1981

A CRYPTOSYSTEM ARISING FROM LOGARITHMIC SIGNATURES OF FINITE GROUPS

SPYROS S. MAGLIVERAS

University of Nebraska, Lincoln, Nebraska 68588-0115

1. Abstract

In this paper we present a new cryptographic system which relies on a certain method of machine representation for permutation groups. The method allows for encryption and decryption algorithms based on a space-efficient data structure which we call a *logarithmic signature* for the group. The number of keys afforded by a group of order $\prod_{i=1}^{s} r(i)$ is $\left\{\prod_{i=1}^{s}\left(\prod_{j=i+1}^{s} r(j)\right)^{r(i)}\cdot r(i)!\right\}^2$, a number of staggering size. The space required to store a key is of the order of $2\cdot\sum_{i=1}^{s} r(i)$. We defer a discussion of the algebraic properties of the system to a later publication. An analysis of random number generators based on the cryptosystem shows them to pass succesfully a battery of tests including tests for uniformity, sequencial independence, arbitrarily long cycle-periods, and very low autocorrelations.

2. A New Cryptosystem from Permutation Groups.

If G is a finite group and $G = G_0 > G_1 > \cdots > G_s = 1$ a descending sequence of subgroups of G, we define a *logarithmic signature* of G to be an ordered collection $\beta = \{B_1, B_2, \cdots, B_s\}$ of ordered subsets B_i of elements of G such that $B_i = \{u(i,j) : 1 \le j \le r(i)\}$ is a complete set of right coset representatives of G_i in G_{i-1}. In case G is a finite permutation group, specified by a set X of generators, C. Sims [28] describes an algorithm which generates a logarithmic signature of G. We call this the Sims-Schreier algorithm as it relies also on a theorem of Schreier's to obtain recursively generators for the subgroup G_i from generators of G_{i-1} and the list $B_i = \{u(i,j) : 1 \le j \le r(i)\}$ of coset representatives. The block B_i of coset representatives is itself obtainable from the generators of G_{i-1}. This procedure has been refined considerably and used by C. Sims, M. Hall, J. Cannon J. McKay, J. Leon, V. Pless, J. Neubuser, V. Felsch, the author, and others in the study of finite groups, and their applications. The Sims-Schreier algorithm can be easily adapted to other modes of machine representation of groups, for example, representations by matrices over a Galois field (see [3]), provided that

computationally efficient algorithms exists for determining the coset $G_i \cdot u(i,j)$ to which an element x of G_{i-1} belongs.

We take advantage of the special properties of logarithmic signatures of finite permutation groups to construct encrypting and decrypting functions which have desirable cryptographic properties. In addition, the functions can be used for constructing a new kind of random number generator. This generator compares favorably [18] with existing power-residue number-theoretic ones.

Although the cryptosystem discussed here is not a Public Key Cryptosystem (see [6], [8], [11], [19], [30]), strong one way functions can be constructed by means of *wild* logarithmic signatures, which we shall not discuss here. To this day we have found no appropriate *trap−doors* to embed so as to construct a Public Key System. The situation appears to be very promissing. In this paper however we deal only with the symmetric version of the cryptosystem.

If $\beta = \{B_i : 1 \le i \le s\}$ is a logarithmic signature of a group G, where $B_i = \{u(i,j) : 1 \le j \le r(i)\}$, we denote by $\mathbf{r}$ the vector $(r(1), r(2), \cdots, r(s))$. Note that while $\beta = \{B_i : 1 \le i \le s\}$ is a logarithmic signature for $G = G_0$, the set of blocks $\beta^{(k)} = \{B_i : k+1 \le i \le s\}$ is a logarithmic signature for G_k. If the element $u(i,j)$ of $B_i \in \beta^{(k)}$ is replaced by $h \cdot u(i,j)$, where $h \in G_i$, the resulting collection $\beta^{(k)*}$ is a new logarithmic signature for G_k. Moreover, any rearrangement of the elements of a block $B_i \in \beta^{(k)}$ yields a new logarithmic signature for G_k. It follows that there are a total of

