is at most n and by determining the minimal n over the collection of all such sets of one-parameter groups. Note that n depends on the choice of the set of one-parameter groups.

The first part is answered easily. Let S_n be all products of lengths less than or equal to n. S_n is compact and SO(d) is the union of S_n for all positive n. By the Baire category theorem, some S_m contains an open set whose translates cover SO(d). This open cover has a finite subcover and the result is proved. To determine the number n for a given set of groups is rather complicated. One needs to study the geometry of the (d-1)-sphere S^{d-1} on which SO(d) acts and uses some mathematics in (3). The minimal number n can be shown to be d(d-1)/2.

In order to generate random elements, we generate random numbers on the real parameters. First, we generate random numbers on the interval $[0,1]$. By iteration, we get the whole real parameter space. The transition from SO(d) to O(d) is easy. The index of O(d) over SO(d) is two.

Since a direct product of low dimensional orthogonal groups is a subgroup of a higher dimensional one, we may increase the speed of encryption by segmenting the signal, applying lower dimensional groups and globally scrambling segments. This scheme provides a trap door for the system.

The advantage of our encryption system is that the set of one-parameter groups is fixed once for all as well as the form of the random orthogonal matrix.

This constancy is useful to hardwire the box to eliminate the intensive computation for generating a random orthogonal matrix. The pseudo-random scheme (11) using Hadamard matrices does not seem to generate truly random matrices. It is proved that for d greater than or equal to 8, the subgroup $\dot{G}$ generated by the set S is topologically dense in O(d), where S is a certain set of matrices (11). For d = 8, the cardinality of S is 4954521600. For d = 48, the cardinality becomes 1.1765... times 10^{146}. We like to point out that the length of a finite product in the topological closure may have to be extremely large.

Finally, we may introduce other trap doors to our system to increase the speed of encryption, but our opponent still need to decrypt the signal randomly. One may use pseudo-random number generators, partial products of one-parameter subgroups or other structural constraints of Lie groups. The structure of Lie groups is very elegant and simple on one hand as we have seen above. On the other hand, extremely hairy situation may occur. For instance, we can embed a free group of two generators in a compact Lie group. Then this subset contains a free subgroup of infinitely many generators. Anyway, I agree with G. R. Blakley (2) that group theory offers a lot of opportunity for cryptologists to explore.

REFERENCES

1. R. Bernhard, Breaching system security, IEEE Spectrum, 19 (1982), 24-31.
2. G. R. Blakley, Information theory without the finiteness assumption, I: Cryptosystems as group-theoretic objects, Crypto '84 Conference.
3. S. Chen and L. Greenberg, Hyperbolic spaces, Contribution to Analysis, Papers dedicated to L. Bers, Academic Press, 1974, 49-88.
4. S. Chen, Transformation groups and semigroups as cryptosystems, to appear.
5. S. Chen and R. Yoh, The category of generalized Lie groups, Trans. Amer. Math. Soc., 199 (1974), 281-294.
6. B. S. Kaliski, jr., Wyner's speech scrambler, Crypto '84 Conference.

7. A. G. Konheim, Cryptography: A Primer, John-Wiley & Sons, 1981.

8. N. R. F. MacKinnon, The development of speech encipherment, Radio and Electronic Engineer, 50 (1980), 147-155.

9. J. Reeds, Cracking a random number generator, Cryptologia, 1 (1977), 20-26.

10. D. Slepian, Prolate spheroidal wave functions, fourier analysis, and uncertain-ty, Part V: the discrete case, Bell System Tech. Journal, 57 (1978), 1371-1430.

11. N. J. A. Sloane, Encrypting by random rotations, Cryptography, T. Beth Ed., Springer-Verlag, Lecture Notes in Computer Sciences, 1983, 71-128.

12. A. D. Wyner, An analog scrambling scheme which does not expand bandwidth, Part I: discrete time, IEEE Trans. Information Theory, IT-25, No. 3, 1979, 261-274.