A Fast and Resource Efficient FPGA Implementation of Secret Sharing for Storage Applications

ABSTRACT

- Outsourcing data into the cloud gives wide benefits and opportunities to customers. Beside these advantages, new challenges such as confidentiality and accessibility have to be addressed. One approach to overcome these challenges is by applying secret sharing in a distributed storage setting, known as cloud of clouds approach. For this purpose we present a new hardware architecture of a wide parametrizable secret sharing core.
- Performance metrics for various applied bitwidths of secret words are given, which are crucial for benefits of higher level protocols in the cloud of clouds approach. Additionally, a complete system which is able to operate in a network environment is presented.
- The achieved throughputs are in the order of Gbit/s. It is significantly faster than similar comparable hardware architectures and orders of magnitude higher than software implementations.

EXISTING SYSTEM

- In recent years, cloud computing has emerged as a new way to access information technology (IT) and has transformed the digital landscape in many ways. The basic idea of the cloud is to centralize IT and leverage economies of scale to provide cheaper services.
- One major trend in cloud computing is away from dedicated monolithic storage solutions of specific vendors towards the use of cheap commercial offthe-shelf (COTS) hardware to reduce costs and avoid vendor lock-in.
- However, because of the high failure rate of COTS hardware, an additional layer of redundancy is needed to reach the desired reliability and availability of the overall storage system.

PROPOSED SYSTEM

- Outsourcing data into the cloud gives wide benefits and opportunities to customers. Beside these advantages, new challenges such as confidentiality and accessibility have to be addressed.
- One approach to overcome these challenges is by applying secret sharing in a distributed storage setting, known as cloud of clouds approach. For this purpose we present a new hardware architecture of a wide parametrizable secret sharing core.
- Performance metries for various applied bitwidths of secret words are given, which are crucial for benefits of higher level protocols in the cloud of clouds approach. Additionally, a complete system which is able to operate in a network environment is presented.

HARDWARE REQUIREMENTS

- Processor - Pentium –III
- Speed - 1.1 Ghz
- RAM - 256 MB(min)
- Hard Disk - 20 GB
- Floppy Drive - 1.44 MB
- Key Board - Standard Windows Keyboard
- Mouse - Two or Three Button Mouse
- Monitor - SVGA

SOFTWARE REQUIREMENTS

- Operating System : Windows 8
- Front End : Java /DOTNET
- Database : Mysql/HEIDISQL

CONCLUSION

- We presented the first hardware based computational secret sharing core including information theoretical secret sharing and information dispersal as dedicated components. Furthermore the proposed core is widely parametrizable and the influence of the secret word-width on the performance has been evaluated and shown in detail. We show the feasibility of significant performance increase when performing secret sharing on hardware. While a significant performance drop for higher bit-widths is observable, as it is in software, higher bit-widths are still processable with throughput orders of magnitudes higher than in software solutions.

REFERENCE

[1] H. Weatherspoon and J. Kubiatowicz, “Erasure coding vs. replication: A quantitative comparison,” in Revised Papers from the First International Workshop on Peer-to-Peer Systems, 2002.

[2] D. Demirel, S. Krenn, T. Loruenser, and G. Traverso, “Efficient and Privacy Preserving Third Party Auditing for a Distributed Storage System,” in International Conference on Availability, Reliability and Security, 2016.

[3] S. Krenn, T. Loruenser, and C. Striecks, “Batch-verifiable Secret Sharing with Unconditional Privacy,” in International Conference on Information Systems Security and Privacy, 2017.

CONTINUE

[4] A. Shamir, “How to share a secret,” Communications of the ACM, vol. 22, no. 11, pp. 612–613, nov 1979.

[5] H. Krawczyk, “Secret sharing made short,” in International Cryptology Conference on Advances in Cryptology, 1994.

[6] M. O. Rabin, “Efficient dispersal of information for security, load balancing, and fault tolerance,” Journal of the ACM (JACM), vol. 36, no. 2, pp. 335–348, 1989.