On Single Cycle Functions

Ilya O. Levin, eli@literatecode.com

Abstract: The purpose of this note is to present a few invertible functions with a single cycle.

In [1], Klimov and Shamir described the nonlinear invertible function with a single cycle which requires only three primitive operations $x \rightarrow x + (x^2 \vee C)$, where $C = *..*1*1_2$. Here we introduce a few more functions of same properties. All functions are mod 2^n.

The first function is a straightforward modification of the referenced one where x^2 replaced with a bit rotation:

$$x \rightarrow x + ((x{<}{<}{<}a) \vee C)$$

This function has a single cycle for $0 < a < 6$ and $C = *..*11_2$, $C < n$. However, not all of such pairs (a, C) produce a single cycle. If $n = 32$ then the proper pairs are: (1, 7), (1, 11), (1, 15), (1, 23), (1, 27), (2, 3), (2, 7), (2, 11), (2, 15), (2, 23), (2, 27), (2, 31), (3, 7), (3, 15), (3, 23), (3, 31), (4, 15) and (5, 31). Clearly, the function simply renders to $x \rightarrow x + (2^t x \vee C)$ for most pairs.

The next function compliments bit rotation with bit inversion

$$x \rightarrow (a(\neg x)) {<}{<}{<}\, b$$

Again, not every pair of (a, b) produce a single cycle, but only a few from those with even a. For $n = 32$ the pairs are: (6, 31), (12, 30), (14, 31), (22, 31), (24, 29), (28, 30) and (30, 31). The statistical properties of this function seems to be weaker than the properties of the other described functions.

The third function uses bit rotation and bit inversion together with right shift

$$x \rightarrow x + (x {<}{<}{<}\, a\,) + ((\neg x) >> b)$$

This function has a single cycle for $2 > a > n$ and $b = n - a$. Smaller a gives better statistical quality thus $a = 3$ is a good choice. The function takes five operations though.

Another function is a LCG of form

$$x \rightarrow ax + C$$

It is a single cycle invertible function when a is a 5^t and C is an odd number.

The last function to introduce is

$$x \rightarrow x^2 + ax + C$$

where C is odd and a is a form of $(2^t + 1)$. This function is not exactly a single cycle, but it is a single cycle among the odd numbers regardless of initial x. It is a very helpful function to substitute an odd constant C in above functions or wherever else a generic odd parameter may be involved.

In conclusion let us remind that a single cycle invertible functions have some properties to be careful about. This is the first 56 outputs of the $x \rightarrow x + (x^2 \vee 5)$ for $n = 32$ and $x_0 = 12345678_{\text{hex}}$:

```
30292ebd 113ba64a f75bb3af e5e3e554 ae4b48e9 37952cfe c3297903 51534f10
ce1e3015 e81211d2 0ad7a217 801ac02c 194cc7c1 01c26746 3d83ce6b 23762f28
9505e56d 3ae415da f111937f faeaac84 a07c5099 0e144c0e 8edc9cd3 8d9672c0
ba0602c5 1f49ae62 c5f70be7 4446b65c 607da771 125c4756 840d183b d45635d8
ccc95c1d cb78376a e6d6ef4f d29f89b4 7a49b049 1150251e 4571d4a3 8bf63470
fdf3e575 a9bc6cf2 5f8981b7 4921728c dc7a6f21 b02c1166 ec6ac60b cebbca88
31a6b2cd 0a646afa 5268671f 21225ce4 b76707f9 2004982e bbeb4073 2146f420
```

The last digits pattern is obvious. Quoting [1]: "Note that the i-th least significant bit in any iterated single cycle T-function repeats every 2^i steps and depends only on the first i state bits, and thus the most significant bits are much stronger than the least significant bits".

References:

[1] A. Klimov, A. Shamir, "Cryptographic Applications of T-Functions," Selected Areas in Cryptography 2003 (M. Matsui, R. J. Zuccherato, eds.), vol. 3006 of LNCS, pp. 248-261, Springer-Verlag, 2004. (Online copy at http://www.wisdom.weizmann.ac.il/~ask/t1.ps.gz)