Midterm appraisal Report for ReX exchange Program between LUND and ISI

December 3, 2002

1 Exchange plan

Proposed Exchange Plan

- Prof. Bimal Roy (ISI) and Prof. Thomas Johansson (LUND) for 1 month each.
- One Post Doctoral fellow each from LUND and ISI. Research fellow.
- One research Scholar each from LUND and ISI.

Achieved So Far

- Prof. Bimal Roy to LUND (May-June, '02).
- Post Doctoral fellow, Dr. Soumen Maity, ISI to LUND (Feb., '02 - Aug., '02).

To be Done
The exchange program is to be completed within a period of another eight (8) months (July, 2003). The plan of exchange has been finalised subject to your approval.

- Prof. Thomas Johansson (Jan '03).
- One Post doctoral Fellow from LUND to ISI (Two months)
- One Research fellow from ISI (for Three months) to LUND.
- Two Faculty mmebers from ISI (for one month each) to LUND.
- One Post Doctoral fellow from ISI (for one month) to LUND.

We were unable to stick to the regular appraisal schedule (at regular intervals of 2-3 weeks) of our progress to the ReX committee. From now on we hope to send a monthly report.

2 Deliverables

Proposed:

1. Developing a byte-oriented software stream cipher, based on LFSRs, for fast and secure communication purpose.

2. Theoretical studies of relevant cryptographic properties of the the Boolean function and the connection polynomials of the LFSR.

3. Fast software implementation of the LFSR in software.

4. Evaluating the scheme against existing and proposed attack.

Achieved So far:

- We have developed a very fast software stream cipher scheme based on the well-known nonlinear combiner model. A detailed report [1] on these scheme is attached here. We have earlier sent a draft report of this scheme to you. The present version is a modified one. We have discussed the detailed design procedure, security of the scheme against most of the relevant existing attacks. A fast implementation technique of the LFSRs and the Boolean function has been developed in this work. Th scheme is faster than any of the existing software stream cipher scheme in LINUX and SUN platform (19 - 71 Gbps).

- Various properties of the connection polynomialsn of LFSRs are studied in the paper [2]. This paper has been presented in SAC 2002. The cryptographic properties of the Boolean function has been discussed in [3]. Here an Important construction technique of resilient Boolean function have been described. The paper is to be presented in INDOCRYPT 2002.

.

To be done:

The security of the proposed scheme is to be studied in the light of some very recently proposed attacks on similar scheme. We also need to study the performance of the proposed scheme in various platforms. Lastly we intend to explore the possibility of using this scheme in embedded software for secure communication over desktop PCs.

We also plan to develop a fast software stream cipher system based on SNOW and AES. Preliminary discussion has been completed between Prof. Johansson and Prof. Roy. Detailed work is to be started during second half of the project.

3 Financial Report

Total amount of grant	USD 41,150
Amount released so far	USD 20,575

Details of expenditure done till 30^{th} November, 2002:

Item	Amount in USD
Airfare for Dr. Soumen Maity (Calcutta - Copenhagen - Calcutta)	1100
Visa expense for Dr. Maity	100
Transport from Copenhagen to Lund (for Prof. Roy)	100
Cost of accomodation & other living expenses for Dr. Maity for the months of February to August 2002	12250
Airfare for Prof. Bimal Roy (Calcutta - Copenhagen - Calcutta)	1150
Visa expense for Prof. Roy	100
Transport from Copenhagen to Lund (for Prof. Roy)	100
Cost of Accommodation and other living expenses for Prof. Roy	2900
Airfare for Prof. Thomas Johansson (Copenhagen - Calcutta - Copenhagen) (Already Booked)	1500
Cost of Accommodation and other living expenses for Prof. Johansson (Already Booked)	500
Total expenditure	19, 800

Amount Left	USD 775
Amount to be spent in second half	USD 21,350

Proposed expenditure for second half,
subjected to approval.

Item	Amount in USD
One post Doctoral fellow from LUND to ISI (for 2 months) Air Fare & local expenses	4,100
One post Doctoral fellow from ISI to LUND (for 1 months), Air Fare & local expenses	3,400
Two faculties from ISI to LUND (for 1 months each) Air Fare & local expenses	6,500
One research felow from ISI to LUND (for 3 months) Air Fare & local expenses	7,350
Proposed Expenditure	21,350

4 Future Prospect

The interaction between crypto group of ISI and Lund has become a very well-knit one. The research interest of the two groups are similar. Members of both the groups have made some interesting and novel contribution in different areas of cryptography, specially new construction of cryptographically significant Boolean function and development of software stream ciphers. Continuing this exchange programs for a longer period will lead to some productive development in the fast developing world of cryptography.

References

[1] S. Chowdhury, S. Maitra and B. Roy. A practical design of Nonlinear Combiner Model as a software stream cipher. In pre-print.

[2] S. Maitra, K. C. Gupta and A. Venkateswarlu. Multiples of Primitive Polynomials and Their Products over GF(2). In *SAC 2002*, August 2002, pages 218–234 in pre-proceedings.

[3] S. Maity, T. Johansson. Construction of cryptographically important Boolean Function. In *INDOCRYPT 2002*, December 2002, to be published.