

July - OCT 2010

# the BIT

the bulletin of information technology



**RSET**  
RAJAGIRI SCHOOL OF  
ENGINEERING & TECHNOLOGY

**Rajagiri School of Engineering & Technology**  
Rajagiri Valley, Kakkanad, Cochin.

## From HOD's Desk



## Virtualization – need of the day

Now a days more and more enterprises are becoming IT oriented and more IT resources and IT applications are required. In this scenario the use of virtualization technology becomes more relevant. Virtualization technology enables single physical resource like server or OS or application to appear as multiple logical resources. It can also be used to aggregate multiple physical resources like storage or network and present them as single logical resources to the server and applications. By virtualization one can improve the asset utilization and reduce the cost of physical assets and can improve the efficiency, reduce the space, power and cooling and can have Greener IT.

The different ways of obtaining virtualization are

Server virtualization by which one can run multiple virtual machines on a single physical server with the support of special virtualization software like hypervisor. This can be achieved as full virtualization, para-virtualization or OS level virtualization.

Storage virtualization is obtained by adding a new layer of hardware/software between server and storage system and allows pooling of storage from different storage devices to a single pool. This enables easy grouping of storage devices from different suppliers and also reallocation of storage space or easy addition of fresh device.

Network virtualization supports the network administrator to manage, maintain and easily reconfigure the network from a single console without disturbing any device or cable.

Application virtualization in which the application program is installed in a server in a datacentre and its graphical output is available for a remote client and the client or the end user needs only the CPU and the RAM to run the software. By this the enterprise can easily maintain and control the application and keep it up-to-date.

Desktop virtualization becomes relevant when the end user's PC is being executed on a central server. By this type of virtual desktop infrastructure the IT team can manage the client system updates and patches from a single centralized location and can provide high data security and ensure business continuity.



## Staff Corner



Ms. Nithya Joy

CryptoManiac processor is a fast and flexible co-processor for cryptographic workloads. This design that runs the standard Rijndael cipher algorithm 2.25 times faster than a 600MHz Alpha 21264 processor. Moreover, the implementation requires 1/100th the area and power in the same technology. The trend towards virtual private networks (VPNs) and secure IP (IPSEC) will further emphasize the significance of cryptographic processing among all types of communication. CryptoManiac, addresses the primary bottleneck in private-key ciphers, namely efficiency, through the application of an efficient VLIW architecture with a well-matched instruction set and functional unit resources. The programmable feature supports many private-key ciphers, in contrast to the IDEA engine.

By combining CryptoManiac processors into parallel configurations, we are able to scale cryptographic performance for applications with inter-session and inter-packet parallelism. CryptoManiac processor and analyze its performance using architectural and physical design models. Cryptographic co-processor design requires a thorough understanding of the nature of private key cryptography, its essential operations, and its inherent bottlenecks. The selected eight cipher kernels for cryptanalysis. They are 3DES, Blowfish, IDEA, Mars, RC4, RC6, Rijndael, and Twofish. These eight ciphers are selected because each is generally considered a strong cipher as they have undergone aggressive review and cryptanalysis.

### CryptoManiac Architecture

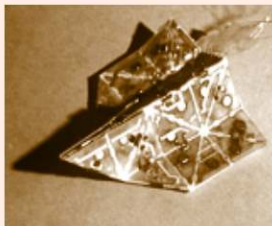
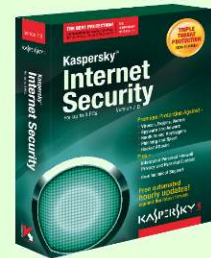
Cryptography is a Greek word that literally means the art of writing secrets. Cryptographic algorithms (or ciphers, as they are often called) are special programs designed to protect sensitive information on public communication networks. During encryption, ciphers transform the original plaintext message into unintelligible ciphertext. Decryption is the process of retrieving plaintext from ciphertext. Two forms of cryptography are commonly used: secret-key ciphers and public-key ciphers. Secret-key ciphers (sometimes referred to as symmetric-key ciphers) use a single private key to encrypt and decrypt. Public-key ciphers (or asymmetric-key ciphers) uses a well-known public key to encrypt and require a different private key to decrypt.

In order to reach better cipher performance, efficiency becomes the goal of our design. In pursuing our goal, the design will focus on a simple micro architecture, an efficient implementation of operations, and more efficient use of the clock cycle. There are many potential applications of the CryptoManiac processor. The main two applications are: secure web server and disk controller. analyze the performance of general purpose and cryptographic processors using I/O trace-based simulation, measuring the response time for each processor configuration to service requests. The instruction combining feature not only made executing instructions with varied latencies efficient, but the design catered to cryptographic processing.



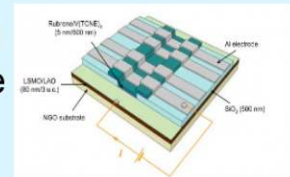
## New@IT

Kaspersky Lab announced the launch of the latest versions of its flagship consumer products Kaspersky Internet Security 2011 and Kaspersky Anti-Virus 2011.



By combining origami and electrical engineering, researchers at MIT and Harvard are working to develop the ultimate reconfigurable robot — one that can turn into absolutely anything. Studded with magnets and electronic muscles known as actuators, a prototype robot developed at MIT can automatically fold itself into an airplane or an origami boat.

Researchers at Ohio State University have demonstrated the first plastic computer memory device that utilizes the spin of electrons to read and write data.



The first prototype robots capable of developing emotions as they interact with their human caregivers and expressing a whole range of emotions have been finalized by researchers at the University of Hertfordshire

Fujitsu has announced the global availability of the new Primergy RX900 S1 x86 eight-socket rack server to drive x86 economical benefits into the mission-critical computing realm.



# EVENTS

## Compiler Workshop



With support from ISTE and Dept. of Computer Science and Engineering NIT, Calicut, the Dept. of Information Technology and Dept. of Computer Science of RSET organized a staff development programme on Compiler Construction ( June 21st to July 2nd 2010 ) for the faculties and research scholars in various Engineering colleges.



Dr. P. X Joseph, HOD, Dept. of Computer Science, Rajagiri School of Social Science was the chief guest on the inaugural day.

The resource persons included Dr. Vineeth K Paleri, NIT Calicut, Dr. K.Murali Krishnan, NIT Calicut and Mr.Biju B Varghese, MBCET Trivandrum. The faculty members Mr.Unnikrishnan C, Ms.Shimmi Asokan, Ms.Sminu Izudheen, and Ms.Preetha K G, of RSET contributed for the workshop. Prof. Paulose Jacob, the eminent academician from CUSAT was the chief guest on the valedictory function. Prof. Sunil Kumar C.P, Secretary of ISTE released the proceedings CD.



## ITRAX Inauguration



Mr. B. Remani, Additional Director, CDAC, Trivandrum inaugurated the activities of ITRAX for the academic year 2010 - 2011, on 27th July 2010. He delivered a talk on "Cyber Security-Challenges and Solutions".

ITRAX conducted a Technical Quiz for IT students on 3rd August 2010. Two teams from each batch participated. Jesvin Jose and Mahesh Mohan (S7 IT) came in the first place, and Giffin George and Vishnu M (S7 IT) came in the second place.

