Its main components are $6(m + 1)$ registers for storing the three pairs (u_i, v_i), $2(m + 1)$ registers used in multiplication, and adders. This implementation is independent of the irreducible polynomial defining the field; if the irreducible polynomial is fixed in advance (as would usually be the case) there is a reduction in area. The control unit (CU) provides the control signal for the registers, adders and multipliers, and incorporates the degree comparator required by eqn. 1.

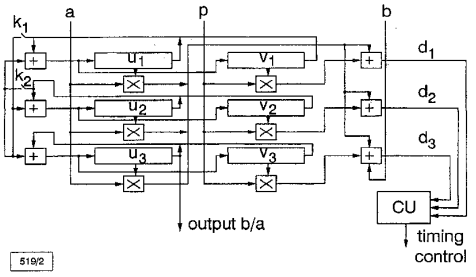

Fig. 2 *Divider structure*

Example: We illustrate the algorithm using an example in $GF(2^4)$, with $p = x^4+x+1$, $a = x^3+x+1$, $b=x^3+x^2+1$. Writing the pairs (u_1, v_1), (u_2, v_2), (u_3, v_3) in order at each step, the computations are presented in Table 1. At this stage, since the last discrepancy d_3 is 0, we have $(x^3+x^2)\ a+(x^2+x+1)\ p=x^3+x^2+1$ so $b/a = x^3+x^2$.

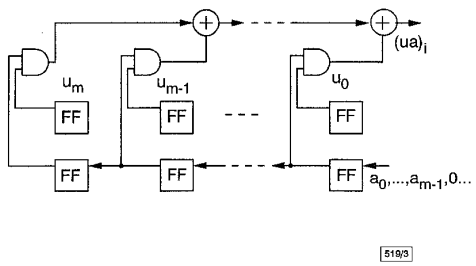

Fig. 3 *Multiplier circuit*

Serial multipliers: A serial-in, serial-out structure for implementing the multiplication is presented in Fig. 3. The multiplier performs the calculation of the ith coefficient in the product ua or vp (denoted by $()_i$). At each step only one of the discrepancies d_k, $d_{\bar{k}}$ needs to be calculated as the operation of multiplication by x preserves the discrepancies from one step to the next. Since we have to perform $au_{j=1..3}$ and $pv_{j=1..3}$ products, the structure presented in Fig. 2 uses just two shift registers corresponding to the a and p inputs. A further reduction in area can be obtained by multiplexing the calculation of the discrepancies.

Table 1: Division computation

m	(u_j, v_j)	d_i	m	(u_j, v_j)	d_i
0	(1, 0)	1	4	$(x^3 + 1, 1)$	0
	(0, 1)	1		(x, x)	1
	(0, 0)	1		$(x + 1, 0)$	1
1	$(x, 0)$	1	5	$(x^3 + 1, 1)$	0
	(1, 1)	0		(x^2, x^2)	1
	(1, 0)	1		$(1, x)$	1
2	$(x^2, 0)$	1	6	$(x^3 + 1, 1)$	1
	(1, 1)	0		(x^3, x^3)	1
	$(x + 1, 0)$	0		$(x^2 + 1, x^2 + x)$	1
3	$(x^3, 0)$	1	7	$(x^4 + x, x)$	1
	(1, 1)	1		$(1, x^3 + 1)$	1
	$(x + 1, 0)$	0		$(x^3 + x^2, x^2 + x + 1)$	0

Conclusion: A new method for division in $GF(2^m)$ is presented. The algorithm has the advantage that both operands are represented in canonical basis. Also, design and expansion to high order finite fields are easy to realise. The area complexity is $O(m)$. The algorithm performs division in a fixed number $(2m)$ of clock cycles, whereas the dividers presented in [5, 6] require a variable number of clock cycles. The division presented in [5] yields an area complexity of $O(m)$ and requires up to 2^m clock cycles, while the structure proposed in [6] yields a computational time that varies from $4m + 3$ to $5m + 2$ time steps and has an area complexity of $O(m)$. The systolic implementation presented in [7] has an area complexity of $O(m^2)$. Owing its regularity and simple control, the architecture presented in this Letter is hardware efficient and is suitable for VLSI implementation.

