20th International Conference on Computing in High Energy and Nuclear Physics (CHEP2013)

Contribution ID: **388** Type: **Poster presentation**

Efficient computation of hash functions

Monday, 14 October 2013 15:00 (45 minutes)

The performance of hash function computations can impose a significant workload on SSL/TLS authentication servers. In the WLCG this workload shows also in the computation of data transfers checksums. It has been shown in the EGI grid infrastructure that the checksum computation can double the IO load for large file transfers leading to an increase in re-transfers and timeout errors. Storage managers like SToRM try to reduce that impact by computing the checksum during the transfer. That may not be feasible, however, when multiple transfer streams are combined with the use of hashes like MD-5 or SHA-2.

We present two alternatives to reduce the hash computation load.
First we introduce implementations for the Fast SHA-256 and SHA-512 that can reduce the number of cycles per second of a hash computation from 15 to under 11. Secondly we introduce and evaluate parallel implementations for two novel hash tree functions:
NIST SHA-3 Keccak and Skein. These functions were conceived to take advantage of parallel data transfers and their deployment can significantly reduce the timeout and re-transfer errors mentioned above.

Primary author: Dr LOPES, raul (School of Design and Engineering - Brunel University, UK)

Co-authors: Prof. HOBSON, Peter (Brunel University (GB)); Dr FRANQUEIRA, Virginia (University of Central Lancashire, UK)

Presenter: Dr LOPES, raul (School of Design and Engineering - Brunel University, UK)

Session Classification: Poster presentations

Track Classification: Distributed Processing and Data Handling A: Infrastructure, Sites, and Virtualization