22 October 1952

MEMORANDUM FOR THE CONSULTANT

SUBJECT: Comments on SCAMP

Reference: Report on SCAMP by Stewart S. CAIRNS, dtd 8 September 1952

1. I make the following comments concerning SCAMP:

a. The idea of a two-month mathematical seminar on Agency problems is excellent. It provides three badly-needed things:

(1) The introduction of new, competent scientific thought on important unsolved problems many of which have been around so long that the Agency personnel assigned to them have begun to grow stale;

(2) The opportunity for the Agency's better cryptomathematicians, or mathematical cryptologists, to free themselves for an extended period from the extensive morass of administrative and executive detail with which all too many of them are saddled and to participate full time in the attempted solution of significant problems with which they are technically competent to cope;

(3) The opportunity for bona-fide mathematicians employed by AFSA to recover a bit of their professional skill through informal discussion with recognized leaders in mathematical specialties.

b. The actual carrying-out of SCAMP during the summer of 1952 left a good deal to be desired:

(1) There was considerable uncertainty as to who would participate; this uncertainty persisted into the seminar itself, and seems to have been due, at least in part, to the late date at which invitations to participate were issued.

(2) Clearance difficulties hampered the project immensely. These difficulties were of three kinds:

(a) Some technically desirable people were excluded because of non-clearance or imcomplete clearance;

(b) The highest clearance granted to visiting firemen was CONFIDENTIAL; this was too low;

(c) The heterogeneity of clearance levels made security leaks almost unavoidable.

22 October 1952

(3) The major SCAMP topic was the existence of finite projective planes of various orders, as set forth on pp. 4-5 of the reference. The significance of this topic to AFSA seems small to me, and the arguments adduced to support the idea that the topic is significant are, in my estimation, rather tenuous. I agree that the topic is of great mathematical interest; I agree further that certain steps forward were made; I question, however, the relevance of the subject and the adaptability of the methodology to AFSA problems.

c. There is a very real danger in projects such as SCAMP and AFSASAB that the Agency may make itself an enthusiastic but unwitting sort of computing machine for the use of "outside experts" who do not have any real responsibility for the operation of the Agency but who are very much aware of the advantages to pure research of having so large and rich an organization to support their personal research goals.

2. In line with these comments, I make the following recommendations:

a. Being done

b. Start has been made

✓ b. Participation lists should be made up now.

c. Will begin very soon. Headland ✓ c. Clearances should be started now. All hands should have full cryptologic clearance and indoctrination.

d. Will discuss with Headland, Canna, et al.

d. The agenda should be established now, and thrashed out by the offices to insure that all subjects for discussion are in fact closely related to the AFSA effort. I feel that the Agency should not attempt to support pure research without some assurance that the results, if any, will be appropriate to its mission.

R. H. SHAW
Chief, Cryptosecurity Branch

Copies to:
Chief, Cryptomathematical Division (34)
Chief, Technical Projects Group (206)
Technical Director, Office of Operations (~~20~~ 02T)
Chief, Office of Communication Security (04)
Chief, Analysis and Evaluation Division (41)

~~CONFIDENTIAL - Security Information~~

Report on SCAMP

to the

Director

of the

Armed Forces Security Agency

Submitted by

Stewart S. Cairns

8 September 1952

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

Report on SCAMP

TABLE OF CONTENTS

Section	Title
1.	Introduction, origins of the symposium
2.	The scientific work of the symposium
3.	Administrative work
4.	Suggestions regarding possible future efforts

Appendices

I.	List of participants
II.	List of seminar meetings
III.	List of conferences
IV.	List of other reports
V.	Computations attacked
VI.	Reproduced seminar reports
VII.	Reproduced conference reports
VIII.	Other reproduced reports
IX.	Budgetary material
X.	Suggestions from SCAMP members regarding future work
XI.	Miscellaneous selected correspondence

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

Report on SCAMP

1. Introduction

The summer symposium to which the name SCAMP was finally attached grew from discussions in SCAG. The initial proposals leading to SCAMP were made in 1951 by C. B. Tompkins in his role as a member of SCAG. Originally, a continuing project was intended. However, after various discussions, it was decided to conduct a summer symposium and, on the basis of experience therewith, to consider the desirability of later efforts. This decision was reached in March 1952, with the result that only about three months were available for the preliminaries to the symposium. Among the proposals by Tompkins was the use of the primarily mathematical part of SCAG, referred to as SCAM (Special Committee Advising in Mathematics), in an advisory capacity. The code name SCAMP was created in AFSA by adding the letter P to SCAM.