10 July 1998
Electronics Letters Online No: 19981297

E.M. Popovici and P. Fitzpatrick (*National Microelectronics Research Centre, University College Cork, Ireland*)

E-mail: popovici@nmrc.ucc.ie

References

1 BLAHUT, R.E.: 'Theory and practice of error control coding' (Addison-Wesley, Reading, MA, 1983)
2 WICKER, S., and BHARGAVA, V.: 'Reed-Solomon codes and their applications' (IEEE Press, Piscataway, NJ, 1994)
3 STINSON, D.: 'On bit-serial multiplication and dual bases in GF(2^m)', *IEEE Trans.*, 1991, **IT-37**, pp. 1733–1736
4 HSU, I., TRUONG, T., DEUTSCH, L., and REED, I.: 'A comparison of VLSI architecture of finite field multipliers using dual, normal or standard bases', *IEEE Trans.*, 1988, **C-37**, pp. 735–739
5 FENN, S.J., TAYLOR, D., and BENAISSA,: 'Division over $GF(2^m)$', *Electron. Lett.*, 1992, **28**, pp. 2259–2261
6 ARAKI, K., FUJITA, I., and MORISUE, M.: 'Fast inverter over finite field based on Euclid's algorithm', *Trans. IEICE*, 1989, **E-72**, pp. 1230–1234
7 HASSAN, M., and BHARGAVA, V.: 'Bit serial systolic divider and multiplier for finite fields GF(2^m)', *IEEE Trans.*, 1992, **C-41**, pp. 972–980

Observer design for cryptography based on hyperchaotic oscillators

G. Grassi and S. Mascolo

The authors describe a combination of cryptography and hyperchaos synchronisation in order to obtain a secure communications scheme. The transmitter and the receiver, which are based on a 4D hyperchaotic oscillator, are synchronised by exploiting the concept of the observer from control theory. The scalar transmitted signal is designed so that the hyperchaotic carrier masks the encrypted signal, which in turn hides the message signal. The approach leads to communication systems with higher security.

Introduction: Chaotic synchronisation and its application to secure communications have been discussed frequently in recent years [1 – 5]. Different techniques have been proposed in order to hide the contents of a message by exploiting chaotic systems. To increase the level of security, the adoption of hyperchaotic systems, characterised by two or more positive Lyapunov exponents, is more advantageous than the use of chaotic systems with only one positive Lyapunov exponent. This consideration has led to the development of interesting techniques for hyperchaos synchronisation [6 – 8].

In this Letter, a secure communications scheme is proposed, which combines cryptography and the synchronisation of hyperchaotic systems. The transmitter and receiver, which are based on a 4D hyperchaotic oscillator [9], are synchronised via a scalar signal by exploiting the concept of the observer from modern control theory [10]. The effectiveness of the communication scheme is enhanced, since the hyperchaotic carrier masks the encrypted signal, which in turn hides the message signal.

Cryptography based on hyperchaotic oscillators: A block diagram illustrating the proposed approach is reported in Fig. 1. The transmitter consists of a 4D hyperchaotic oscillator [9] and an encryp-

tion function [5], which is used to encrypt the message signal $p(t)$ by means of the hyperchaotic key $K(t)$. The hyperchaotic behaviour of the oscillator, which contains an opamp, two LC circuits and a diode, has been confirmed by both laboratory experiment and numerical simulation (see [9] for the circuit parameter values). The encrypted signal $e_{en}(t)$ is fed back to the hyperchaotic oscillator as follows [3, 5]:

$$\begin{aligned}\dot{x}_1 &= 0.7x_1 - x_2 - x_3\\ \dot{x}_2 &= x_1\\ \dot{x}_3 &= 3(x_1 - x_4)\\ \dot{x}_4 &= 3x_3 - 30(x_4 - 1)H(x_4 - 1) - 30e_{en}(t)\end{aligned} \tag{1}$$

