Title: **The Need for Parallel Ultra Fast Cryptographic Designs for Emerging Technologies**

Authors: Danilo Gligoroski[1], Svein Johan Knapskog[2], Simona Samardjiska[1]

1. Department of Telematics, NTNU, Norway
2. Q2S, NTNU, Norway

Abstract:

While the development of CPUs is continuing its exponential growth by introducing massive parallelism both internally for every CPU core, and by increasing the number of cores, the design of cryptographic primitives such as public key primitives or hash functions is still essentially sequential.

The consequence is that employment of secure cryptographic primitives in several emerging technologies that have potentially billions of user/client nodes or process tens of petabytes of data, has already hit the usability barrier. Relying solely on the existing sequential cryptographic primitives, the situation will go from bad to worse in the near future.
We offer several concrete examples from different emerging technologies:

1. Public key algorithms in "Social Networking" or electronic banking:
   Facebook, Yahoo, Gmail, and many commercial banks still use 1024 bit RSA, although the current NIST recommendation is 2048 bits.
2. Hash functions in "Cloud Computing":
   a. The designers of the increasingly popular OpenStack decided to use MD5 due to its efficiency.
   b. The designers of Apache's Hadoop, where the files have block size of at least 64 MB, decided to use CRC32 and MD5 due to efficiency reasons.
3. The size of medical images that must be digitally signed in the current DICOM standard can exceed 160 MB, consequently more than 99.9% of the computation efforts are for computing the hash of the image.

In order to overcome the mentioned performance barriers of the public key algorithms and hash functions **we need new parallel ultra fast cryptographic designs.**

Based on the positive experience of several previously conducted cryptographic contests (DES, AES, NESSIE, eSTREAM, SHA-3) where the cryptographic community was galvanized, motivated, gained new knowledge, and provided a huge amount of scientific feedback, **we propose to establish a regular mechanism for Cryptographic Contests** for addressing the cryptographic challenges for the emerging technologies.