No fixed objectives were officially adopted for the symposium. A set of proposed objectives was contained in a document "Notes on a proposed research project and symposium" by Tompkins, 18 March 1952, subsequent to an agreement by the writer to serve as leader of the symposium, and these proposed objectives proved useful in preparing for and conducting the symposium. (The "Notes" are in Appendix XI.)

Because of the lateness of the decision to conduct the symposium, difficulties were encountered in the recruitment of personnel. Many desirable participants had previous commitments, and the time was too

short for the normal clearance procedures. This led to the use largely of personnel for whom evidence of clearability existed and also to the conduct of the symposium largely on a confidential level, though a higher security level would have been advantageous. (See Appendix for list of participants.)

Through the cooperation of members of the staff of the Institute for Numerical Analysis in Los Angeles and of the University of California at Los Angeles, adequate office space was provided and provisions made for the necessary office supplies and equipment.

The symposium benefited in a number of ways from being located on the UCLA campus and associated with the Institute for Numerical Analysis of the National Bureau of Standards. A minor, but not inconsiderable, advantage was the comparative freedom from excessive summer heat, as a result of which more effective work can be accomplished there than in most parts of the country. Scientifically, SCAMP benefited by the availability of the computing equipment (SWAC and IBM) at the INA and by the proximity of mathematicians connected, at least for the summer, with UCLA, and INA and the Rand Corporation. This latter advantage extended beyond the pleasure and the general stimulation of associating with colleagues. Since one of the principal problems of the symposium was unclassified and of general mathematical interest, SCAMP sponsored a seminar on the subject (finite projective planes) and also a shorter seminar on mechanical aids to computation. Various mathematicians of the groups listed above not only attended the seminar meetings and

participated in discussions, but also took part as invited speakers. One such speaker, Assistant Professor Lowell J. Paige of UCLA, later became a member of SCAMP for three weeks. Conversely, a number of lectures sponsored by the INA and the Rand Corporation had a direct bearing on the interests of SCAMP and were attended with profit by various participants. Particularly valuable were (1) a series of talks at the INA on programming for computers, and (2) lectures by John von Neumann and Tjalling Koopmans at Rand on the so-called "assignment problem," whose formulation in terms of matrices is very closely related to one of the mathematical problems most significant to AFSA.

2. The Scientific Work of the Symposium

The choice of the problems to which SCAMP devoted most of its effort was determined partly by the need for maintaining a low level of classification and partly, as the work progressed, by the interests of the participants. Prior to the opening of the symposium, a number of problems were suggested and discussed with AFSA personnel. In order to avoid a scattering of efforts over a variety of special questions and to enhance the likelihood of useful contributions, attention was concentrated on introducing and studying

a. Combinatorial problems with possible numerical solutions involving permutations.

b. Computational schemes leading to exhaustive attacks on such problems,

~~CONFIDENTIAL~~

c. Methods of attack involving the imbedding of such problems in a continuous space and the study of appropriate functions defined over the convex hull of the discrete set of potential solutions.

For a number of reasons, these general subjects were specialized to the question of the existence of finite projective planes of various orders. The participants devoted most of their efforts to items a. and b., on which definite progress was made. Promising approaches exist to the attacks in continuous spaces, and it is to be hoped that later efforts will involve their further development.

The study of finite projective planes leads to general questions involving permutations. Since every permutation can be realized as a cross-wired rotor, and since every cross-wired rotor yields a permutation, some fairly direct connections between AFSA's problems and those encountered in studying finite projective planes may be expected. These are outlined in the paper "Problems related to finite Geometries," Conference No. 18, Appendix VII, but in summary it might be pointed out that

(1) The construction of a hitherto unknown finite projective plane might lead to an example from which new and valuable knowledge of permutations could be gleaned;

(2) The problem of studying finite projective planes supports exhaustive attacks on SWAC which are very likely to carry over to AFSA applications.