where $H(z)$ is the Heaviside function, that is $H(z < 0) = 0$ and $H(z \geq 0) = 1$. To encrypt the message signal $p(t) = 0.5 \sin t$, an n-shift cipher [5] is chosen

$$e_{en}(t) = f_1(\cdots f_1(f_1(p(t), K(t)), K(t)), \cdots, K(t)) \tag{2}$$

where the following nonlinear function:

$$f_1(x, K) = \begin{cases} (x + K) + 2h & -2h \leq (x + K) \leq -h \\ (x + K) & -h < (x + K) < h \\ (x + K) - 2h & h \leq (x + K) \leq 2h \end{cases} \tag{3}$$

is recursively used for the encryption, with $h = 4$, $n = 30$ and $K(t) = x_2(t)$. Notice that the decryption rule is the same as the encryption rule [5], i.e.

$$p(t) = f_1(\cdots f_1(f_1(e_{en}(t), -K(t)), -K(t)), \cdots, -K(t)) \tag{4}$$

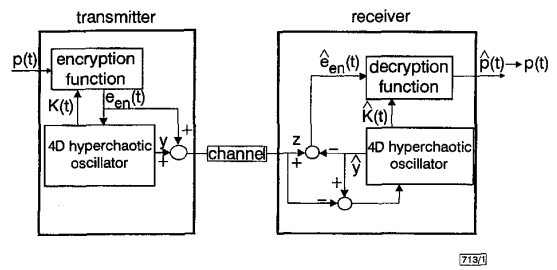

Fig. 1 *Block diagram illustrating proposed secure communications scheme*

The scalar output of the oscillator is chosen as

$$y(t) = (x_4 - 1)H(x_4 - 1) + \sum_{i=1}^{4} k_i x_i \tag{5}$$

that is, it can be obtained by adding the current in the diode to a linear combination of the circuit state variables. The weights k_i will be determined later on. The state equations (eqn. 1) and the output equation (eqn. 5) constitute the dynamical equation of the transmitter. The receiver is designed as an observer [7] for the state of the transmitter. In particular, the state equations of the receiver in the observer form are

$$\begin{aligned}\dot{\hat{x}}_1 &= 0.7\hat{x}_1 - \hat{x}_2 - \hat{x}_3\\ \dot{\hat{x}}_2 &= \hat{x}_1\\ \dot{\hat{x}}_3 &= 3(\hat{x}_1 - \hat{x}_4)\\ \dot{\hat{x}}_4 &= 3\hat{x}_3 - 30(\hat{x}_4 - 1)H(\hat{x}_4 - 1) - 30(z(t) - \hat{y}(t))\end{aligned} \tag{6}$$

where

$$\hat{y}(t) = (\hat{x}_4 - 1)H(\hat{x}_4 - 1) + \sum_{i=1}^{4} k_i \hat{x}_i \tag{7}$$

is the prediction of $y(t)$ derived from the observer, whereas

$$z(t) = y(t) + e_{en}(t) \tag{8}$$

is the observed quantity, that is, the scalar signal transmitted through the channel. Note that the receiver is a copy of the transmitter modified with a term depending on the difference between the received signal $z(t)$ and the prediction $\hat{y}(t)$ derived from the observer. This additional term aims at attenuating the difference between the state of the transmitter and the state of the observer system. Moreover, notice that $z(t)$ has been designed so that the hyperchaotic carrier $y(t)$ masks the encrypted signal $e_{en}(t)$, which in turn hides the message signal $p(t)$. The synchronisation error system between the receiver and the transmitter is linear time-invariant, i.e.

