A Cryptanalysis of $Step_{k,m}$-Cascades

Dieter Gollmann[1] William G.Chambers[2]

[1] Fakultät für Informatik, Universität Karlsruhe
D-7500 Karlsruhe, Germany

[2] Department of Electronic and Electrical Engineering
King's College London
London WC2R 2LS, United Kingdom

We examine cascades of clock-controlled shift registers where registers are clocked by more general schemes than simply "stop-and-go". In particular, we consider the relation between the stepping function and the number of keys of such a cascade.

1 Introduction

The history of stop-and-go generators can be traced back to mechanical devices where a rotor is stepped if and only if a pin in a controlling wheel has been set. In an electronic device clock-control can be easily generalized to arbitrary stepping functions and it seems plausible that the security of a generator can be improved by choosing a stepping function other than stop-and-go. Indeed, several attacks on "clock-controlled" rotor machines rely on the fact that rotors do not step on input 0. We extend results for "stop-and-go"-registers to registers with more general stepping functions, in particular, we examine the existence of equivalent states in such cascades. Clock controlled shift registers of length 3 will demonstrate the influence of the stepping function on the cryptographic merits of the resulting cascade.

J.J. Quisquater and J. Vandewalle (Eds.): Advances in Cryptology - EUROCRYPT '89, LNCS 434, pp. 680-687, 1990.

2 Cascades of clock-controlled shift registers

We consider cascades of clock-controlled cyclic shift registers over $GF(2)$ (see Fig.1). A $\text{step}_{k,m}$-register steps k times on input 0 and m times on input 1. Stop-and-go is thus $\text{step}_{0,1}$. The output of a register and the input to its clock are added modulo 2 to give the input to the clock of the next register (or the output of the cascade respectively). No register shall be loaded with $0\ldots0$ or $1\ldots1$. Properties of $\text{step}_{0,1}$-cascades have been reported e.g. in [2,3] and are stated in the following theorem. $\text{prob}_n(w)$ will denote the probability to observe a binary word w in the output sequence generated by a cascade of n registers when the input to the cascade is constantly 1.

Theorem 1 *$\text{Step}_{0,1}$-cascades of n clock-controlled shift registers of length p, $p \geq 3$ prime, generate sequences with*

- *period p^n*
- *linear complexity greater or equal $d\frac{p^n-1}{p-1}$ where d is the degree of the irreducible polynomials with period p and $p^2 \nmid 2^{p-1}-1$*
- $\lim_{n\to\infty} \text{prob}_n(w) = \frac{1}{2^{|w|}}$
- *different output sequences for all $(2^p-2)^n$ legal initial states.*

$\text{Step}_{0,1}$-cascades are invertible and the inverse cascade can be synchronized [2]. If the initial states of all registers are known but for their rotations these can be deduced with high probability by feeding the output sequence to the inverse cascade. The security of the cascade should thus not be related to $(2^p-2)^n$, the number of legal initial states, but to $((2^p-2)/p)^n$, the number of equivalence classes modulo rotation of registers.

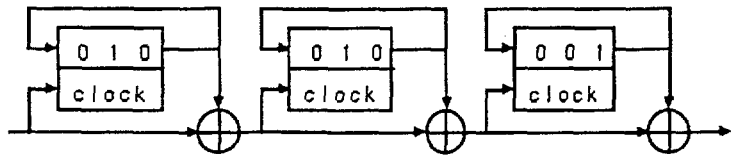

Figure 1: A cascade of clock-controlled shift registers of length 3

3 Properties of $\text{step}_{k,m}$-cascades

Most of the properties of $\text{step}_{0,1}$-cascades also hold for $\text{step}_{k,m}$-cascades. We first state a simple but fundamental lemma on the period of the output sequences.

Lemma 1 *A cascade of n $\text{step}_{k,m}$-registers of length p, $p \geq 3$ prime, $k \neq m$, generates sequences with period p^n.*

Proof. One may show by induction that sequences generated by a cascade of length n have period p^n and contain a number of 1's which is coprime to p. More details can be taken from the proof for $\text{step}_{0,1}$-cascades given in [3]. □

Given the period of the sequences we can state a lower bound for their linear complexity.

