Tatra Mt. Math. Publ. **37** (2007), 105–112

TATRA MOUNTAINS
Mathematical Publications

ON GENERATION OF RANDOM COVERS FOR FINITE GROUPS

Pavol Svaba — Tran van Trung

ABSTRACT. Covers for finite groups, a generalization of logarithmic signatures, form the basis of the ElGamal-like public-key cryptosystem MST_2. A relevant and open problem about the practical use of covers is the question of how to generate random covers for groups of large order. In this paper we show the connection between this problem and the classical occupancy problem. As a consequence, we can solve the problem of generating random covers for arbitrarily large finite groups completely. We also present several experimental computer results about covers and uniform covers for some alternating groups. These results provide useful hints for generating uniform random covers.

1. Introduction and Preliminaries

Covers for finite groups, which have been introduced in [5], are the basis of the public-key cryptosystem MST_2. The cryptosystem MST_2, which can be viewed as a generalization of the ElGamal cryptosystem for non-abelian groups, makes use of random $[r, s]$-meshes as its public-keys, where $[r, s]$-meshes are a special type of covers. The problem of generating random covers for finite groups is therefore crucial for the realization of MST_2 and for public-key cryptosystems based on random covers (see [5, 2, 3]). To date, this problem remains unsolved. Our aim is to show a connection of this problem with the classical occupancy problem. The connection allows us to derive the probability of deciding whether or not a randomly generated "object" for a given group is a cover. The problem of generating random covers for finite groups of arbitrarily large order can therefore be completely solved. Furthermore, generation of random covers can be done with high efficiency and at minimum cost.

2000 Mathematics Subject Classification: 94A60, 20B05.
Keywords: cover, uniform cover, $[r, s]$-mesh, logarithmic signature, finite group, public-key cryptosystem.

Let $\mathfrak{G}$ be a finite group and let $\mathfrak{X}$ be a subset of $\mathfrak{G}$. Let $\alpha = [A_1, \ldots, A_s]$ be a collection of ordered subsets $A_i = [a_{i1}, a_{i2}, \ldots, a_{ir_i}]$ of $\mathfrak{G}$. We say that α is a *cover* for $\mathfrak{G}$ (resp. for $\mathfrak{X}$) if for each element $g \in \mathfrak{G}$ (resp. $g \in \mathfrak{X}$) there are elements $a_{ij_i} \in A_i$ such that

$$g \quad = \quad a_{1j_1}.a_{2j_2} \ldots a_{sj_s}. \tag{1.1}$$

In particular, if equation (1.1) is unique, then α is called a *logarithmic signature* for $\mathfrak{G}$ (resp. for $\mathfrak{X}$) [4]. Thus, logarithmic signatures are a special form of covers. The vector $(r_1, r_2, \ldots, r_s)$, where $r_i = |A_i|$, is called the *type* of α and the value $\ell = r_1 + \cdots + r_s$ is called the *length* of the cover. For simplicity of discussion we will consider covers for $\mathfrak{G}$.

Let $\alpha = [A_1, \ldots, A_s]$ be a cover of type $(r_1, r_2, \ldots, r_s)$ for $\mathfrak{G}$. Let λ_g denote the number of ways for which an element $g \in \mathfrak{G}$ has a representation given in equation (1.1). Let $\lambda_{min} = \min\{\lambda_g : \ g \in \mathfrak{G}\}$ and $\lambda_{max} = \max\{\lambda_g : \ g \in \mathfrak{G}\}$. The ratio $\lambda := \lambda_{max}/\lambda_{min} \geq 1$ measures the degree of uniformity of α. A cover α is *uniform* if $\lambda \leq 2$. We note here that the reason for taking $\lambda \leq 2$ as bound for uniform covers is that we want to include the case of 1-*quasi logarithmic signatures* [5], for which $\lambda_{min} = 1$ and $\lambda_{max} = 2$. If, however, the value of λ_{min} is large, we shall expect that the ratio λ would be much smaller than 2, namely close to 1, in the above definition. A uniform cover of type $(r_1, \ldots, r_s)$ with $r_i = r$ for all $i = 1, \ldots, s$ is called an $[s, r]$-*mesh*.

2. A bound for random covers

Assume that we are given a collection $\alpha = [A_1, \ldots, A_s]$ of random subsets A_i of a group $\mathfrak{G}$. We want to determine the probability, proving the "covering property" for α. It should be noted that in a real cryptographic application the order of $\mathfrak{G}$ is very large, hence a direct checking of the covering property of α by running through all elements of $\mathfrak{G}$ is obviously impossible.

In what follows we show that the problem is strictly related to a well known problem, the classical occupancy problem (see e.g.[1]), and can therefore be completely solved.