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

In addition, it is true that finite projective planes have long been of general mathematical interest, and research articles are currently being published concerning them. Hence it was possible to conduct open seminars (see Appendix for list) in connection with SCAMP, thus strengthening our ties with the considerable group of mathematicians in the Los Angeles area during the summer, and stimulating their interest in a pure mathematical problem whose solution would be of practical value to AFSA.

Another short seminar (four meetings) and several conferences were devoted to the capabilities of various computing devices, especially with reference to the problems mentioned above. The talks given at these meetings were not reproduced, since the existing literature covers their subject matter.

Supplementing the open seminars was a series of conference (see Appendix III for list), some of them classified and all of them confined to SCAMP participants.

With few exceptions, the speakers at seminar meetings and at conferences wrote up their material, which was reproduced for later use. Copies of the resulting papers are in the appendices, as are a number of other SCAMP reports written by the participants. The papers resulting from the seminar on finite projective planes were reproduced in sufficient quantities to permit some distribution by the Institute for Numerical Analysis, as well as within AFSA and among members of SCAMP. The remaining papers were not made available to the INA but were entirely reserved

~~CONFIDENTIAL~~

for AFSA and SCAMP uses.

The purposes of the conferences were (1) to present introductory material indicating, within security limitations, the general area of the sponsor's interests (2) to suggest mathematical problems appropriate to SCAMP and (3) to discuss results and methods. Conference topics included depths, weights and factors, measures of roughness, information theory, and permutation problems. (See Appendix VI.)

Research was pursued on both an individual and a collaborative basis. The spirit of teamwork was strong, and the participants from AFSA furnished valuable assistance in directing the other members along useful lines.

Among the results obtained, the following may be mentioned as samples. They are mere samples, and their listing here should not be taken to imply that they are considered more significant than other results which might have been listed:

(1) In a paper by Paige and Wexler (Appendix VI, No. 2) new light was thrown on methods for passing back and forth between an incidence matrix of a finite projective plane and a corresponding set of mutually orthogonal latin squares.

(2) Certain rational matrices associated with finite projective planes were developed and presented in a seminar talk by Albert, who plans, if approval is granted, to publish the results in a research journal.

(3) Dr. Ward concentrated his efforts on computational procedures. He developed and successfully tried out a SWAC program of a

search for so-called "magic sets" or "transversals" in a latin square, of order 10; also for a test to see whether such a square contains magic sets so related as to assure the existence of an orthogonal mate. This latter is a necessary, but not sufficient, condition for the existence of a finite projective plane of order 10. The methods can be used through order 12 on SWAC. (Report to be added to Appendix VI.)

(4) Dr. Tompkins, besides stimulating and advising other members on a variety of problems, obtained on SWAC a difference set of 513 numbers connected with a finite projective plane of order 512. In connection therewith, he programmed a search for a certain class of irreducible polynomials. (Appendix VI, Nos. 14, 15.)

(5) A brief method was presented by Botts for demonstrating the non-existence of five nutually orthogonal 6 x 6 latin squares, hence the non-existence of a projective geometry of order 6. While the result was known, the method is new and may lead to successful attacks on unknown cases. (Report to be added to Appendix VI.)

(6) A theorem was proved by Hanson on the number of permutations associated with a given difference set. (Report to be added to Appendix VI.)

Various promising attacks on problems were initiated but left

incomplete at the end of the symposium. Among these may be mentioned a collaborative approach by D. W. Hall and G. A. Hedlund to the problem of the existence of a finite projective plane of order 10. Furthermore, the results listed above are mere stages on the way toward larger problems and thus also represent incomplete attacks. In addition, members of SCAMP proposed, for possible future consideration, several problems related to those on which actual work was performed.

The valuable work of the participants from AFSA is not individually recorded in this report, since it would be difficult to do so without seeming to make comparisons among them. Much of their contributions took the form of oral discussions and of direct assistance to the other members of SCAMP, who are relatively unfamiliar with the problems of AFSA.

3. Administrative work.

As indicated in Section 1 above, SCAMP was brought into being with little time for advance planning. The writer, as chairman, assumed responsibility for almost all phases of the arrangements: (1) administration of funds, (2) recruitment of personnel, (3) scheduling of conferences and seminars, (4) general supervision of research activities, and of the reproduction of reports. These duties might well have been divided among a number of people. The important matter of arranging for office space and equipment was handled with the aid of C. B. Tompkins, who was in the Los Angeles area in advance of the symposium, and with the cooperation of staff members of INA and UCLA.