$$\begin{aligned}\dot{e}_1 &= 0.7e_1 - e_2 - e_3\\ \dot{e}_2 &= e_1\\ \dot{e}_3 &= 3(e_1 - e_4)\\ \dot{e}_4 &= 3e_3 - 30u\end{aligned} \tag{9}$$

where the variable $u = -\Sigma_{i=1}^{4} k_i e_i$ plays the role of a state feedback. Since the controllability matrix of the system of eqn. 9 is full rank, from linear control theory [10] it follows that the system eigenvalues can be placed anywhere by proper choice of the feedback gains k_i. By placing the eigenvalues in the left plane, the error dynamics is stabilised at the origin. This means that $\hat{x}(t) \to x(t)$ as $t \to \infty$, that is, the receiver becomes an observer for the state of the transmitter [7]. For instance, by choosing the eigenvalues $\{-0.5 \mp 3.486j, 0.5 \mp 0.8222j\}$, the result is $k_1 = -3.6937$, $k_2 = 0.2445$, $k_3 = 1.0727$ and $k_4 = -2.7000$. The encrypted signal recovered by the receiver is

$$\hat{e}_{en}(t) = z(t) - \hat{y}(t) \tag{10}$$

whereas the following message signal is retrieved using the key $\hat{K}(t) = \hat{x}_2(t)$ generated by the 4D oscillator in the receiving system:

$$\hat{p}(t) = f_1(\cdots f_1(f_1(\hat{e}_{en}(t), -\hat{K}(t)), -\hat{K}(t)), \cdots, -\hat{K}(t)) \tag{11}$$

Since transmitter and receiver are synchronised, $\hat{x}(t) \to x(t)$, $\hat{K}(t) \to K(t)$ and $\hat{e}_{en}(t) \to e_{en}(t)$ (see eqns. 8 and 10). Consequently, from eqns. 4 and 11 it follows that $\hat{p}(t) \to p(t)$. The validity of the proposed secure communications scheme is confirmed by simulation results. In particular, the hyperchaotic transmitted signal (eqn. 8) is reported in Fig. 2, whereas the recovered message signal (eqn. 11) is shown in Fig. 3. This Figure clearly highlights that $\hat{p}(t) \to p(t)$.

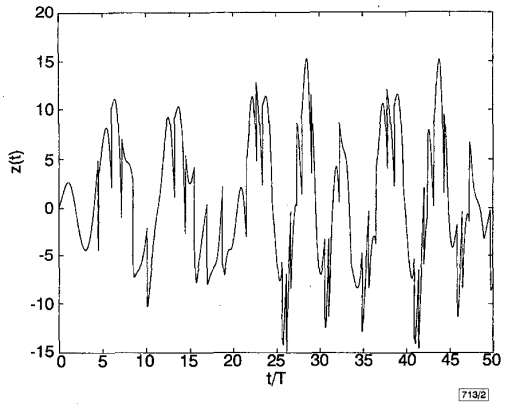

Fig. 2 *Time waveform of transmitted signal $z(t)$, with $T = \sqrt{(L_1 C_1)}$*
See [9] for circuit parameter values

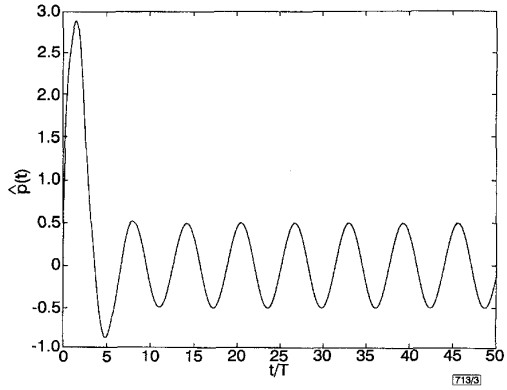

Fig. 3 *Time waveform of recovered signal $\hat{p}(t)$*
After transient, $\hat{p}(t) = 0.5 \sin t$