Lemma 2 *A cascade of n $\text{step}_{k,m}$-registers of length p, $p \geq 3$ prime, $p^2 \nmid 2^{p-1} - 1$, $k \neq m$, generates sequences with linear complexity greater or equal $d(p^n - 1)/(p - 1)$ where d is defined as in Theorem 1.*

Proof. The last register in the cascade contributes at least one polynomial $f(x^{p^{n-1}})$ to the generating polynomial of some given output sequence where $f(x)$ is an irreducible polynomial of period p. With [1], Theorem 6.23, we find that $f(x^{p^{n-1}})$ decomposes into irreducible factors of period p^n. [1], Theorem 6.52 and $p^2 \nmid 2^{p-1} - 1$ imply that $f(x^{p^{n-1}})$ is irreducible and has degree $d \cdot p^{n-1}$. Again, arguments from [4] can be used to construct a detailed proof. □

The results from [2] also can be extended to $\text{step}_{k,m}$-cascades. The impact on the security has already been stated above for $\text{step}_{0,1}$-cascades.

Lemma 3 *A $\text{step}_{k,m}$-register of length p, $p \geq 3$ prime, $k \neq m$, is invertible. The inverse automaton can be synchronized.*

Lemma 4 *Cascades of $\text{step}_{k,m}$-registers of length p, $p \geq 3$ prime, $k \neq m$, generate sequences with*

$$\lim_{n \to \infty} \text{prob}_n(w) = \frac{1}{2^{|w|}}.$$

Proof. We adapt the corresponding proof from [3]. We have to prove that for any initial state $\underline{q}$ of a cascade of length n, any input $\underline{x}$ and output $\underline{y}$ of length n there exists a state $\underline{q}'$ so that

- there exists an input sequence that sends the cascade from $\underline{q}$ to $\underline{q}'$
- input $\underline{x}$ applied to the cascade in state $\underline{q}'$ generates output $\underline{y}$.

Assume that this proposition holds up to some given n. Prefix $\underline{x}$ and $\underline{y}$ with new bits x_0 and y_0 respectively and consider a cascade of length $n+1$ with initial state $(\underline{q}, q_{n+1})$. Without loss of generality we choose q_{n+1}, the state of the last register, so that if the last register is turned back k steps its output is y_0 and if it is turned back m steps its output is $\bar{y}_0$.

As $\text{step}_{k,m}$-registers are invertible, there exists a word $\underline{z}$ of length n so that $\underline{x}$ generates the internal signal $\underline{z}$ after n stages of the cascade and output $\underline{y}$. Furthermore, there exists a state $\underline{q}_0$ so that x_0 sends the first n registers of the cascade from $\underline{q}_0$ to $\underline{q}$, generating some output bit c. If $c = 0$ we start the last register with q_{n+1} turned back k steps, i.e. with y_0 in the output position, thus the overall output is also y_0. If $c = 1$ we start the last register with q_{n+1} turned back m steps, i.e. with $\bar{y}_0$ in the output position, thus the overall output is $1 \oplus \bar{y}_0 = y_0$.

As a next step, for any $s \geq 1$ and any cascade of length n, consider $2^s \times 2^s$-matrices where the entry in position x, y , $1 \leq x, y \leq 2^s$ gives the number of states where input $\underline{x}$ produces output $\underline{y}$, $\underline{x}$ and $\underline{y}$ are the binary representations of x, y. Divide all entries by $1/p^n$. The matrix corresponding to a cascade is the product of the matrices of the individual stages, these matrices are contraction operators with the equidistribution of s-tupels as fixed point (see [3]). Thus the output distribution of s-tupels will converge to equidistribution as the length of the cascade goes to infinity. □

The rate of convergence that follows from the above proof is in general much slower than the rate observed in practice. However, in the particular case of $\text{step}_{1,2}$-cascades of registers of length 3 the output sequences can be proven to have almost ideal statistical properties. The distribution of s-tupels in the output is nearly flat for all $s \geq 1$. Words of the same length appear with probabilities differing at most by $1/3^n$. We have

Remark 1 *$\text{Step}_{1,2}$-cascades of n clock-controlled shift registers of length 3 generate sequences with*

$$\frac{1}{3^n}\left\lceil \frac{3^n}{2^{|w|}} \right\rceil \leq \text{prob}_n(w) \leq \frac{1}{3^n}\left\lfloor \frac{3^n}{2^{|w|}} \right\rfloor \text{ , for all } w \in \{0,1\}^*.$$

Proof. Consider a register with initial state 001. We will see later (Lemma 6) that this is no undue restriction. Let x_1x_2 denote an input string and y_1y_2 the corresponding output. Map the states $\{100, 001, 010\}$ to $\{0, 1, 2\}$

as follows, $100 \to 0, 001 \to 1, 010 \to 2$. Let $q(0)$ be the initial state of the register and $q(i)$ the state after processing $x_1 \ldots x_i$, $i \geq 1$. Tabulate $x_1\bar{x}_2$ and $q(2)$ in dependence of $y_1\bar{y}_2$ and $q(0)$.

