IRIIE 2010

IIUM Research, Innovation & Invention Exhibition 2010 (IRIIE 2010)

ENHANCING QUALITY RESEARCH & INNOVATION for SOCIETAL DEVELOPMENT

functionality.

P-126 Unique Class Encryption (UCE) substitution boxes (S-Boxes) using mysterious Quranic objects for block ciphers in ICT Security

***Ahmad Faizul Shamsudin**, Mohd. Adam Suhaimi, Rusydi Hasan Makarin, Abi Dzar Jaafar*
Dept. Computer Science, Kulliyyah of Information & Communication Technology
International Islamic University Malaysia

Unforeseen attacks on ICT systems incurred billions of dollars of losses to public and private communities. The current parametric encryption algorithms suffer the unconventional and paranormal attacks. A search for a new paradigm against the unforeseen and paranormal attacks lead to an invention called Unique Class Encryption (UCE) that is based on the non-parametric and mysterious verses of the Al-Quran.Earlier, the Al-Muqatta'at based UCE was developed and tested in a Red-Hat cluster funded under IRPA and completed in 2006. The Al-Muqattaat UCE was patent filed in 2007. A block cipher is required as a medium to translate the non - parametric Al-Muqatta'at algorithm into a suite so that it can be an embedded system for FPGA chips. This would require the construction of substitution boxes (S-Boxes) with the other non-parametric objects from Al-Muawwidzatain and Ayatul Qursi verses. It is a completed Type A research endowment fund project in August 2009. The approach was to construct bigger S-Boxes that have no algebraic relations. The random bijective 8-bit S-Boxes that used the non-parametric and non-deterministic components of the Al-Qura'an would transform the objects into specific values for the S-Box construction. Thus the vital component of the non-parametric UCE block ciphers, that are the S-Boxes were developed. About 13.5 million of 8-Bit S-Boxes were generated. The non-linearity and differential uniformity tests by MIMOS Cyber-security Laboratory showed the standing of UCE S-Box to be equivalent to that of Khazad's block ciphers. Collaborative research with MIMOS Cyber-security Laboratory are using the strong UCE S-Boxes to develop hybrid round functions and key distribution algorithms to construct the UCE block cipher. This on-going phase is conducted under Type B research endowment fund. In an envisaged pre-commercialization phase, the UCE block cipher would be implemented in FPGA chips. The potential use for the UCE encryption chips will be as embedded cryptographic system in VPN routers, gateways, computing machines and security device firmware.

P-127 Development of an Intelligent Robotic Donation Box for IIUM Mosque

***M.J. E Salami**, A. M Aibinu, Siti Aisha Bt Mansor, Safinas Qadri*
Mechatronics, Kulliyyah of Engineering
International Islamic University Malaysia

The design and development of an intelligent robotic donation box is presented in this project. The mobile robotic system is equipped with the capability to collect donation from the people within the mosque during a specified period of time before the compulsory prayer commences. Also fitted with the ability to attract the attention of people by making audible sound, recognize person and wait for his/her donation as well as to avoid obstacles due to either a person praying, the wall or any other detected objects. The device covers a given number of rows before returning to place of storage.

P-128 A New Technique to Improve the Machinability of Hardened Steel AISI H13 in End Milling

***AKM Nurul Amin**, Suhaily Mokhtar, Anayet U Patwari, Nurhayati Ab. Razak*
Department of Manufacturing and Materials Engineering, Kulliyyah of Engineering
International Islamic University Malaysia

Hardened materials like AISI H13 steel are generally regarded as difficult to cut materials because of their high hardness due to high carbon content, which however allows them to be used extensively as the hot working tools like, dies and moulds. The challenges in machining this steel in hardened state led to many research works dedicated towards enhancing its machinability. In this work, preheating technique has been used to improve machinability of the material under different cutting conditions. An