Let $n = |\mathfrak{G}|$ be the order of $\mathfrak{G}$ and let $\alpha = [A_1, \ldots, A_s]$ be an ordered collection of random subsets A_i of $\mathfrak{G}$, i.e., each element of A_i is chosen with probability $1/n$. Let $N = r_1 \times \cdots \times r_s$, where $r_i = |A_i|$. The elements of A_i, $i = 1, \ldots, s$, can be interpreted as a set of randomly chosen elements from $\mathfrak{G}$ with replacement.

The set of all elements $g \in \mathfrak{G}$ which can be expressed by equation (1.1) is said to be created by α. Note that, in general, g can be written in more than one way by equation (1.1). Thus, as with the elements of α, we may assume that the set of elements created by α is a random set of elements of $\mathfrak{G}$. We assign each of n *cells* $1, 2, \ldots, n$ to each of the n elements $g_1, g_2, \ldots, g_n$ of $\mathfrak{G}$. An element $g_i \in \mathfrak{G}$ of the form $g_i = a_{1j_1}.a_{2j_2} \ldots a_{sj_s}$ is interpreted as a *ball* in cell i. Thus the problem becomes the problem of a random distribution of N balls (N elements generated by α) in n cells, where each arrangement has probability n^{-N}. Let $E_{j_1,j_2,\ldots,j_m}$ be the event that elements $g_{j_1}, g_{j_2}, \ldots, g_{j_m} \in \mathfrak{G}$ are not created by α, i.e., $E_{j_1,j_2,\ldots,j_m}$ is the event that cells $j_1, j_2, \ldots, j_m$ are empty. In this event all N balls are placed in the remaining $n - m$ cells, and this can be done in $(n-m)^N$ different ways. Thus $p_{j_1,j_2,\ldots,j_m} = (1 - \frac{m}{n})^N$ is the probability of event $E_{j_1,j_2,\ldots,j_m}$. Set

$$T_m := \binom{n}{m}\left(1 - \frac{m}{n}\right)^N.$$

The method of inclusion and exlusion shows that the probability that at least one cell is empty equals

$$\sum_{i=1}^{n}(-1)^{i-1}T_i = \sum_{i=1}^{n}(-1)^{i-1}\binom{n}{i}\left(1 - \frac{i}{n}\right)^N.$$

Let $p_m(N, n)$ denote the probability that exactly m cells remain empty. Then the probability that all elements of $\mathfrak{G}$ are covered by α (i.e., no cell is empty) is $p_0(N, n)$ and we have

$$p_0(N, n) = \sum_{j=0}^{n}(-1)^j\binom{n}{j}\left(1 - \frac{j}{n}\right)^N. \tag{2.1}$$

Consider now $p_m(N, n)$. Since m cells can be chosen in $\binom{n}{m}$ ways and since each of the remaining $n - m$ cells is occupied, the number of patterns of these distributions is $(n - m)^N p_0(N, n - m)$. Dividing by n^N we obtain $p_m(N, n)$. Thus

$$p_m(N, n) = \binom{n}{m}\sum_{j=0}^{n-m}(-1)^j\binom{n-m}{j}\left(1 - \frac{m+j}{n}\right)^N.$$

Define $\mu := ne^{-N/n}$. It has been shown (see [1]) that if N, $n \to \infty$ but μ remains bounded, then

$$p_m(N, n) - e^{-\mu}\frac{\mu^m}{m!} \to 0$$

for each fixed m. Hence we have

$$p_m(N,n) \approx e^{-\mu}\frac{\mu^m}{m!}$$

for large n.

In particular,

$$p_0(N,n) \approx e^{-\mu}.$$

This implies that for any given value $0 < \nu < 1$ there is an $N_0 \in \mathbb{Z}_+$ such that for any $N \geq N_0$ random covers of type $(r_1, \ldots, r_s)$ with $N = r_1 \times \cdots \times r_s$ can be generated with probability $p_0(N,n) \geq \nu$. This means that we can choose N so that $1 - p_0(N,n)$ is close to 0.

Thus we have the following theorem.

Theorem 2.1. *Let $\mathfrak{G}$ be a finite group with $|\mathfrak{G}| = n$. For any given value $0 < \nu < 1$ there is an $N_0 \in \mathbb{Z}_+$ such that any collection $\alpha = [A_1, \ldots, A_s]$ of random subsets A_i of $\mathfrak{G}$ with $N = |A_1| \times \cdots \times |A_s| \geq N_0$ is a cover for $\mathfrak{G}$ with a probability $p_0(N,n) \geq \nu$. Moreover, for large n we have*

$$p_0(N,n) \approx e^{-\mu},\ \mu = ne^{-\theta},$$

where $\theta := \frac{N}{n}$.