$$\prod_{i=1}^{s} |G_i|^{r(i)\cdot r(i)!} = \prod_{i=1}^{s} \Big(\prod_{j=i+1}^{s} r(j) \Big)^{r(i)\cdot r(i)!}$$

logarithmic signatures for a Group G with vector $\mathbf{r} = (r(1), \cdots, r(s))$. This number is of course astronomical. Even in the case of the relatively small finite simple group $PSU_3(5^2)$ of order 126,000, degree 50 and vector $\mathbf{r} = (50,7,6,6,5,2)$, the number of logarithmic signatures is

$$2520^{50} 360^{7} 60^{6} 10^{6} 2^{5} \cdot 50! \cdot 7! \cdot 6! \cdot 6! \cdot 5! \cdot 2! \approx 3 \cdot 10^{282}.$$

If $x \in G_{i-1}$ then $x \in G_i \cdot u(i,j)$ for some $u(i,j) \in B_i$, and therefore, $x = y.u(i,j)$ for some y of G_i. If it is computationally efficient to determine the coset $G_i \cdot u(i,j)$ in which x lies, equivalently determine the corresponding coset representative $u(i,j)$, the decomposition $x = y \cdot u(i,j)$ can be achieved by computing $y = x \cdot u(i,j)^{-1}$. It follows that each element $g \in G$ has a unique representation as a product of elements of the logarithmic signature, one factor per block, $g = u(s,P_s) \cdots u(2,P_2) \cdot u(1,P_1)$. Converesly, if $(P_1, \cdots, P_s)$ is an s-tuple of positive integers with $1 \le P_i \le r(i)$, then the element $g = u(s,P_s) \cdots u(1,P_1)$ belongs to G, and as $(P_1, \cdots, P_s)$ ranges over all possible s-tuples of indices $(P_1, \cdots, P_s)$, with $1 \le P_i \le r(i)$, g scans G, so that each element of G will be obtained exactly once.

Let β be a logarithmic signature for G, with vector $\mathbf{r} = (r(1), \cdots r(s))$, and let

$$Q = Z_{r(1)} \times \cdots \times Z_{r(s)} = \{(P_1, \cdots, P_s) : P_i \in Z, \quad 1 \le P_i \le r(i)\}$$

We define a mapping $\Theta_\beta : G \to Q$ as follows: If $g \in G$, express g in its unique representations as $g = u(s,P_s) \cdots u(1,P_1)$;define $\Theta_\beta(g) = (P_1, \cdots, P_s)$. It is

immediate that Θ_β is a bijection of G onto Q. Both Θ_β and Θ_β^{-1} are computable with extreme efficiency in the case of permutation groups. (see [4],[5],[28]). In this case G is a permutation group acting on a set $\Omega = \{1,2, \cdots ,n\}$ and G_k is chosen to be the pointwise stabilizer of $\{1,2, \cdots ,k\}$. If $\Delta = \{k = \delta_1,\delta_2, \cdots ,\delta_{r(k)}\}$ is the orbit under G_{k-1} of the letter $k \in \Omega$, then a complete set of right coset representatives of G_k in G_{k-1} can be chosen by selecting one element $u(k,j) \in G_{k-1}$ for each $\delta_j \in \Delta$, such that $u(k,j)$ carries $k=\delta_1$ to δ_j. Furthermore, an element $x \in G_{k-1}$ belongs to $G_k \cdot u(k,j)$ if and only if $x(k)=[u(k,j)](k)=\delta_j$, a very fast test.

Now, given $\mathrm{r}=(r(1),\ldots,r(s))$, let $m_i = \prod_{j=1}^{i-1} r(j)$, $1 < i \leq s$. If Y is the set of positive integers 1, 2, $\cdots$,$|G|$, then the function $\lambda : Q \rightarrow Y$ defined by:

$$\lambda(\mathrm{P}_1, \cdots ,\mathrm{P}_s) = 1 + \sum_{i=1}^{s} m_i \cdot (\mathrm{P}_i - 1)$$

is a bijection, with $\lambda^{-1}(m)$, easily, and efficiently computable by successive subtractions (knapsack with superincreasing knapsack vector). If β is a logarithmic signature for G with vector $\mathrm{r} = (r(1), \cdots ,r(s))$ we define the function $\hat{\beta} : G \rightarrow Y = Z_{|G|}$ to be the composition $\hat{\beta} = \Theta_\beta \lambda$.

