

Post-doc position proposal

Source: <http://www.derkeiler.com/Newsgroups/sci.crypt/2003-03/1007.html>

From: Sez nec Andre (Andre.Seznec@irisa.fr)

Date: 03/06/03

From: Sez nec Andre <Andre.Seznec@irisa.fr>

Date: Thu, 06 Mar 2003 13:44:47 +0100

Cryptanalysis and/or new usages of the empirically strong random number generator HAVEGE.

Brief presentation of HAVEGE:

Random numbers with high cryptographic quality are needed to enhance the security of cryptography applications. Hardware true random number generators are not implemented on all computer systems. Then, many implementations rely on software heuristics such as entropy gathering from measuring unpredictable external events. These generators only deliver a few bits per event. This limits them for being used as seeds for pseudo-random generators.

HAVEGE (HARDware Volatile Entropy Gathering and Expansion) is a new software heuristic for generating "empirically strong random numbers" on processor systems implemented around modern superscalar microprocessors, as for instance PCs, workstations or PDAs. By empirically strong random numbers, we mean that 1) to the best of our knowledge the distributions of the generated sequences do not exhibit any bias, 2) that reproducing the generated sequences appears to be impossible in practice.

General-purpose processors feature a large number of hardware mechanisms that aim to improve performance: for instance caches and branch predictors. The state of these components is not architectural (i.e., the result of an ordinary application does not depend on it). It is also volatile and cannot be directly monitored by the user. On the other hand, every operating system interrupt modifies thousands of these binary volatile states.

HAVEGE combines entropy/uncertainty gathering from the internal hardware volatile states of the processors with pseudo-random number generation.

Internal hardware states are indirectly probed through the hardware clock counter and maintained in chaotic states.

Since the internal state of HAVEGE includes thousands of internal

volatile hardware states, it is virtually impossible even for the user itself to reproduce the generated sequences.

HAVEGE presents an unprecedented throughput for an empirically strong random number generator: than 100 Mbits/s on recent PCs and workstations.

More information on HAVEGE:

<http://www.irisa.fr/caps/projects/hipsor/HAVEGE.html>

Postdoc proposal:

The precise post-doc subject will be defined by the candidate in collaboration with André Seznec (CAPS team from IRISA/INRIA at Rennes) and Nicolas Sendrier (CODES team at INRIA Rocquencourt)

Depending on the profile of the candidate, the subject may include work on the cryptanalysis/enhancement for HAVEGE, and/or on the new usages of HAVEGE (porting HAVEGE on new types of platforms such as PDAs, embedded systems, ..), but also new applications using the unprecedented throughput of the generator.

Desired profiles:

We will be considering candidates with a Ph. D. in any of the following domains: cryptology, random number generation, operating systems, security.

Computer architecture expertise will be provided by IRISA.

Contact and further information on the post-doc proposal:

André Seznec

sez nec@irisa.fr

tel: (33) 299847336

Further information:

–about IRISA/INRIA in general:

http://www.irisa.fr/accueil/index_uk.htm

–about CAPS team:

<http://www.irisa.fr/caps/>

–about funding and administrative informations:

<http://www.inria.fr/travailler/opportunités/postdoc.en.html>