$q(2)$

$y_1\bar{y}_2$	$q(0)=0$	1	2
00	1	1	1
01	0	0	2
10	1	0	0
11	2	2	2

$x_1\bar{x}_2$

$y_1\bar{y}_2$	$q(0)=0$	1	2
00	00	10	01
01	01	11	00
10	11	00	10
11	10	01	11

On inspection we see that the above tables define the computation

$$\begin{aligned} \tilde{x} &= 3 \cdot \tilde{y} + q(0) \pmod 4 \\ \tilde{y} &= \lfloor (3 \cdot \tilde{y} + q(0))/4 \rfloor \end{aligned}$$

where $\tilde{x} = 2\bar{x}_2 + x_1$, $\tilde{y} = 2\bar{y}_2 + y_1$. The final state $q(2)$ serves as a carry that is handed on to the next inputs and outputs of length 2, say x_3x_4 and y_3y_4. Repeating the above argument we get for $x_1 \ldots x_m$, $y_1 \ldots y_m$, m even

$$\begin{aligned} \tilde{x} &\equiv 3 \cdot \tilde{y} + q(0) \pmod{2^m} \\ \tilde{y} &\equiv \lfloor (3 \cdot \tilde{y} + q(0))/2^m \rfloor \end{aligned}$$

with

$$\begin{aligned} \tilde{x} &= \bar{x}_m 2^m + x_{m-1}2^{m-1} + \cdots + \bar{x}_2 2 + x_1 \ , \\ \tilde{y} &= \bar{y}_m 2^m + y_{m-1}2^{m-1} + \cdots + \bar{y}_2 2 + y_1 \ . \end{aligned}$$

For odd m we find the same relation between inputs, outputs, and the states of the register. However, in this case we have to invert the odd bits in input and output. Now consider a cascade of length n. We get

$$\tilde{x} \equiv 3^n \cdot \tilde{y} + \underline{\tilde{q}} \pmod{2^m}$$

with

$$\underline{\tilde{q}} = \sum_{j=1}^{n} 3^{j-1} q_j(0)$$

where $q_j(0)$ is the initial state of the j^{th} register. As the cascade has period 3^n, $\underline{\tilde{q}}$ will take on all values in $[0, 3^n - 1]$ exactly once. Hence

$$\left\lceil \frac{3^n}{2^{|\omega|}} \right\rceil \leq \underline{\tilde{q}} \pmod{2^m} \leq \left\lfloor \frac{3^n}{2^{|\omega|}} \right\rfloor$$

and the same holds for the outputs $\tilde{y}$ if the input $\tilde{x}$ is fixed. □

4 Equivalent states in $\text{step}_{k,m}$-cascades

Two states of a finite automaton are called equivalent when, for any input, both will produce the same output. A finite automaton is called minimal if equivalence implies equality. (For more details see e.g.[5]).

We consider $\text{step}_{k,m}$-cascades with constant input 1. In the context of cryptographic applications, equivalent states are seeds that produce the same pseudo random sequence. The set of keys is thus not the set of seeds but the set of equivalence classes. Different seeds generate different sequences if and only if the cascade is minimal. In a first step we examine the structure of internal signals in equivalent states of a $\text{step}_{k,m}$-cascade.

Lemma 5 *If two two states $\underline{q}$, $\underline{q}'$ of a $\text{step}_{k,m}$-cascade are equivalent then corresponding internal signals are either identical or bitwise complemented.*

Proof. More generally, consider two states $\underline{q}$, $\underline{q}'$ of a cascade of length n producing outputs that are either identical or bitwise complemented and assume that the proposition does not hold for the input to the last stage. Without loss of generality assume that there exists a time frame $(i, i+1)$, where inputs 01 and 11 respectively are fed to the last stage. We know from Lemma 1 that the cascade has period p^n. If we observe the cascade at instances $(i + \lambda p^{n-1}, i + 1 + \lambda p^{n-1})$, $0 \leq \lambda < p$, then the inputs to the last stage will be repeated but the last register will be in a different rotation every time. If $\underline{q}$ and $\underline{q}'$ produce the same output then the observations at times $i + \lambda p^{n-1}$ imply that the number of 1's in the last stage of $\underline{q}$ is the complement (mod p) of the number of 1's in the last stage of $\underline{q}'$. From the observations at times $i + 1 + \lambda p^{n-1}$ we find that both numbers should be the same. This is impossible as p is odd. We get the same contradiction when the outputs are complemented. By induction, the lemma can be shown to hold for all internal signals. □

