MUHAMMAD REZAL BIN DATO' DR. KAMEL ARIFFIN

Ph.D. (Universiti Kebangsaan Malaysia)

Assoc. Prof. Dr.
Department of Mathematics
Faculty of Science
Tel: 03 89466838
Fax: 03 89437958
rezal@upm.edu.my

EXPERTISE

Assoc. Prof. Dr. Muhammad Rezal bin Dato' Dr. Kamel Ariffin is Program Head for Mathematical Cryptography at the Institute for Mathematical Research, UPM. He focuses in designing and cryptanalyzing public key cryptography primitives. Since appointed as Lecturer in 2005, has published various 74 scientific writings (22 in indexed proceedings), acquiring 5 research grants totaling >RM450,000, obtained 8 innovation awards (5 international), reviews submissions for a number of international conferences, invited as Visiting Researcher at the Univerisite de Caen, France and the Chinese Academy of Science, China, 2 research products patented in Malaysia and 1 in USA and has generated more than RM 1 million in sales and services through UPM (either in cash or in kind). Occasionally he is invited to give presentations and expert opinions for organizations in Malaysia. He is on the International Journal of Cryptology Re-search editorial board and has chaired 5 International cryptology conferences since 2008.

Current Research Interest

- **Post Quantum Public Key Cryptosystems (PQPKC)**

Post 2010, a number of PQPKC based on various NP-hard problems have been put forward, but setbacks not favorable for large scale implementation can be found and need to be addressed. The subset sum problem, one of the earliest NP hard problems to be utilized, can be explored. Previous attempts have failed due to the need to design a trapdoor. It is conjectured that maybe one needs to generalize the subset sum problem in order to successfully utilize it.

- **Integer Factorization Problem (IFP)**

IFP has been utilized as a source of difficulty in designing public key cryptography since late 1970's. Research in identifying cases where factoring product of integers is not difficult has become popular. Integers have many internal structures not yet properly understood. It is through this research, one can understand this issue, and avoid such integers to be utilized for cryptography.

LINK TO POSTGRADUATE FIELD OF STUDY:
Mathematical Cryptography, Pure Mathematics

ADDITIONAL INFORMATION: