Abstract:

For pseudorandom number generators (PRNG) which are widely applied for non-cryptographic use, MT19937 generator is one of the quite popular PRNG(s). The extraordinary high period outperforms other types of generators such as Multiplicative Linear Congruential Generators (MLCG). But the most distinctive feature should be its equidistribution property. Its high value of k in k-distribution for typical d-bit resolution, such as d=32, may explain why it can pass most of the statistical tests, for example, Birthday Spacings test. MT and its other Linear Feedback Shift Register (LFSR) cousins are mostly implemented over GF(2) field. This choice has many advantages, such as performance and allowing the use of Mersenne primes in MT. And one could achieve higher period with these prime numbers.

Based on these factors, the use of p=2 seems unquestionable. But MT19937 fails the Linear Complexity in the Crush battery of tests in TestU01 package.

If one would have this effect in the use of LFSR types of generators, one may consider applying other types of generators besides LFSR generators. But equidistribution is still a desirable feature which we cannot afford. One possible alternative would be applying a LFSR over GF(p) with p not equal to 2 such that the effect, which is fail to comply with the Linear Complexity test statistics deduced from GF(2), is substituted with the effect which is based on GF(p) with p not equal to 2.

In this research, we would build a LFSR generator over GF(p) with equidistribution feature, then apply the generator to different tests. We would expect the generator passes many tests and especially the Linear Complexity test. This would demonstrate that the use of LFSR over GF(p) with p not equal to 2 should be reconsidered and a battery of tests should have a GF(p) version of Linear Complexity test.

About the Speaker:

Tso Chi Wai is a part-time PhD Student at the Department of Computer Science, The University of Hong Kong. His supervisor is Dr. S.M. Yiu. His research interest is Cryptography.