On the security of shift register based keystream generators

Jovan Dj. Golić

Information Security Research Centre, Queensland University of Technology
and
School of Electrical Engineering, University of Belgrade

Abstract. Security against divide and conquer correlation attacks of binary keystream generators based on regularly or irregularly clocked shift registers combined by a function with or without memory is discussed. A comprehensive survey of the results published in the literature is presented, some new concepts are introduced, and many open problems are pointed out.

1 Introduction

Stream ciphers with keystream generators are generally considered as reliable tools for secure communication, although it appears practically impossible to prove that any particular keystream generator scheme is secure. One can only prove that a scheme is secure against certain types of divide and conquer cryptanalytic attacks. However, little is published regarding the cryptanalysis of such schemes, except for some elementary ones.

In this paper we consider the immunity of shift register based binary keystream generators to divide and conquer correlation attacks. Shift registers can have linear or nonlinear feedback, can be autonomous or not, can be clocked regularly or irregularly, and can be combined by a memoryless function or a function with memory. The secret key is assumed to control the shift registers initial contents and the initial states of the clock-generators appearing in the scheme. The problem is to find out the conditions under which it is possible or impossible to reconstruct the initial contents of individual shift registers knowing a segment of the keystream generator output sequence, based on the correlation/statistical dependence between the keystream sequence and a set of the shift register sequences. If instead of the blind search over the initial contents of the corresponding shift registers a faster search is possible, then we deal with the so-called fast correlation attacks.

Another type of cryptanalytic attacks on clock-controlled shift registers is a divide and conquer attack on the initial state of a clock-generator based on the collision test Anderson [1] or, more generally, on the linear consistency test Zeng, Yang, Rao [42], Anderson [2]. Cascades of (0, 1)-clocked (stop-and-go) and (k, m)-clocked shift registers were cryptanalysed in Chambers, Gollmann [3] and Gollmann, Chambers [18], respectively, based on a specific lock-in effect. Recently, Menicocci [24, 25] has developed correlation-like attacks on cascades of stop-and-go shift registers. Intrinsic repetition of symbols in stop-and-go shift registers seems to be a cause for their potential insecurity. In this paper, only the clock-controlled shift registers that are clocked at least once per output symbol are considered.

Note that in general, an arbitrary shift register based binary keystream generator seems to be vulnerable to a divide and conquer attack in which the overall initial state uncertainty is reduced by the initial content uncertainty of the longest shift register, based on the fact that the output keystream sequence is known, see Dawson, Clark [7], Dawson [6], and Rubin [33], for example.

2 Regular clocking and no memory

When the shift registers are clocked regularly and the combining function is memoryless, it is possible to apply the well known ciphertext-only correlation attack based on the Hamming distance between two binary sequences of the same length Siegenthaler [37]. He showed that, given a sufficiently long segment of the generator output sequence, one can statistically reconstruct with arbitrarily small error probability the initial content of any register whose output is correlated to the generator one. He also obtained an estimate of the necessary length of the observed keystream sequence which is essentially linear in the shift register length. This attack also applies in general, to an arbitrary mth-order correlation immune Boolean function. Recall that according to Siegenthaler [38], a Boolean function f of n variables is said to be mth-order correlation immune, $0 \leq m \leq n-1$, if m is the maximum integer such that the random variable f is statistically independent of every set of m random input variables, assuming that the input variables are balanced and independent. It is interesting to note that $m < n-1$ holds for nonlinear Boolean functions Siegenthaler [38]. Due to Xiao, Massey [39] the output of a mth-order correlation immune function is correlated to at least one linear function of exactly $m+1$ input variables. It is worth noticing that there may exist a nonlinear function of these $m+1$ input variables that is more correlated to the considered Boolean function than the linear ones. Consequently, the initial contents of the corresponding $m+1$ shift registers can be recovered by applying the same correlation attack. Use of the contingency statistical tests, which take into account the full statistical dependence between the $m+1$ inputs and the output, is also possible if m is not large. When the $m+1$ shift registers have linear feedback and their feedback polynomials f_i, $0 \leq i \leq m$, are pairwise coprime, it is even possible to reconstruct their initial contents separately. For example, the generator output and the output of the shift register with the feedback polynomial f_0 become mutually correlated when filtered through the linear filter with the transfer function $f_1 f_2 ... f_m$. This essentially means that every memoryless combiner becomes zero-order correlation immune when the inputs are not regarded as purely random binary sequences.