We are now ready to describe the encryption and decryption algorithms. Select a pair of logarithmic signatures α, β, for a group G of sufficiently large size to accommocate the message space. For a given message m, compute the encrypted image $E_{(\alpha,\beta)}(m)$ by :

$$E_{(\alpha,\beta)}(m) = [\hat{\alpha}^{-1}\hat{\beta}](m) = [\lambda^{-1}\Theta_\alpha^{-1}\,\Theta_\beta\lambda](m)$$

The decryption function $D_{(\alpha,\beta)}$ is of course $D_{(\alpha,\beta)} = \hat{\beta}^{-1}\hat{\alpha}$. Thus, we see that a key in the above cryptosystem consists of an ordered pair of logarithmic signatures of a finite group, and decryption consists of encrypting with the pair of logarithmic signatures flipped. If G is chosen to be the Mathieu group M_{24} of order 244,823,040, degree 24 and $\mathrm{r} = (24,23,22,21,20,48)$, then the number of logarithmic signatures is of the order of 10^{612} , and therefore the number of keys of the order of $10^{1224} \approx 2^{4066}$. The mappings $E_{(\alpha,\beta)}$, $D_{(\alpha,\beta)} = E_{(\beta,\alpha)}$ will be referred to collectively as *Permutation Group Mappings* (*PGM*).

3. An example

We shall currently illustrate the principles discussed in previous section by an example. The group used here is the simple group $G = PSL_3(2) = PSL_2(7)$ of order 168, in its doubly transitive representation on 7 points. This means that the message space is the set $Y = \{1, 2, \cdots ,168\}$. The logarithmic signature β_1 is obtained by using the Schreier-Sims algorithm and the generators $\alpha = (1\ 2)(3\ 4)(5)(6)(7)$, $\beta = (1\ 2\ 3\ 6\ 7\ 4\ 5)$. β_1 is written in *normal representation*. This means that each block begins with the identity permutation, and the rows of the i^{th} block are arranged in ascending order of the images of the element $i \in \Omega$. The number of blocks is $s = 3$, and the vector of block lengths is $\mathrm{r} = (7,6,4)$. Logarithmic signature β_2 is obtained by applying the procedure SHUFFLE to β_1 . This has the effect of performing the following

operations for each of the blocks of β_1 :

(1) For each $i : 1 \leq i \leq 3$, and for each $j : 1 \leq j \leq r(i)$, $u(i,j)$ of β_1 is replaced by $h(i,j) \cdot u(i,j)$, where $h(i,j)$ is a "random" element of the stabilizer G_i.

(2) For each $i : 1 \leq i \leq 3$, the $r(i)$ rows of the i^{th} block are permuted according to a random permutation.

β_1	β_2
1 2 3 4 5 6 7	7 3 6 1 5 2 4
2 1 4 3 5 6 7	1 5 4 6 7 3 2
3 5 4 7 6 1 2	6 2 3 5 4 1 7
4 1 2 3 5 7 6	3 7 4 5 6 2 1
5 3 7 4 6 1 2	4 7 6 2 3 1 5
6 7 2 4 1 5 3	5 6 4 1 2 7 3
7 6 4 2 1 5 3	2 1 7 5 3 6 4
1 2 3 4 5 6 7	1 6 4 5 7 2 3
1 3 6 7 2 5 4	1 7 2 5 6 4 3
1 4 3 2 5 7 6	1 4 5 6 3 7 2
1 5 4 6 7 3 2	1 3 4 2 7 5 6
1 6 5 4 3 2 7	1 5 2 7 6 3 4
1 7 6 3 2 4 5	1 2 3 4 5 6 7
1 2 3 4 5 6 7	1 2 3 4 5 6 7
1 2 4 3 7 6 5	1 2 7 5 4 6 3
1 2 5 7 3 6 4	1 2 4 3 7 6 5
1 2 7 5 4 6 3	1 2 5 7 3 6 4

Fig. 1

For ease of computation we represent the permutations in β_1 and β_2 in their decomposition as the product of cycles. Furthermore, we append a precomputed superincreasing vector m of row-indeces,

$$\mathrm{m} = (0,1,2,3,4,5,6;0,7,14,21,28,35;0,42,84,126)^T$$

to facilitate in the computation of λ and λ^{-1}.

