Call for Contributions
SHARCS – Special-Purpose Hardware for Attacking Cryptographic Systems
www.sharcs.org
February 24 -25, 2005, Paris

The **SHARCS Workshop** is the first open meeting ever devoted entirely to the challenging subject of special-purpose cryptanalytical machines.

Much of the earlier work in this area was done on key searches for symmetric-key algorithms, with a particular emphasis on attacks against DES. More recently there has been interest in hardware architectures for sieving methods for attacking the RSA scheme. However, it seems that much work remains to be done including, for instance, special purpose hardware crackers for:

- index calculus algorithms
- elliptic curve based schemes
- lattice based schemes
- specific block and stream ciphers

In addition to algorithmic issues, it is also the workshop's goal to make advances on implementational issues such as:

- optical devices for cryptanalysis
- analog computers for cryptanalysis
- digital architecture for cryptanalysis

The ultimate objective of SHARCS is to determine whether special purpose hardware poses a real threat for today's cryptographic algorithms, and whether there are advantages over software-based attacks. Since this is an intrinsically interdisciplinary subject, it is hoped that the workshop can bring together researchers with different backgrounds for discussing and advancing this exciting field.

The workshop will consist of invited keynote presentations and some contributed presentations. We welcome submissions of extended abstracts (at least 3 pages.) We would like to stress that we do *not* aim at receiving contributions on side channel attacks nor on attacks carried out on conventional computer platforms with conventional attack algorithms. Furthermore, at this point we exclude quantum cryptologic devices. Theoretical papers analyzing the feasibility and costs of attacks using specialized hardware are, however, very much welcomed.

For more information on the workshop visit: `www.sharcs.org`

The workshop is organized by **ECRYPT**, the European Network of Excellence in Cryptography (www.ecrypt.eu.org). The workshop is an activity of ECRYPT's VAMPIRE - Virtual Application and Implementation Research Lab.

There will be no formal proceedings, but a handout with abstracts will be provided to all participants. (This avoids submissions to SHARCS from conflicting with submissions to forthcoming conferences with proceedings).

Important dates:

January 3, 2005:	submission of abstracts
January 24, 2005:	notification of acceptance or rejection
February 10, 2005:	revised version of accepted papers
February 24 & 25, 2005:	SHARCS workshop

The dates were chosen to have SHARCS immediately after Fast Software Encryption (FSE) 2005, which runs from February 21-23. Most likely, SHARCS will be held in ENSTA, the same location that is used for FSE.

The submission should start with a title, a list of the authors together with their affiliations and a short abstract describing the content of the paper. This should be followed by an extended abstract of at least 3 and at most 12 pages. The authors of accepted papers must guarantee to present their paper at the workshop.

To submit send your contribution to

`submit@sharcs.org`

no later than January 3, 2005, in ps or pdf format. You should receive an acknowledgment of submission no later than one day after submission.

Program Committee:

Gerhard Frey (Essen)	Elisabeth Oswald (Graz)
Tanja Lange (Bochum)	Christof Paar (Bochum)
Arjen Lenstra (Lucent/Eindhoven)	Nigel Smart (Bristol)

Invited Speaker:

So far the following speakers have confirmed giving invited talks:

Dan Bernstein	Adi Shamir
Arjen Lenstra	Eran Tromer
Jean-Jacques Quisquater	Mike Wiener
Tony Sale	