Although being a divide and conquer one, the described statistical procedure requires the exhaustive search over all possible initial contents of the corresponding shift registers. The concept of a fast correlation attack was first introduced in Meier, Staffelbach [21] where a bit-by-bit reconstruction procedure based on iterative probabilistic and threshold decoding is proposed for linear feedback shift registers. The basic underlying ideas regarding the probabilistic decoding of low-density parity-check linear codes can be found in Gallager [10] and Massey [19]. After the pioneering work of Meier and Staffelbach, various algorithms of this type have been published and theoretically or experimentally analysed so far Zeng, Huang [40], Forré [9], Zeng, Yang, Rao [41], Mihaljević, Golić [26, 27, 28, 30], Chepyzhov, Smeets [4], and Živković [43]. All of them share two basic features, that is, an iterative error-correcting algorithm and a method of obtaining low-density parity-checks. If one uses a simple method for parity-check generation proposed by Meier, Staffelbach [21], then the computational complexity remains essentially linear in the shift register length, but the reconstruction capability is limited. If one forms all the parity-checks up to a certain weight and length, based on all the multiples of the feedback polynomial Chepyzhov, Smeets [4], the performance is improved but at a cost of the computational complexity exponential in the shift register length. Another method of obtaining orthogonal low-density parity-checks based on the powers of the shift register state-transition matrix was proposed by Mihaljević, Golić [26, 30].

On the other hand, the convergence of various iterative error-correcting algorithms has been analysed both experimentally Meier, Staffelbach [21], Mihaljević, Golić [26, 27] and theoretically Zeng, Huang [40], Zeng, Yang, Rao [41], Živković [43], Chepyzhov, Smeets [4], and Mihaljević, Golić [28]. It appears that the Bayesian iterative error-correcting algorithm Meier, Staffelbach [21], Živković [43], Mihaljević, Golić [27], based on iterative recalculation of the noise posterior probabilities using the posterior probabilities from the current iteration as the prior probabilities for the next one, is the most efficient one suggested so far. However, deriving an analytical expression for a necessary and sufficient condition for this algorithm to converge to the true solution, still remains an open problem. Živković [43] obtained a mathematical characterisation of the convergence process, but not a convergence condition in terms of the parameters of the problem as well. A convergence condition theoretically derived in Mihaljević, Golić [28] seems to be a good approximation of the desired necessary and sufficient condition. It essentially claims that the Bayesian iterative algorithm based on orthogonal parity checks converges to the true solution if and only if

$$\frac{p}{1-p}\prod_{w\in\Omega}\left(\frac{1+(1-2p)^w}{1-(1-2p)^w}\right)^{N_w} > 1 \tag{1}$$

where p is the correlation noise probability, N_w is the number of parity checks of weight w, the weight being defined as the number of bits involved in a parity check minus one, and Ω is the set of possible weights used in a given attack. More precisely, this condition applies to a simplified iterative algorithm in which in each iteration the prior probabilities are assumed to be equal for every bit of noise.

3 Regular clocking and memory

Use of functions with memory in keystream generators in order to avoid the trade-off Siegenthaler [38] between the linear complexity and correlation immunity was suggested by Rueppel [34]. He extended the notion of correlation immunity to combiners with memory and showed that one can achieve the maximum order correlation immunity, regardless of the linear complexity, by using only one bit of memory. Several combiners with one bit of memory have been proposed so far, for example, the summation generator Rueppel [35], Massey, Rueppel [20] and the universal logic sequences Dawson, Goldburg [5]. Meier and Staffelbach [23] investigated a general combiner with one bit of memory from the bitwise correlation standpoint. Namely, they considered the correlation between each bit of output and linear functions of successive inputs and derived the corresponding sum of the squares of the correlation coefficients, thus extending their result for memoryless combiners Meier, Staffelbach [22]. They also introduced the concept of the correlation conditioned on the output.