Advantages of both cryptography and hyperchaos synchronisation: The approach, by exploiting hyperchaos as well as transmitted signals of high complexity, makes a contribution to the development of communications systems with higher security. In fact, suppose that an intruder is able to predict the dynamics of the hyperchaotic carrier $y(t)$ by means of a reconstruction of the geometric structure in the phase space [11, 12]. Note that this is very hard to do for hyperchaotic systems [11, 12]. Anyway, suppose that the encrypted signal $e_{en}(t) = z(t) - y(t)$ is reconstructed by the intruder. Taking into account that the key $x_2(t)$ is not transmitted through the channel, it is clear that it is not possible to recover the message $p(t)$ from $e_{en}(t)$. Moreover, by considering the results available in the literature, it can be concluded that it is not possible to *reconstruct* the key $x_2(t)$ starting from the reconstruction of $y(t)$, since $x_2(t)$ and $y(t)$ are completely different signals [11, 12]. Therefore, taking into account that the key is not transmitted or reconstructed, it is not possible for an intruder to obtain the message, even if he is able to reconstruct in some way the encrypted signal. The synchronisation approach proposed herein is simple and rigorous. By taking into account that the system of eqn. 9 has been globally asymptotically stabilised at the origin, the method does not require either the computation of the Lyapunov exponents or initial conditions belonging to the same basin of attraction [8]. Finally, since the system eqn. 9 is controllable, all its modes can be arbitrarily assigned. Consequently, synchronisation can be achieved according to any specified design features [7].

Conclusions: In this Letter, a secure communications system based on a 4D hyperchaotic oscillator has been described. The approach combines cryptography and hyperchaotic synchronisation. It generates transmitted signals of high complexity, which enable the effectiveness of the secure communications scheme to be enhanced.

20 July 1998
Electronics Letters Online No: 19981285

G. Grassi (*Dipartimento di Matematica, Università di Lecce, 73100 Lecce, Italy*)

E-mail: grassi@ingle01.unile.it

S. Mascolo (*Dipartimento di Elettrotecnica ed Elettronica, Politecnico di Bari, 70125 Bari, Italy*)

E-mail: mascolo@poliba.it

References

1 CARROLL, T.L., and PECORA, L.M.: 'Synchronizing chaotic circuits', *IEEE Trans.*, 1991, **CAS-38**, (4), pp. 453–456

2 CUOMO, K.M., OPPENHEIM, A.V., and STROGATZ, S.H.: 'Synchronisation of Lorenz-based chaotic circuits with applications to communications', *IEEE Trans.*, 1993, **CAS-40**, (10), pp. 626–633

3 MILANOVIC, V., and ZAGHLOUL, M.E.: 'Improved masking algorithm for chaotic communications systems', *Electron. Lett.*, 1996, **32**, (1), pp. 11–12

4 TAMASEVICIUS, A.: 'Reproducible analogue circuit for chaotic synchronisation', *Electron. Lett.*, 1997, **33**, (13), pp. 1105–1106

5 YANG, T., WU, C.W., and CHUA, L.O.: 'Cryptography based on chaotic systems', *IEEE Trans.*, 1997, **CAS-44**, (5), pp. 469–472

6 TAMASEVICIUS, A., MYKOLAITIS, G., CENYS, A., and NAMAJUNAS, A.: 'Synchronisation of 4D hyperchaotic oscillators', *Electron. Lett.*, 1996, **32**, (17), pp. 1536–1538

7 GRASSI, G., and MASCOLO, S.: 'Nonlinear observer design to synchronize hyperchaotic systems via a scalar signal', *IEEE Trans.*, 1997, **CAS-44**, (10), pp. 1011–1014

8 GRASSI, G., and MASCOLO, S.: 'Synchronisation of hyperchaotic oscillators using a scalar signal', *Electron. Lett.*, 1998, **34**, (5), pp. 424–425

9 TAMASEVICIUS, A., NAMAJUNAS, A., and CENYS, A.: 'Simple 4D chaotic oscillator', *Electron. Lett.*, 1996, **32**, (11), pp. 957–958

10 BROGAN, W.L.: 'Modern control theory' (Prentice-Hall, New Jersey, 1991)

11 SHORT, K.M.: 'Steps toward unmasking secure communications', *Int. J. Bifurcation Chaos*, 1994, **4**, (4), pp. 959–977

12 SHORT, K.M.: 'Unmasking a modulated chaotic communications scheme', *Int. J. Bifurcation Chaos*, 1996, **6**, (2), pp. 367–375

55.0Gbit/cm data bandwidth density interface in 0.5μm CMOS for advanced parallel optical interconnects

B. Madhavan and A.F.J. Levi

The authors demonstrate that low cost 0.5μm CMOS technology may be used to form a bridge between a slow parallel electrical interface and a very high-speed parallel optical interface. The 1cm wide integrated circuit produced has a bisection data bandwidth of 55Gbit/s and dissipates 5.7W.