Experimental results in the next section show that even with moderate values of n the error of the approximation of $p_0(N,n)$ in Theorem 2.1 is small.

3. Experimental results for generating random covers

We present the experimental results with the alternating groups $\mathfrak{A}_8$, $\mathfrak{A}_9$ and $\mathfrak{A}_{10}$. For each group $\mathfrak{G} = \mathfrak{A}_i$ and for each *test* we randomly generate 10000 collections $\alpha = [A_1, \ldots, A_s]$ of subsets of $\mathfrak{G}$ of a certain type $(r_1, \ldots, r_s)$, and then count the number of elements of $\mathfrak{G}$ covered by α. We repeat the test for several types of α. Eventually, we obtain the probabilities that α is a cover. The results show that these probabilities are almost identical with those of the theoretical results in Theorem 2.1.

Each line in the table below presents a test (10000 random collections of α). The theoretical bounds for the probabilities $P_m := p_m(N,n)$ and the corresponding test results from the experiment, also denoted by P_m, are in the second and third column, respectively. We are mainly interested in P_0 given in Theorem 2.1. For instance, the second line of the table shows that $\mathfrak{G} = \mathfrak{A}_8$,

$s = 8$, $r_1 = \cdots = r_7 = 5$ and $r_8 = 4$, i.e., $\ell = r_1 + \cdots + r_8 = 39$ and $N = r_1 \times \cdots \times r_8 = 5^7.4$ and $\theta = \frac{N}{n} = 15.5$, where $n = |\mathfrak{A}_8| = \frac{1}{2}8! = 20160$.

					theoretical [%]				experimental [%][1]			
$\mathfrak{G}$	s	ℓ	N	θ	P_0	P_1	P_2	P_3	P_0	P_1	P_2	P_3
$\mathfrak{A}_8$	8	38	$5^6 \cdot 4^2$	12.4	92.0	7.6	0.4	0	90.5	8.6	0.8	0.1
		39	$5^7 \cdot 4$	15.5	99.6	0.4	0	0	99.6	0.4	0	0
		40	5^8	19.4	100	0	0	0	100	0	0	0
		41	$6 \cdot 5^7$	23.3	100	0	0	0	100	0	0	0
		42	$6^2 \cdot 5^6$	27.9	100	0	0	0	100	0	0	0
$\mathfrak{A}_9$	9	47	$6^2 \cdot 5^7$	15.5	96.7	3.2	0.1	0	97.0	3.0	0	0
		48	$6^3 \cdot 5^6$	18.6	99.8	0.2	0	0	100	0	0	0
		49	$6^4 \cdot 5^5$	22.3	100	0	0	0	100	0	0	0
		50	$6^5 \cdot 5^4$	26.8	100	0	0	0	100	0	0	0
$\mathfrak{A}_{10}$	10	56	$6^6 \cdot 5^4$	16.1	82.7	15.7	1.5	0.1	83.7	14.7	1.6	0
		57	$6^7 \cdot 5^3$	19.3	99.2	0.8	0	0	100	0	0	0
		58	$6^8 \cdot 5^2$	23.1	100	0	0	0	99.3	0.7	0	0
		59	$6^9 \cdot 5$	27.8	100	0	0	0	100	0	0	0