A general case of regularly clocked shift registers combined by an arbitrary function with M bits of memory was investigated by Golić [14]. He showed that for a general combiner with M bits of memory there exist a linear function of at most $M+1$ successive output bits and a linear function of at most $M+1$ successive input bit vectors that produce correlated binary sequences. Also, an efficient procedure based on the linear sequential circuit approximation of a Boolean function with memory for finding such pairs of linear functions is developed. Moreover, when the shift registers have linear feedback with pairwise coprime feedback polynomials, it is demonstrated how to obtain correlated linear functions of the output and individual inputs, respectively, which would imply that every such combiner with memory is zero-order correlation immune. However, unlike memoryless combiners, it might happen that every linear function of an input that is correlated to the output is identically equal to zero, which means that the correlation attack is not possible. Note that the complete initial content reconstruction is possible only if the polynomial corresponding to the input linear function is relatively prime to the shift register feedback polynomial. If the shift register feedback polynomial divides the linear function polynomial, then the reconstruction is not possible at all. Once a pair of suitable correlated input and output linear functions is obtained, it is then possible to apply the same fast correlation attacks as for the memoryless functions. It follows that the noise probability is in general closer to one half than in the memoryless case, which makes these schemes more secure, especially when M is large. According to the linear sequential circuit approximation attack, large distance from the affine functions for the balanced output function and for all the component functions in the next-state function of the combiner with memory proves to be a good criterion, along with the well-known one of not using the low weight feedback polynomials. It is interesting to see whether other design criteria for functions with memory can be derived as well.

We proceed by pointing out some still open problems. First, assume that the shift registers have linear feedback with pairwise coprime feedback polynomials.

When the function is memoryless, we have shown in the previous section that there always exists an input and a linear function of it, correlated to a linear function of the output, with the corresponding polynomial relatively prime to the shift register feedback polynomial, which enables the correlation attack. The problem is to determine the conditions under which this also holds for a function with memory and the conditions under which an input can be decorrelated from the output. The analogous problem also holds when the shift registers are allowed to be non-autonomous. Note that it seems plausible that a linear feedback shift register may be decorrelated from the generator output when it is non-autonomous. Second, it remains an open question whether similar or more efficient procedures than the one described in Golić [14] exist for finding linear functions of the output and input that are mutually correlated. Third, one can try to generalise the result from Meier, Staffelbach [23] regarding the functions with one bit of memory and thus derive the sum of the squares of the correlation coefficients between all the linear functions of $M+1$ successive output bits and all the linear functions of $M+1$ successive input bit vectors, for any function with M bits of memory.

Finally, since the linear sequential circuit approximation attack Golić [14] is in principle applicable to arbitrary finite-state machines, it remains to investigate its application to a general keystream generator and, especially, to a generator containing clock-controlled shift registers. For example, stop-and-go shift registers seem to be vulnerable to such attacks.

4 Irregular clocking and no memory

There are numerous results in the literature showing that the use of irregularly clocked shift registers in keystream generators is a good way of obtaining sequences with long periods, high linear complexities, and nice statistical properties, see Gollmann, Chambers [17], Rueppel [36], Ding, Xiao, Shan [8], and Golić, Živković [11]. Several cryptanalytic attacks on clock-controlled shift registers have already been pointed out in Section 1. In this section, we concentrate on the correlation attacks on irregularly clocked shift registers combined by a memoryless function. The registers are assumed to be clocked at least once at a time.

When the shift registers are clock-controlled and the combining function is memoryless, it is no longer possible to apply the correlation attacks from Section 2, because the Hamming distance between binary sequences of different lengths makes no sense. However, in Golić, Mihaljević [12, 13] it is shown that in this case one can use the so-called constrained Levenshtein-like distances and then apply basically the same statistical correlation attack as in the regular clocking case. Recall that in general the constrained Levenshtein distance (CLD) is defined as the minimum sum of elementary distances associated with edit operations of deletion, insertion, and substitution needed to transform one sequence into the other, under given constraints. In our case, insertions are not allowed and the constraints result from the characteristics of the clock-controlling sequences. A typical constraint relates to the maximum number of consecutive deletions. The problem of how to compute the CLD efficiently was resolved in Golić, Mihaljević [13], by a recursive algorithm similar to dynamic-programming ones.

So, when the memoryless function is zero-order correlation immune, by a correlation attack based on the Levenshtein-like distances it is in principle possible to reconstruct the initial content of the shift register whose output is correlated to the generator output, regardless of the initial contents of other shift registers and regardless of the clock-generators appearing in the scheme. It still remains an open problem to find out the conditions under which the described procedure yields an arbitrarily small error probability given a sufficiently long segment of the output sequence. The problem appears to be very difficult and related to the one of deriving the lower bounds on the capacity of certain types of communication channels with synchronisation errors.

