# 2nd Call for papers: PROOFS 2014
# http://www.proofs-workshop.org/

*PROOFS: Security Proofs for Embedded Systems*
*Busan (Korea) — Saturday September 27, 2014*

**Venue**

PROOFS will take place at Busan, Korea, on Sept 27th, 2014.

**Publication**

* It is planned to publish revised papers of PROOFS 2014 as an LNCS post-proceeding (Springer Verlag).
* Selected papers will be reviewed by and published in a Special Section of the Journal of Cryptographic Engineering.

**Agenda**

The workshop will feature two/three invited talks and contributed talks.

* Submission deadline : Saturday June 7th, 2014
* Authors notification : Saturday August 9th, 2014
* Final version due : Saturday September 13rd, 2014
* PROOFS workshop venue : Saturday September 27th, 2014

**Programme Committee**

* Alessandro Barenghi, Politecnico di Milano, Italy.
* Loïc Correnson, CEA LIST, France.
* François Dupressoir, IMDEA, Spain.
* Emmanuelle Encrenaz, LIP6, France.
* Naofumi Homma, Tohoku U., Japan.
* Éliane Jaulmes, ANSSI, France.
* Debdeep Mukhopadhyay, IIT Kharagpur, India.
* Svetla Nikova, K.U.Leuven, Belgium.
* Renaud Pacalet, TELECOM-ParisTech, France.
* Bruno Robisson, ENSMSE, France.
* Graham Steel, LSV, France.
* Mehdi Tibouchi, NTT, Japan.
* Yongbin Zhou, CAS, China.

**Steering committee**

* Sylvain Guilley, TELECOM-ParisTech, France.
* Çetin Kaya Koç, UCSB, USA.
* David Naccache, ENS, France.
* Akashi Satoh, UEC, Japan.
* Werner Schindler, BSI, Germany.

**Local Committee**

* Prof. Howon Kim, Busan National Univ., Korea.

**Goal of the Workshop**

The goal of the PROOFS workshop is to promote methodologies that increase the confidence level in the security of embedded systems, especially those that contain cryptographic mechanisms.
Embedded system security currently consists mainly in security by obscurity solutions. This has obvious drawbacks:

* it requires costly black-box evaluation,
* there is no certainty about the correctness of the security, etc.

Formal methods allow to increase the trust level of digital systems. They are very appealing, for the following reasons:

* they are mature in theory, and there are tried and tested methods and tools,
* they have been applied on software for a long time, mainly for safety and conformance tests.

Some important security features (random number generation, physically unclonable functions, etc. ) rely on analog devices. Their correct functioning can be ascertained by techniques such as physical modeling and unitary experimental testing.
An important objective for the PROOFS workshop is to bridge the gap between both topics, and therefore to pave the way to « security by clarity » for embedded systems.