SE&T Colloquium Series-Winter 2012

Speaker	Dr. Tai-Chi Lee Department of Computer Science and Information Systems
Title	***An Elliptic Curve Cryptosystem***
Abstract	The majority of products that use public-key cryptography for encryption/decryption use RSA (Rivest-Shamir-Adelman) algorithm. But as we know, the key length for secure RSA has increased over the years. This would demand a heavy computing power for applications, especially for electronic commerce site that process a large number of transaction. Recently, a different approach of generating public key based on Elliptic Curve Cryptography (ECC) has begun to challenge the weakness of RSA. ECC is a form of encryption using elliptic curves to encode messages based on public key exchange. ECC can achieve strong encryption using keys of shorter bit length than would be needed for comparable security using RSA encryption. Its security relies on the problem of computing logarithms on the points of an elliptic curve. The main attraction of ECC is that it appears to offer equal security for a far smaller key size, thereby saving the processing overhead. To improve the strength of encryption and the speed of processing, the public key and the private key of ECC are used in 3BC (Block Byte Bit Cipher) algorithm, which generates session keys for the data encryption. We will be investigating a novel approach of hardware co-design implemented in Verilog Hardware Description Language (VHDL), which produces hardware algorithm components to place onto the FPGAs, thereby it will speed up the computation with a built-in custom arithmetic Logic Unit (ALU).
Date	Tuesday, April 17
Time	4:10-5:00pm
Place	Pioneer 240
	Refreshments will be served at 4:00pm.