Lemma 6 *A $\text{step}_{k,m}$-cascade is minimal if and only if $k \neq p - m$.*

Proof. Consider two equivalent states $\underline{q}$, $\underline{q}'$ of a cascade of length $n > 1$. If all internal signals were the same then obviously the states would be the same. So we may assume that the inputs to the last stage are bitwise complemented.

Let $(q_n(1), \ldots, q_n(p))$ and $(q'_n(1), \ldots, q'_n(p))$ be the respective states of the last stages. We know that there must be times i, $i + j$, $p \nmid j$, so that the cascade starting in $\underline{q}$ is in the same position, otherwise the last register would rotate with period p. Denote the number of 1's in the interval $[i, i + j - 1]$ by t. Without loss of generality assume that the output of the last stage is

$q_n(p)$ and that the outputs of the last stage for the initial state $\underline{q}'$ are $q'_n(r)$ and $q'_n(r')$. Let σ_n denote the number of 1's in the input to the last stage. Observing the cascade at instances $(i + \lambda p^{n-1}, i + j + \lambda p^{n-1})$, $0 \leq \lambda < p$, we get

$$q'_n(r - \lambda\sigma_n(k-m)) = \bar{q}_n(p - \lambda\sigma_n(m-k)) = q'_n(r' - \lambda\sigma_n(k-m)) \ ,$$

thus the shifts of $(q'_n(1), \ldots, q'_n(p))$ corresponding to r and r' are equal. Because p is prime we have $r = r'$. This implies

$$\begin{aligned} t \cdot m + (j-t) \cdot k &\equiv 0 \pmod{p} \\ t \cdot k + (j-t) \cdot m &\equiv 0 \pmod{p} \end{aligned}$$

hence

$$(m+k) \cdot j \equiv 0 \pmod{p}$$

and finally

$$m + k \equiv 0 \pmod{p} \ .$$

□

5 Conclusion

We collect our results in

Theorem 2 *A $step_{k,m}$-register of length p, $p \geq 3$ prime, $k \neq m$, is invertible. The inverse automaton can be synchronized. A cascade of n $step_{k,m}$-registers of length p, $p \geq 3$ prime, $k \neq m$, generates sequences with*

- *period p^n*
- *linear complexity $\geq d\frac{p^n-1}{p-1}$ where d is defined as in Theorem 1 and $p^2 \nmid 2^{p-1} - 1$*
- $\lim_{n\to\infty} \mathrm{prob}_n(w) = \frac{1}{2^{|w|}}$
- *different output sequences for all $(2^p - 2)^n$ legal initial states if and only if $k \neq -m$.*

The minimality of $\mathrm{step}_{k,m}$-cascades depends only on the choice of the stepping function. For $step_{k,-k}$ the number of useful initial states is reduced to $((2^p - 2)/2p)^n$ as we may replace registers which contain more than $p/2$ 1's by registers with less than $p/2$ 1's. This will invert the internal signal after the stage where this replacement had taken place but there also exits a modification for the state of the next stage so that we can recover the original signal after that next stage.

It is interesting to note that sequences from $step_{1,2}$-cascades of registers of length 3 are at the same time totally insecure and almost perfect with respect to standard criteria like linear complexity or statistical distribution.

References

[1] E.Berlekamp, *Algebraic Coding Theory*, McGraw-Hill, New York, 1968

[2] W.G.Chambers, D.Gollmann, *Lock-in Effect in Cascades of Clock-Controlled Shift-Registers*, Proc.Eurocrypt88, Springer LNCS 330, pp.331-342, 1988

[3] D.Gollmann, *Pseudo Random Properties of Cascade Connections of Clock Controlled Shift Registers*, Proc.Eurocrypt84, Springer LNCS 209, pp.93-98, 1985

[4] D.Gollmann, *Linear Recursions of Cascaded Sequences*, Contributions to General Algebra 3, Hölder-Pichler-Tempsky, Wien, Teubner, Stuttgart, 1985

[5] Z.Kohavi, *Switching and Finite Automata Theory*, McGraw-Hill, New York, 1970