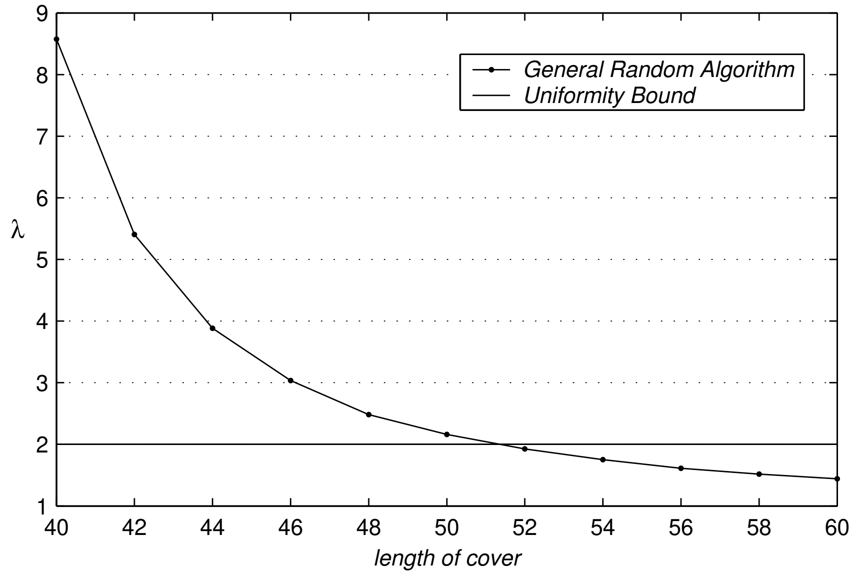
4. Uniform random covers

4.1. Random generating covers

The value $\lambda = \lambda_{max}/\lambda_{min} \geq 1$ defined in the introduction measures the degree of uniformity of a cover. Our further experiment shows that the values of λ decrease and tend to 1 when the lengths $\ell = r_1 + \cdots + r_s$ of the covers increase, i.e., the uniformity of the covers increases with their lengths ℓ. We conjecture that this fact is true in general. This would imply that we could generate random covers with a high degree of uniformity by increasing the lengths. It is therefore interesting to find a formula expressing the degree of uniformity of covers with respect to their lengths. The diagram in the following table shows the degree of uniformity λ as a function of the length ℓ of the covers for the alternating group $\mathfrak{A}_8$. Experiment has been done with 1000 repeats for each length. The table shows for instance that random generated covers of length $\ell \geq 52$ for $\mathfrak{A}_8$ are uniform.

[1]Experiment done with 10000 repeats for each type of cover.

General random algorithm for covers of *specified length* for $\mathfrak{A}_8$.



4.2. Comparison of covers from a random algorithm and a greedy algorithm

As we have seen in the previous experiment, the uniformity of the covers increases with their lengths. A natural question emerges: for a given length ℓ, can we construct random covers with higher degree of uniformity than that of random generating covers? An experiment has been made with a greedy algorithm for the groups $\mathfrak{A}_i$, $i = 5, 6, 7, 8$. And the results in the table below show that improvements can indeed be obtained.

- *Greedy algorithm*

  input : *Random cover* ($table[s][r]$)
  output : *Improved cover*

```
FOR i:= 2 TO s STEP 1 DO
    FOR j:= 2 TO r STEP 1 DO
        bestelm:= Find best from T elements for position [i,j]
        table[i][j]:= bestelm
    END;
END;
```

- *Find best from T elements for position* $[i,j]$ function returns

  a) element which *maximizes product*, if group not covered,
  b) element with *best uniformity product*, otherwise.

Greedy algorithm compared to general random for small alternating groups

$\mathfrak{G}$	s	ℓ	N	θ	λ_{rand}	λ_{greedy}[2]	$\frac{\lambda_{greedy}}{\lambda_{rand}}$
$\mathfrak{A}_5$	5	20	4^5	17.1	2.66	1.64	0.62
$\mathfrak{A}_6$	6	27	$5^3 \cdot 4^3$	17.4	4.40	2.40	0.55
$\mathfrak{A}_7$	7	33	$5^5 \cdot 4^2$	18.6	6.56	3.85	0.53
$\mathfrak{A}_8$	8	40	5^8	19.4	8.49	5.25	0.62

s : number of blocks in cover,
ℓ : length of cover,
$N = r_1 \times \cdots \times r_s$,
$\theta = N/n$.

Finally, we have carried out two further experiments concerning the degree of uniformity for random covers for $\mathfrak{A}_8$. These include random covers generated with elements of specified orders and random covers generated with elements of specified distance to the identity. In both cases no improvement of the degree of uniformity has been obtained when compared with the general generated random covers.

REFERENCES

[1] FELLER, W.:*An Introduction to Probability Theory and Its Applications,* John Wiley & Sons, Vol. 1, New York, 1957.
[2] GONZALES VASCO, M. I.—STEINWANDT, R.: *Obstacles in two public key cryptosystems based on group factorizations,* Tatra Mt. Math. Publ. **25** (2002), 23–37.
[3] GONZALES VASCO, M. I.—MARTINEZ, C.— STEINWANDT, R.: *Towards a uniform description of several group based cryptographic primitives,* Des. Codes Cryptogr. **33** (2004), 215–226.
[4] MAGLIVERAS, S. S.—MEMON, N. D.: *Algebraic properties of cryptosystem PGM,* J. Cryptology **5** (1992), 167–183.

[2]Experiment done with $T = n/10$ (tries for each possition in cover) and 1000 repeats for each cover.

[5] MAGLIVERAS, S. S.—STINSON, D. R.—VAN TRUNG, T.: *New approaches to designing public key cryptosystems using one-way functions and trap-doors in finite groups,* J. Cryptology **15** (2002), 285–297.

Received November 2, 2005

Institut für Experimentelle Mathematik
Universität Duisburg-Essen
Ellernstrasse 29
45326 Essen
GERMANY

E-mail: svaba@iem.uni-due.de
trung@iem.uni-due.de