β_1	m	β_2
(1)(2)(3)(4)(5)(6)(7)	0	(1 7 4)(2 3 6)(5)
(1 2)(3 4)(5)(6)(7)	1	(1)(2 5 7)(3 4 6)
(1 3 4 7 2 5 6)	2	(1 6)(2)(3)(4 5)(7)
(1 4 3 2)(5)(6 7)	3	(1 3 4 5 6 2 7)
(1 5 6)(2 7 3)(4)	4	(1 4 2 7 5 3 6)
(1 6 5)(2 7 3)(4)	5	(1 5 2 6 7 3 4)
(1 7 3 4 2 6 5)	6	(1 2)(3 7 4 5)(6)
(1)(2)(3)(4)(5)(6)(7)	0	(1)(2 6)(3 4 5 7)
(1)(2 3 6 5)(4 7)	7	(1)(2 7 3)(4 5 6)
(1)(2 4)(3)(5)(6 7)	14	(1)(2 4 6 7)(3 5)
(1)(2 5 7)(3 4 6)	21	(1)(2 3 4)(5 7 6)
(1)(2 6)(3 5)(4)(7)	28	(1)(2 5 6 3)(4 7)
(1)(2 7 5)(3 6 4)	35	(1)(2)(3)(4)(5)(6)(7)
(1)(2)(3)(4)(5)(6)(7)	0	(1)(2)(3)(4)(5)(6)(7)
(1)(2)(3 4)(5 7)(6)	42	(1)(2)(3 7)(4 5)(6)
(1)(2)(3 5)(4 7)(6)	84	(1)(2)(3 4)(5 7)(6)
(1)(2)(3 7)(4 5)(6)	126	(1)(2)(3 5)(4 7)(6)

Fig. 2

Let us now consider each of the operations for encoding. If, for example, $m = 111$ is a message to be encrypted, then $m - 1 = 110$ can be found between 84 and 126. in m. Thus $m - 1 = 84 + 26$. Now, 26 can be found between 21 and 28, therefore we write $m - 1 = 84 + 21 + 5$. This process determines the vector of row indices $\lambda^{-1}(111) = (6,11,16)$. We next compute $\pi = \Theta_{\beta_1}{}^{-1}(6,11,16) = \beta_1[16;] \cdot \beta_1[11;] \cdot \beta_1[6;] =$ (1)(2)(3 5)(4 7)(6) ·(1)(2 5 7)(3 4 6) ·(1 6 5) (2 7 3)(4) = (1 6 2)(4 7 5) $\in G$. We proceed now to compute $\Theta_{\beta_2}(\pi)$, i.e. to represent π with respect to β_2. Since $\pi(1) = 6$, we locate the element of block 1 in β_2 that sends 1 to 6. This element is $(16)(45) = \beta_2[3;]$, hence, we write $\pi = h_1 \cdot (1\ 6)(4\ 5) = h_1 \cdot \beta_2[3;]$, therefore $h_1 = \pi \cdot ((1\ 6)(4\ 5))^{-1} =$ (1 6 2)(4 7 5)(1 6)(4 5) = (1)(2 6)(3)(4 7)(5). Since $h_1(2) = 6$, we write $h_1 = h_2 \cdot (2\ 6)(3\ 4\ 5\ 7) = h_2 \cdot \beta_2[8;]$ therefore, $h_2 = h_1 \cdot ((2\ 6)(3\ 4\ 5\ 7))^{-1} = (2\ 6)(4\ 7) \cdot (2\ 6)(3\ 7\ 5\ 4)$ hence, $h_2 =$ (1)(2)(3 7)(4 5)(6) = (3 7)(4 5). Now, since $h_2(3)=7$, we write $h_2 = h_3 \cdot (3\ 7)(4\ 5) = h_3 \cdot \beta_2[15;]$, i.e. $h_3 = h_2 \cdot ((3\ 7)(4\ 5))^{-1} =$ (3 7)(4 5)(3 7)(4 5) = 1. We have $\pi = h_1 \cdot \beta_2[3;] = h_2 \cdot \beta_2[8;] \cdot \beta_2[3;] = h_3 \cdot \beta_2[15;] \cdot \beta_2[8;] \cdot \beta_2[3;]$, with $h_3 = 1$. Hence, $\pi = \beta_2[15;]\beta_2[8;]\beta_2[3;]$. This determines the vector of row pointers for β_2 : $\mathbb{P} = \Theta_{\beta_2}(\pi) = (3,8,15)$, from which $\lambda(\mathbb{P})$ can be computed directly by $\lambda(\mathbb{P}) = 1 + \mathrm{m}(3) + \mathrm{m}(8) + \mathrm{m}(15) =$ 1 + 2 + 0 + 42 = 45. Thus, we have $E_{(\beta_1,\beta_2)}(111) = 45$. The permutation

