Further results on the security of MQ_DRBG

Grigory Marshalko, Alexey Pokrovskiy

In 2011 ISO standardized [2] a family of deterministic pseudorandom bit generators MQ_DRBG, based on multivariate quadratic functions satisfying certain properties. The security of the generator could be described in terms of complexity of solving the corresponding system of multivariate quadratic equations.

In our previous article [1] we proposed two different techniques for constructing systems of equations, which satisfy the restrictions of the standard, but could be solved with less complexity than stated in [2]:

- The first technique is based on guessing the part of the variables, which leads to further linearization. The possibility of constructing such systems is based on the existence of a linear code with given parameters.
- The second technique exploits the meet-in-the-middle approach by splitting variables into two parts and constructing part of polynomials as sums of two polynomials which depend on different parts of the variables. For several parameters of MQ_DRBG one can construct such systems by random choice.
- One can use the combination of both techniques.

Here we study the possibility of application of our methods to various instances of MQ_DRBG with different values of parameters, and one method for detection of such systems.

As for the first problem, we've found appropriate binary codes for several values of parameters of MQ_DRBG which allow to construct "weak" systems of equations. The most profound decrease of complexity was for the system with $n = 272$ variables and $r = 256$ output bits: from 2^{256} stated in [2] down to 2^{153} binary operations.

As for the second problem, our observation is that the distribution of the rank of multivariate quadratic functions could be skewed (for example, the first technique gives a system, where all functions have the same rank). For a randomly selected functions this distribution could be obtained through the weight spectrum of Reed-Muller linear code $R(n, 2)$.

The distribution of quadratic functions with restrictions proposed in [2] is unknown, nevertheless, our experiments show that for many instances of MQ_DRBG nearly every randomly selected set of functions satisfies the restrictions of [2]. This implies that the distribution of rank of such systems is indistinguishable from the distribution of rank of randomly selected functions without restrictions, when the number of equations is equal to the number of equations specified in [2].

This gives an empirical statistical criterion for detection of possibly "weak" systems, by applying any goodness-of-fit test for the distribution of rank of subsystems corresponding to the output bits, bits of internal state, and their joint distribution.

Our experiments show that the distribution of systems, generated with the second technique, is practically indistinguishable from the distribution of the random one.

References

[1] V.O. Drelikhov, G.B. Marshalko, A.V. Pokrovskiy, On the security of MQ_DRBG, http://eprint.iacr.org/2011/548.pdf

[2] ISO/IEC 18031 – Information technology – Security techniques – Random Bit Generation.