Introduction: Edge-connector bandwidth density (Gbit/s/cm) is a known barrier to efficient system integration [1]. A promising solution exploits the inherently high bandwidth density of ribbon-fibre based parallel optical interconnects. The industry standard MT fibre connector uses ~6mm wide ferrule which holds 12 multimode glass fibres on a 250μm pitch. Hence, an optoelectronic transceiver port with 12 transmit and 12 receive fibres is best accommodated using a sub-12mm wide (< 2 × 6mm) electronic interface. The challenge for CMOS technology is to deliver the needed bandwidth density to the optoelectronic interface while at the same time effectively bridging to the lower bandwidth density of conventional CMOS electronics. The purpose of this Letter is to demonstrate that low-cost 0.5μm CMOS technology is capable of providing a multiplexed 55Gbit/s/cm interface. This edge-connector bandwidth density is a factor of 10 greater than the competing state-of-the-art HIPPI-6400 parallel electrical interconnect [2].

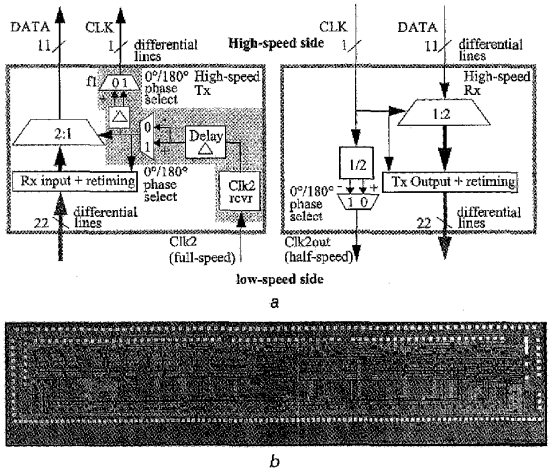

Fig. 1 *Functional block diagram of 2:1/1:2 mux/demux IC and photograph of mux IC*

a Functional block diagram of 2:1/1:2 mux/demux IC; low-speed side with 22-data and 1-clock LVDS signal lines and high-speed side with 11-data and 1-clock differential signal lines are indicated
b Photograph of mux IC measuring 10.3mm × 2.3mm

Results: A functional block diagram of the circuit is shown in Fig. 1*a*. Each of the 12 transmit (Tx) and 12 receive (Rx) high-speed signal lines of the 2:1/1:2 multiplexer (mux) integrated circuit (IC) sustains a data rate of 2.5Gbit/s without errors. The IC dissipates 5.7W from a 3.6V power supply, of which 0.225W is for the high-speed side parallel load termination and 1.025W for the source and load terminated low voltage differential signalling (LVDS) [3] compatible low-speed side. The Tx part of the IC receives a full-speed clock (Clk2) running at twice the low-speed input data rate. This clock can be delayed to ensure that all input data lines latch successfully. An additional delay circuit is provided for the high-speed clock output path so that the receive side clock-data setup times (hold time is zero on the high-speed input flip-flops) can be satisfied across all the channels. The measured delay range is in excess of 400ps (1ns) at 2.5Gbit/s (1.25Gbit/s) at the high-speed output without exercising the 0°/180° phase selection circuit, which effectively doubles the range. The measured jitter of the high-speed clock output referenced to the input has a minimum value of 3.77ps RMS (26.2PS peak-to-peak) increasing to 4.25ps RMS (27.2ps peak-to-peak) and 6.62ps RMS (46.4ps peak-to-