Consider now the case when no substitution noise is present, that is, the case of a single clock-controlled shift register. When two or more consecutive deletions are not allowed, that is, when the register is clocked once or twice at a time, a constrained embedding correlation attack was developed by Živković [44]. The embedding attack consists in trying to embed a given segment of the keystream sequence into a twice as long segment of the regularly clocked shift register sequence for each assumed initial state, not allowing two or more consecutive insertions except at the end of the shorter sequence. The constrained embedding probability for a given string is defined as the probability that it can be embedded into a twice as long purely random binary string, under the given constraints. Živković [44] derived an upper bound on this probability that exponentially tends to zero when the length of the observed keystream sequence increases. Accordingly, the initial state reconstruction is possible if the length of the observed keystream sequence is greater than a value linear in the shift register length. Note that the embedding attack is essentially the same as the constrained Levenshtein distance attack, since the embedding is possible if and only if this distance is minimal. A still open problem is to examine the general case when the maximum number of consecutive deletions is an arbitrary integer greater than one. In particular, it would be interesting to see whether by making this number large one can render the clock-controlled shift register theoretically immune to constrained embedding attacks.

Another related problem is to investigate the unconstrained embedding attack in which one employs the embedding without constraints. This attack is applicable to an arbitrary clock-controlled shift register that is clocked at least once per output symbol. A similar attack based on a variation of the unconstrained Levenshtein distance was suggested in Mihaljević [29], but without theoretical results about its effectiveness.

In Golić, Petrović [15], it is shown that instead of using the Levenshtein-like distances, one can use a probabilistic constrained edit distance (PCED) which actually represents the probability that one sequence is transformed into the other for an appropriately defined statistical model. A recursive algorithm for its efficient computing is also derived in Golić, Petrović [15]. The PCED results in the maximum posterior probability decision rule and, hence, is statistically optimal for the adopted statistical model. This also implies that the PCED is statistically better than the CDL, which has indeed been supported by experiments. It is in principle possible that the Levenshtein-like distance correlation attack may not be effective in some cases, whereas we conjecture that the probabilistic correlation attack is successful whenever the correlation noise probability is different from one half, provided that the length of the observed keystream sequence is sufficiently large.

By a suitable generalisation of the constrained Levenshtein distance from the one-to-one to many-to-one string case, it is demonstrated in Golić, Petrović [16] how the described correlation attack can be extended to the general case of an arbitrary mth-order correlation immune memoryless function. The probabilistic constrained edit distance can be generalised analogously. Further work on reducing the space and time complexities of the recursive algorithms for the efficient computation of the described edit distances might be useful.

At present, there are no fast correlation attacks on noised clock-controlled shift registers reported in the literature and in general it appears unlikely that they would be feasible in the near future. In this sense, these schemes can be considered as very secure. Consequently, irregular clocking is not only a way of achieving long periods and high linear complexities, but is also a way of obtaining the immunity against the fast correlation attacks.

Finally, it is interesting to note that besides the irregular clocking, one may also introduce the irregular interleaving of two or more individual keystream generators in order to obtain the output sequence. However, correlation attacks on these schemes may also be possible by using the Levenshtein-like or probabilistic distances that allow insertions besides deletions and substitutions, see Petrović, Golić [31].

5 Irregular clocking and memory

Consider now the most general case so far, of irregularly clocked shift registers combined by a function with memory. A question is whether these schemes are not immune to divide and conquer correlation attacks. A step in this direction is made in Petrović, Golić [32] where a special constrained edit distance (CED) of the many-to-one string type is defined to cope with the memory. This work has not been published yet. We now describe briefly the main ideas. An edit transformation from a set of input strings into an output string is defined in such a way that one first deletes the symbols from the input strings thus reducing them to the strings of the same length, then transforms these strings by a function with memory into a combination output string, and finally substitutes for the symbols in this string in order to obtain the given output string. The constrained edit distance (CED) is defined as the minimum sum of elementary distances associated with edit operations of deletion and substitution needed to transform the input strings into the output string, under given constraints related to the maximum number of consecutive deletions in each of the input strings. Efficient computation of the CED in the memoryless case can be obtained by introducing the partial constrained edit distance $W(e_1, ..., e_K, s)$ as the CED between the prefixes of the K input strings of lengths $e_i + s, 1 \leq i \leq K$, and the prefix of the output string of length s, see Golić, Petrović [16]. Namely, it is shown that $W(e_1, ..., e_K, s)$ can be computed recursively. However, when the function has memory this is no longer possible. The problem can be solved by introducing the partial constrained edit distance $W(S, e_1, ..., e_K, s)$ where the variable S represents the memory state produced during the last substitution Petrović, Golić [32].