$$m \rightarrow E_{(\beta_1,\beta_2)}(m)\ ; 1 \leq m \leq 168$$

is displayed in *Table* 1 below:

Table 1

	0	1	2	3	4	5	6	7	8	9
0		135	84	144	5	139	10	148	2	140
1	151	61	6	122	92	65	119	39	75	69
2	31	127	37	21	32	96	41	87	99	58
3	7	95	82	62	101	71	72	70	130	110
4	76	24	162	51	168	60	89	55	94	64
5	89	56	67	145	90	38	8	149	35	123
6	159	153	115	43	121	105	116	12	125	3
7	15	142	91	11	166	146	17	155	156	154
8	46	26	160	108	78	9	126	18	131	13
9	136	22	128	14	25	103	132	80	50	107
10	77	165	117	111	157	1	163	147	158	54
11	167	45	57	100	133	53	124	104	59	113
12	114	112	4	68	118	150	36	93	42	102
13	47	97	52	106	44	98	109	19	48	164
14	134	23	161	81	33	27	73	85	78	63
15	74	138	83	129	141	16	49	137	40	20
16	143	29	30	28	88	152	34	66	120	

4. Concluding Remarks

Work has been already undertaken in examining the possible strengths and weaknesses of the cryptosystem presented here. When the system is used as a random number generator it produces sequences of pseudo-random numbers that compare favorably with output from well tuned congruential generators. An analysis of the statistical properties of such output is included in [18].

Work is currently under way to further understand the algebraic structure of the cryptosystem. We have addressed and solved several questions relating to the system. These results and results of current research will appear in a future publication. As we proceed to understand more about the algebraic properites of PGM we hope to be able to answer in the affirmative the question of whether or not trapdoor one-way functions can be devised to support public key cryptography.

5. Bibliography

[1] Berlekamp, E. R., *Algebraic Coding Theory,* McGraw-Hill, New York, 1968.

[2] Bright, H.S. and Enison, R.L., *Quasi-Random Number Sequences from a Long-Perion TLP Generator with Remarks on Application to Cryptography,* ACM Computing Surveys, Vol. 11, No. 4, December 1979, 358-370.

[3] Butler, G., *The Schreier Algorithm for Matrix Groups,* Symposium on Symbolic and Algebraic Computation, "SYMSAC" 76, 1976, p. 167.

[4] Cannon, John J., *On Determining the Order of a Group,* Proceedings of the 1976 ACM Symposium on Symbolic and Algebraic Computation, Yorktown

Heights, New Yokd, 1976. Also: SIGSAM bull., Vol. 10, No. 3, 1976, 5.

[5] Cannon, John J., *A Draft Description of the Group Theory Language Cayley,* Proceedings of The 1976 ACM Symposium on Symbolic and Algebraic Computation, Yorktown Heights, New York, 1976.

[6] Diffie, W., and Hellman, M.E., *New Directions in Cryptography,* IEEE Trans. on Information Theory, IT-22, November 1976, pp. 644-654.