The space occupied by SCAMP consisted of Rooms 323 and 325-329 inclusive in the old Chemistry Building at UCLA. Room 323 has a capacity of six persons without crowding, as does 325, which is divided into two rooms holding three each. Room 327 is likewise thus divided, with three desks in one part and appropriate space in the other for the safe file, the librarian and the chairman. Rooms 326 and 329 are offices for three each, and Room 328 was used as a conference room. Such space is adequate for a symposium of the size of SCAMP.

The SCAMP budget was set at a lump sum of $25,000, transferred from AFSA through the ONR to the INA, with assurances of further funds if essential to the success of the undertaking. Roughly speaking, about $18,000 was allocated to salaries, travel expenses and associated overhead, about $6,000 to computing (SWAC and IBM), and about $1,000 to office equipment, supplies, telephone charges, and so on. Some computing on SWAC is still in progress, and some other additional expenses are yet to be incurred before the work of SCAMP is completed. In a supplement to this report, a breakdown of actual expenditures as of 15 September will be given. It appears likely that some unexpended funds will remain after that date and might well be used for further computation growing directly out of the work of SCAMP. Appendix IX contains correspondence relating to budgetary matters.

4. Proposals for the future.

Suggestions for the immediate future were made to the Director of the Armed Forces Security Agency when he visited SCAMP on 14 August and

conferred with the available SCAG members: S. S. Cairns, H. P. Robertson and C. B. Tompkins. It was recommended (1) that AFSA sponsor a second summer symposium similar to SCAMP at the same location in 1953, (2) that there be some work at UCLA on a reduced scale during the academic year 1952-3, to avoid a discontinuity between the two symposiums and (3) that decisions concerning later efforts be reserved until the work of SCAMP has been suitably evaluated.

The following suggestions, some of them obvious and some resulting from the experience of this year's symposium, may prove helpful in future planning.

(1) It is of the greatest importance to start as early as practicable on the task of recruiting and clearing personnel, since clearance procedures are notoriously time-consuming and since the most desirable mathematicians are likely to make other commitments for the summer, if not approached early.

(2) Although the research program will be partly dictated by the talents and interests of the participants, there should be an early decision as to general objectives. Reference is made to the following items in Appendix XI:

(a) "Notes on a proposed research project and symposium," 18 March 1952 by C. B. Tompkins.

(b) Letter of 24 June 1952 from Tompkins to D. C. Spencer.

(c) Memorandum on "The Objectives of SCAMP" from S. S. Cairns to the members of SCAMP, 16 July 1952. Prospective participants should be informed of the general objectives in advance and also, insofar as possible, of particular problems proposed for attack.

(3) It might be well to have both an administrative and a technical chairman. The technical chairman, who might be chosen from the INA or from UCLA, would assume responsibility for financial negotiations with prospective participants and for the provision of suitable working space, office equipment so on. Some secretarial assistance might be provided by the INA, although an AFSA librarian is also needed to take care of the classified files, to prepare classified reports and to supervise their reproduction. The technical chairman could concentrate on the research program, including the planning of expository background lectures, presentation of new results and conference discussions devoted to work in progress. He should also have the duty of preparing a final report. If thus freed from the non-research administrative burden, he might have time to do some mathematics himself. This division of duties, or some modification thereof, should make it easier to secure a good technical chairman.

(4) From the first planning stage on, there might well be an advisory committee of fully cleared mathematicians, who would

nominate the chairman or chairmen, establish a calendar of deadlines, nominate key personnel, and who would be kept informed of significant developments both before and during the symposium, so as to be in a position to render the most useful advice. The advisory committee should, in cooperation with the chairman, ensure that the problems attacked during the symposium are relevant and important to applications on a high security level.

(5) A few carefully selected AFSA personnel should be assigned to the symposium for its entire duration and others, as this summer, for shorter periods of time. Those assigned for the whole period should include persons thoroughly familiar both with the mathematical problems of AFSA and with their prospective applications. Questions of security (classification of problems, reports and so on) should be decided by AFSA representatives.

Appendix X contains suggestions from SCAMP participants relating to various aspects of possible future projects analogous to SCAMP.