We now explain briefly how the CED defined as above can be used in a divide and conquer correlation attack. First note that the output and the next-state functions of a combiner with memory can always be put into the form

$$y_t = f'(\underline{s}'_t, \underline{x}'_t) + \epsilon\,(\underline{s}_t, \underline{x}_t), \quad t \geq 0 \tag{2}$$

$$\underline{s}'_{t+1} = G'(\underline{s}'_t, \underline{x}'_t), \quad t \geq 0 \tag{3}$$

where $\underline{x}'_t$ is a subvector of the input vector $\underline{x}_t$ at time t, $\underline{s}'_t$ is a subvector of the state vector $\underline{s}_t$ at time t, y_t is the binary output at time t, and ϵ is a nonbalanced Boolean function. This actually means that the output sequence is correlated to the sequence produced by a reduced binary combiner with memory, whose output and next-state functions are f' and G', respectively. Accordingly, it is easy to see that the appropriately defined CED can be used for a divide and conquer correlation attack on the shift register sequences producing $\underline{x}'_t$. Note that even if the dimensions of $\underline{x}'_t$ and $\underline{x}_t$ and of $\underline{s}'_t$ and $\underline{s}_t$ are equal, respectively, we still have a divide and conquer attack on the initial contents of the shift registers regardless of the initial states of the clock-generators. In this case ϵ is zero and there is no reduction of the combiner with memory. It is important to note that the recursive computation of $W(S, e_1, ..., e_K, s)$ is exponential in the number of the reduced memory bits. One should take this into account when estimating the effective key uncertainty reduction for this divide and conquer attack. Accordingly, the memory size thus proves to be an important security parameter. Another design criterion that follows is that a function with memory should not have the reduction property.

An interesting and promising problem is to find out an appropriate constrained edit distance related to the correlated linear functions of the output and input determined by the procedure from Golić [14] which hopefully would not have the computational limitation regarding the number of memory bits. The problem of deriving the corresponding probabilistic constrained edit distances is also interesting.

A solution to the problem of designing a fast correlation attack on irregularly clocked shift registers combined by a function with memory seems to be not conceivable yet. These schemes seem to be immune to such attacks. Furthermore, the use of non-autonomous clock-controlled shift registers may be a good way of increasing their security.

6 Conclusion

In this paper, the security against correlation attacks of binary keystream generator schemes based on regularly or irregularly clocked shift registers combined by a function with or without memory is discussed. Judging from the results reported in the literature so far and from the ongoing research known to the author, these generators do not appear theoretically immune to divide and conquer correlation attacks. Further research into analysing the effectiveness of the proposed attacks as well as into defining the new ones is needed.

The published fast correlation attacks apply only to combiners with regularly clocked linear feedback shift registers. Their performance is limited in that they could hardly deal with large correlation noise. Therefore, from the practical standpoint it appears possible to resist the correlation attacks even with regularly clocked shift registers combined by a memoryless function. More complex schemes based on clock-controlled, possibly non-autonomous, shift registers combined by a function with memory seem to be considerably more secure.