[7] Diffie, W., and Hellman, M.E., *Exhaustive Cryptanalysis of the NBS Data Encryption Standard,* Computer 10, 6, Jule 1977, 74-84.

[8] Diffie, W., and Hellman, M.E., *Privacy and Authenticity: An Introduction to Cryptography,* Proceedings IEEE, March 1979.

[9] Felsch, Volkmar, *Programs for Permutation Groups,* Todd-Coxeter, Defining Relations Survey, Permutations (Actes Colloq., University Rene-Descartes, Paris, 1972), pp. 241-250. Gauthier-Villars, Paris, 1974.

[10] Friedman, W.F., *Cryptology,* Encyclopedia Britannica, Vol. 6, 1967, pp. 844-851.

[11] Gardner, M., *A New Kind of Cipher That Would Take Millions of Years to Break,* Sci.Am. 237, August 1977, pp. 120-124.

[12] Golomb, S.W., *Shift Register Sequences,* Holden-Day, San Francisco, California, 1967.

[13] M. Hall, *The Theory of Groups,* MacMillan, 1959.

[14] Hellman, M.E., *The Mathematics of Public-Key Cryptography,* Sci. Am. 241, August 1979, pp. 146-157.

[15] Kahn, D., *The Codebreakers: The Story of Secret Writing,* MacMillan, 1959.

[16] Knuth, D.E., *The Art of Computer Programming,* Vol. 2, Seminumerical Algorithms, Addison- Wesley, Reading Mass., 1968.

[17] Lempel, A., *Cryptology in Transition,* ACM Computing Surveys, Vol. 11, No. 4, December 1979, pp. 286-302.

[18] Magliveras, S.S., Oberg, B.A., and Surkan, A.J., *A New Random Number Generator From Permutation Groups,* Rend. del Sem. Matemat. di Milano, vol. 54

[19] McEliece, R.J., *A Public-Key Cryptosystem Based in Algebraic Coding Theory,* DSN Progress Rep., pp. 42-44, Jet Propulsion Lab., January and February, 1978.

[20] Morris, R., Sloane, N.J.A., and Wyner, A.D., *Assesment of the National Bureau of Standards Proposed Federal Data Encryption Standard,* Cryptologia 1,3, July 1977, pp. 281-284.

[21] Neubuser, Joachim, *Some Applications of Group Theoretical Programs,* Proceedings of the 2nd Symposium on Symbolic and Algebraic Manipulations, L.A., California, 1971, pp. 77, ACM, New York, 1971.

[22] Popek, G.J. and Kline, C.S., *Encryption and Secure Computer Networks,* ACM Computing Surveys, Vol. 11, No. 4, Dec. 1979.

[23] Pless, V., *Encryption Schemes for Computer Confidentiality,* IEEE Trans. Comp. C-26, 11, November 1977, pp. 1133-1136.

[24] Shannon, C.E., *The Mathematical Theory of Communication,* Bell Syst. J., 27, July and October 1948, pp. 379-423 and pp. 623-656.

[25] Shannon, C.E., *Communication Theory of Secrecy Systems,* Bell Syst. J., 28, October 1949, pp. 656-715.

[26] Simmons, G.J., *Symmetric and Assymmetric Encryption,* ACM Computing Surveys, Vol. 11, No. 4, December 1979.

[27] Simmons, G.J., *Cryptology: The Mathematics of Secure Communication,* Math. Intell. 1, 4, January 1979, pp. 233-246.

[28] Sims, C.C., *Computational Methods in the Study of Permutation Groups,* "Computational Problems in Abstract Algebra", Proc. Conf., Oxford, 1964, pp. 169-183, Pergamon Press, Oxford, 1970.

[29] Rabin, M.O., *Probabilistic Algorithms,* in Algorithms and Complexity, J.F. Traub (Ed.), Academic Press, New York, 1976, pp. 21-40.

[30] Rivest, R.L., Shamir, A., and Adleman, L., *A mehtod for Obtaining Digital Signatures and Public Key Cryptosystems,* Commun. ACM 21, 2, 1978, pp. 120-126.

[31] Wielandt, H., *Finite Permutation Goups,* Academic Press, 1964.