On Nonlinear Filter Generators

Markus Dichtl

Siemens Corporate Technology
Email: Markus.Dichtl@mchp.siemens.de

Abstract. In this paper the bits in a linear feedback shift register are treated as if they were independent random variables. A necessary condition for filter functions which result in independent random output bits is given. An example shows that the sufficient condition given by Golić in [2] is not necessary.

1 Nonlinear Filter Generators

It is a common technique to compute the output bits of a stream cipher by a nonlinear function applied to some stages of a linear feedback shift register. The nonlinear function is called filter function, and the generators are called nonlinear filter generators.

In [4] Rueppel gives an overview of known results on such generators, which mainly concern the linear complexity of the resulting bit stream. But surprisingly the consequences of the fact that the same bit is used in the input of the filter function repeatedly started to be discussed in the open literature only very recently. In 1994 Anderson ([1]) introduced a new attack on nonlinear filter generators and showed that it worked for some nonlinear filter functions used in practical applications. He suggested that the filter functions needed further study. This suggestion was taken up by Golić who treated the criteria nonlinear filter functions should meet extensively in [2]. Whereas Anderson had only discussed the nonlinear filter functions, Golić also pointed out the importance of the positions of the tabs for the input of the filter function. Nonlinear Filter Generators have also been discussed from another point of view by Lai and Massey in [3]. In their paper the term "Binary Filter with Input Memory" is used. The authors consider the question of delay-d invertibility, that is, whether it is possible to determine the input bits from the output bits with a delay of at most d clocks.

2 The Model

In this paper, we treat the bits of the shift register as if they were independent random variables with probability $1/2$ of being 0 or 1. This assumption holds for the rest of this paper, even when it is not explicitely mentioned. This model was introduced in [1], but there the emphasis was on information leakage. In [2] the requirement for the nonlinear filter function was given, that under the assumptions of random bits in the shift register, the output bits must be independent random variables with probabilities of $1/2$ of being 0 or 1. Golić also gave a

sufficient condition for the filter function to meet this requirement, namely that the filter function is affine in the input from the leftmost or rightmost tab. Furthermore he conjectured that these are the only solutions which are independent of the choice of the tabs.

In this paper, we only consider the question of choosing the filter function in order to get independent random bits in the output. However, it should be noted that this is not sufficient for filtering the output of linear feedback shift registers. [2] gives a list of 9 requirements a nonlinear filter generator should meet.

3 A Necessary Condition

In this sections we give a condition which is necessary to produce independent random bits in the output of the filter function.

Remark. In order to get zeros and ones at the output of the filter function with probability 1/2, the filter function must be balanced.

In spite of the name of the generator, we do not exclude linear filter functions f. The following theorem is also valid for them.

Theorem 1. *Let $f : GF(2)^n \longrightarrow GF(2)$ $(n \in \mathbb{N})$ be the filter function of a nonlinear filter generator. If the output of the filter functions are random independent bits with probability 1/2 of being 0 and 1, then there exists at most one index j $(1 \leq j \leq n)$ such that the function $f_j : GF(2)^{n-1} \longrightarrow GF(2)$ with $f_j(x_1, \ldots, x_{j-1}, x_{j+1}, \ldots, x_n) = f(x_1, \ldots, x_{j-1}, 0, x_{j+1}, \ldots, x_n)$, that is the function for which the j-th input bit of f is fixed to 0, is not balanced.*

Proof. Let j and k be positive integers less or equal to n with $j \neq k$. Let p be the probability that f_j is zero, and q the probability that f_k is zero.

Each bit of the shift registers goes, at different times, to the inputs x_j and x_k of f. Let y_j be the output of f when such a bit b goes to x_j and y_k the output of f when the same bit b goes to x_k.

When b is zero, the probability of $y_j y_k$ to be 00 is pq. When b is one this probability is $(1-p)(1-q)$. The mean of the two probabilities must be 1/4. This leads to $2p(2q-1) = 2q-1$. This implies $p = 1/2$ or $q = 1/2$, f_j or f_k is balanced. □

4 Looking for Examples

Golić constructed filter functions of the form $f(x_1, \ldots, x_n) = x_1 + g(x_2, \ldots, x_n)$ where x_1 must come from the leftmost or rightmost tab of the shift register, and g is an arbitrary Boolean function. These filter functions give independent random output bits.

But are they the only functions to achieve this?

When we consider functions of three variables, and use tabs at three subsequent stages of the shift register, the answer (found by brute force search) is yes.

When we look at functions of four variables, and use tabs at four subsequent stages of the shift register, the answer is no.

The following table gives a Boolean function f of four variables which is not affine in any of the variables. f_2 is not balanced, the other f_j are, according to Theorem 1.

x_1	x_2	x_3	x_4	$f(x_1, x_2, x_3, x_4)$
0	0	0	0	0
0	0	0	1	0
0	0	1	0	0
0	0	1	1	0
0	1	0	0	1
0	1	0	1	1
0	1	1	0	1
0	1	1	1	1
1	0	0	0	0
1	0	0	1	0
1	0	1	0	1
1	0	1	1	0
1	1	0	0	1
1	1	0	1	1
1	1	1	0	0
1	1	1	1	1

That f with four subsequent tabs produces independent random output bits can be verified by applying Lemma 1 from [2].

There are choices of tabs for which f does not produce independent random output bits, so this example is not in conflict with Golić's conjecture, that his construction may give the only functions which work for all positions of the tabs.

As a matter of fact, for tabs at the stages of the shift register indexed 0, 1, 3, and 7, all filter functions with four inputs which give independent random output bits are according to the Golić construction.

5 Conclusion and Open Questions

In [2] Golić gave a sufficient condition for a filter function to produce independent random output bits. In this paper we gave a necessary condition. Of course it would be interesting to have a necessary and sufficient condition. Our observations from the previous section show that such a condition must involve the position of the tabs of the shift register.

Perhaps the following question is easier to solve: Are all filter functions which give independent random output bits for tabs which form a full positive difference set according to the Golić construction? This would imply that Golić's conjecture is true.

6 Acknowledgement

I would like to thank a referee for bringing [3] to my attention and for sending me a copy of this paper.

References

1. Anderson, R.: Searching for the Optimum Correlation Attack, in Fast Software Encryption, Second International Workshop, Leuven, Belgium, December 1994. Proceedings, Lecture Notes in Computer Science, vol 1008, B. Preneel (Ed.), Springer Verlag 1995, pp. 137–143.
2. Golić, J.: On the Security of Nonlinear Filter Generators, in Fast Software Encryption, Third International Workshop, Cambridge, UK, February 1996. Proceedings, Lecture Notes in Computer Science, vol 1039, D. Gollman (Ed.), Springer Verlag 1996, pp. 173–188.
3. Lai, X. and Massey, J.: Some Connections between Scramblers and Invertible Automata, Proc. 1988 Beijing Int. Workshop on Info. Theory, Beijing, China, July 4-8, 1988, DI-5.1 - DI-5.5
4. Simmons, G. (ed): Contemporary Cryptology: The Science of Information Integrity, IEEE Press 1992