References

1. R. J. Anderson, "Solving a class of stream ciphers," *Cryptologia*, 14(3):285–288, 1990.
2. R. J. Anderson, "Faster attack on certain stream ciphers," *Electr. Lett.*, 29(15): 1322–1323, July 1993.
3. W. G. Chambers and D. Gollmann, "Lock-in effect in cascades of clock-controlled shift registers," Advances in Cryptology – EUROCRYPT '88, *Lecture Notes in Computer Science*, vol. 330, C. G. Günther ed., Springer-Verlag, pp. 331–342, 1988.
4. V. Chepyzhov and B. Smeets, "On a fast correlation attack on stream ciphers," Advances in Cryptology – EUROCRYPT '91, *Lecture Notes in Computer Science*, vol. 547, D. V. Davies ed., Springer-Verlag, pp. 176–185, 1991.
5. E. Dawson and B. Goldburg, "Universal logic sequences," Advances in Cryptology – AUSCRYPT '90, *Lecture Notes in Computer Science*, vol. 453, J. Seberry and J. Pieprzyk eds., Springer-Verlag, pp. 426–432, 1990.
6. E. Dawson , "Cryptanalysis of summation generator," Advances in Cryptology – AUSCRYPT '92, *Lecture Notes in Computer Science*, vol. 718, J. Seberry and Y. Zheng eds., Spinger-Verlag, pp. 209–215, 1993.
7. E. Dawson and A. Clark, "Divide and conquer attacks on certain classes of stream ciphers," to appear in *Cryptologia*.
8. C. Ding, G. Xiao, and W. Shan, *The Stability Theory of Stream Ciphers. Lecture Notes in Computer Science*, vol. 561, Berlin: Springer–Verlag, 1991.
9. R. Forré, "A fast correlation attack on nonlinearly feedforward filtered shift-register sequences," Advances in Cryptology – EUROCRYPT '89, *Lecture Notes in Computer Science*, vol. 434, J.-J. Quisquater, J. Vandewalle eds., Springer-Verlag, pp. 586–595, 1990.
10. R. G. Gallager, "Low-density parity-check codes," *IRE Trans. Inform. Theory*, 8:21–28, Jan. 1962.
11. J. Dj. Golić and M. V. Živković, "On the linear complexity of nonuniformly decimated PN-sequences," *IEEE Trans. Inform. Theory*, 34:1077–1079, Sep. 1988.

12. J. Dj. Golić and M. J. Mihaljević, "A noisy clock-controlled shift register cryptanalytic concept based on sequence comparison approach," Advances in Cryptology – EUROCRYPT '90, *Lecture Notes in Computer Science*, vol. 473, I. B. Damgard ed., Springer-Verlag, pp. 487–491, 1990.
13. J. Dj. Golić and M. J. Mihaljević, "A generalized correlation attack on a class of stream ciphers based on the Levenshtein distance," *Journal of Cryptology*, 3(3):201–212, 1991.
14. J. Dj. Golić, "Correlation via linear sequential circuit approximation of combiners with memory," Advances in Cryptology – EUROCRYPT '92, *Lecture Notes in Computer Science*, vol. 658, R. A Rueppel ed., Springer-Verlag, pp. 113–123, 1993.
15. J. Dj. Golić and S. V. Petrović, "A generalized correlation attack with a probabilistic constrained edit distance," Advances in Cryptology – EUROCRYPT '92, *Lecture Notes in Computer Science*, vol. 658, R. A. Rueppel ed., Springer-Verlag, pp. 472–476, 1992.
16. J. Dj. Golić and S. V. Petrović, "Constrained edit distance for a memoryless function of strings," invited introductory paper, *Proceedings of the Second Spanish Conf. Cryptology*, Madrid, pp. 1–23, Oct. 1992.
17. D. Gollmann and W. G. Chambers, "Clock controlled shift registers: a review," *IEEE J. Sel. Ar. Commun.*, 7(4):525–533, 1989.
18. D. Gollmann and W. G. Chambers, "A cryptanalysis of step$_{k,m}$–cascades," Advances in Cryptology – EUROCRYPT '89, *Lecture Notes in Computer Science*, vol. 434, J.-J. Quisquater, J. Vandewalle eds., Springer-Verlag, pp. 680–687, 1990.
19. J. L. Massey, *Threshold Decoding*. Cambridge, MA: MIT Press, 1963.
20. J. L. Massey and R. A. Rueppel, "Method of, and apparatus for, transforming a digital sequence into an encoded form" U. S. Patent No. 4,797,922, 1989.
21. W. Meier and O. Staffelbach, "Fast correlation attacks on certain stream ciphers," *Journal of Cryptology*, 1(3):159–176, 1989.
22. W. Meier and O. Staffelbach, "Nonlinearity criteria for cryptographic applications," Advances in Cryptology – EUROCRYPT '89, *Lecture Notes in Computer Science*, vol. 434, J.-J. Quisquater, J. Vandewalle eds., Springer-Verlag, pp. 549–562, 1990.
23. W. Meier and O. Staffelbach, "Correlation properties of combiners with memory in stream ciphers," *Journal of Cryptology*, 5(1):67–86, 1992.
24. R. Menicocci, "Cryptanalysis of a two-stage Gollmann cascade generator," *Proceedings of SPRC '93*, Rome, pp. 62–69, 1993.
25. R. Menicocci, "Short Gollmann cascade generators may be insecure," *Abstracts of the Fourth IMA Conference on Coding and Cryptography*, Cirencester, 1993.
26. M. J. Mihaljević and J. Dj. Golić, "A fast iterative algorithm for a shift register initial state reconstruction given the noisy output sequence," Advances in Cryptology – AUSCRYPT '90, *Lecture Notes in Computer Science*, vol. 453, J. Seberry and J. Pieprzyk eds., Springer-Verlag, pp. 165–175, 1990.
27. M. J. Mihaljević and J. Dj. Golić, "A comparison of cryptanalytic principles based on iterative error-correction," Advances in Cryptology – EUROCRYPT '91, *Lecture Notes in Computer Science*, vol. 547, D. V. Davies ed., Springer-Verlag, pp. 527–531, 1991.
28. M. J. Mihaljević and J. Dj. Golić, "Convergence of a Bayesian iterative error-correction procedure on a noisy shift register sequence," Advances in Cryptology – EUROCRYPT '92, *Lecture Notes in Computer Science*, vol. 658, R. A. Rueppel ed., Springer-Verlag, pp. 124–137, 1993.

29. M. J. Mihaljević, "An approach to the initial state reconstruction of a clock-controlled shift register based on a novel distance measure," Advances in Cryptology - AUSCRYPT '92, *Lecture Notes in Computer Science*, vol. 718, J. Seberry and Y. Zheng eds., Spinger-Verlag, pp. 349–356, 1993.
30. M. J. Mihaljević and J. Dj. Golić, "A parity-check weight distribution for maximum-length sequences," *Abstracts of the Second International Conference on Finite Fields*, University of Nevada, Las Vegas, p. 35, 1993.
31. S. V. Petrović and J. Dj. Golić, "String editing under a combination of constraints," *Information Sciences*, 74:151–163, 1993.
32. S. V. Petrović and J. Dj. Golić, "A divide and conquer attack on clock-controlled shift registers combined by a function with memory," submitted, 1993.
33. F. Rubin, "Decrypting a stream cipher based on JK flip-flops," *IEEE Trans. Comput.*, 28(7):483–487, July 1979.
34. R. A. Rueppel, *Analysis and Design of Stream Ciphers.* Berlin: Springer-Verlag, 1986.
35. R. A. Rueppel, "Correlation immunity and the summation generator," Advances in Cryptology - CRYPTO '85, *Lecture Notes in Computer Science*, vol. 218, H. C. Williams ed., Springer-Verlag, pp. 260–272, 1986.
36. R. A. Rueppel, "Stream ciphers," in *Contemporary Cryptology: The Science of Information Integrity*, G. Simmons ed., pp. 65–134. New York: IEEE Press, 1991.
37. T. Siegenthaler, "Decrypting a class of stream ciphers using ciphertext only," *IEEE Trans. Comput.*, 34:81–85, Jan. 1985.
38. T. Siegenthaler, "Correlation immunity of nonlinear combining functions for cryptographic applications," *IEEE Trans. Inform. Theory*, 30:776–780, Sep. 1984.
39. G. Z. Xiao and J. L. Massey, "A spectral characterisation of correlation-immune combining functions," *IEEE Trans. Inform. Theory*, 34:569–571, May 1988.
40. K. C. Zeng and M. Huang, "On the linear syndrome method in cryptanalysis," Advances in Cryptology - CRYPTO '88, *Lecture Notes in Computer Science*, vol. 403, S. Goldwasser ed., Springer-Verlag, pp. 469–478, 1990.
41. K. C. Zeng, C. H. Yang, and T. R. N. Rao, "An improved linear syndrome algorithm in cryptanalysis with applications," Advances in Cryptology - CRYPTO '90, *Lecture Notes in Computer Science*, vol. 537, A. J. Menezes S. A. Vanstone eds., Springer-Verlag, pp. 34–47, 1991.
42. K. C. Zeng, C. H. Yang, and T. R. N. Rao, "On the linear consistency test (LCT) in cryptanalysis and its applications," Advances in Cryptology - CRYPTO '89, *Lecture Notes in Computer Science*, vol. 218, G. Brassard ed., Springer-Verlag, pp. 164–174, 1990.
43. M. V. Živković, "On two probabilistic decoding algorithms for binary linear codes," *IEEE Trans. Inform. Theory*, 37:1707–1716, Nov. 1991.
44. M. V. Živković, "An algorithm for the initial state reconstruction of the clock-controlled shift register," *IEEE Trans. Inform. Theory*, 37:1488–1490, Sep. 1991.