mial time, such that improved protocol is a strong (n, $\mathbf{D}_{2,tn}$, r, ε, δ)-protocol, where

$$r = \Omega(n)$$

$$\varepsilon = r \cdot \left(2^{-n/(2(\log n)^3)+1} + 2^{-r} + 2^{-((t-2m)n/8-2)}\right) = 2^{-\Omega(n)}$$

and

$$\delta \leq 2^{-(m/2)\cdot(t-1/2)n} + 2^{-(m/2)\cdot(t-m-1/2)n/2} + 2^{-(t-m-1/2)n/4+1} = 2^{-\Omega(n)}$$

Proof of theorem 2: Let $0 < m < t - 1/2$ be constant, and $u \in U$ be the particular value known to Eve.

We first assume that Eve is only passive. Since g is independently and randomly chosen, we obtain

$$H_2(S|G = g, A = a, U = u) \geq (t - m)n - s_1$$

with probability at least $1 - 2^{-s_1/2+1}$ according to lemma 2. Similarly, b is also independently and randomly chosen, and we have

$$H_2(S|B{=}b, C{=}c, G{=}g, A{=}a, U{=}u) \geq (t{-}2m)n{-}s_1{-}s_2$$

with probability at least $(1 - 2^{-s_1/2+1})\cdot(1 - 2^{-s_2/2+1})$. Let $s_1 = (t - 2m)n/4$; we obtain

$$H_2(S|B = b, C = c, G = g, A = a, U = u) \geq (t - 2m)n/2$$

with probability at least $1 - 2^{-(t-2m)n/8+2} + 2^{-(t-2m)n/4+2}$. From lemma 1, we have

$$H_\infty(S|B = b, C = c, G = g, A = a, U = u) \geq (t - 2m)n/4 \qquad (1)$$

which holds with probability at least $1 - 2^{-(t-2m)n/8+2} + 2^{-(t-2m)n/4+2} \geq 1 - 2^{-(t-2m)n/8+2}$.

From lemma 3, we know that there exist n_0 and for all $n \geq n_0$ numbers $w < mn$, $r = \Omega(n)$ and a function E: $\{0, 1\}^n \times \{0, 1\}^w \rightarrow \{0, 1\}^r$, computable in polynomial time, with the following property. If T is an n bit random variable satisfying $H_\infty(T) \geq (t - 2m)n/4$, and V is a w bit uniformly distributed random variable, we have

$$H(E(T, V)|V) \geq r\left(1 - 2^{-n/(2(\log n)^3)}\right)\cdot\left(1 - 2^{-n/(2(\log n)^2)} - 2^{-r}\right)$$

Using eqn. 1 and $I(G; SU) = 0$, we obtain

$$\begin{aligned} &H(S'|G, A, B, C, U = u) \\ &\geq r\left(1 - 2^{-n/(2(\log n)^3)}\right)\cdot\left(1 - 2^{-n/(2(\log n)^3)} - 2^{-r}\right) \\ &\quad \times \left(1 - 2^{-(t-2m)n/8+2}\right) \\ &\geq r - r \cdot \left(2^{-n/(2(\log n)^3)+1} + 2^{-r} + 2^{-((t-2m)n/8-2)}\right) \\ &= r - 2^{-\Omega(n)} \end{aligned}$$

Eve is active, we need to determine the upper bound on the probability of the event that Alice and Bob do not both reject although secret-key agreement has not been successful. There are two cases in which this can occur: one is where Eve successfully guesses $a = f_g(S)$ to impersonate Bob and makes Alice accept. The other case is where, after Eve saw $f_g(S)$, she successfully guesses $c = f_b(S)$ to impersonate Alice, and makes Bob accept.

In the first case, Eve knows $U = u$, and $H_2(S|U = u) \geq tn$, so the probability that Eve successfully guesses $a = f_g(S)$ is upper-bounded by

$$2^{-(mn/2n)(H_2(S|U=u)-n/2)} = 2^{-(m/2)\cdot(t-1/2)n} \qquad (2)$$

according to lemma 4 and the fact that success probability of impersonation attack is upper bounded by that of a substitution attack.

In the second case, Eve knows $U = u$, $G = g$, $A = a$, and $H_2(S|G = g, A = a, U = u) \geq (t - m + 1/2)n/2$ holds with a probability of at least $1 - 2^{-(t-m-1/2)n/4+1}$ according to lemma 2. If $H_2(S|G = g, A = a, U = u) \geq (t - m + 1/2)n/2$ holds, the probability that Eve successfully guesses $a' = f_{g'}(S)$ given (g, $a = f_g(S)$) is upper-bounded by $2^{-(mn/2n)(H_2(S|G=g,A=a,U=u)-n/2)} = 2^{-(m/2)\cdot(t-m-1/2)n/2}$ according to lemma 4. Including the case where $H_2(S|G = g, A = a, U = u) \geq (t - m + 1/2)n/2$ does not hold, we have that the success probability is upper bounded by

$$\begin{aligned} &2^{-(m/2)\cdot(t-m-1/2)n/2}\left(1 - 2^{-(t-m-1/2)n/4+1}\right) \\ &\quad + 2^{-(t-m-1/2)n/4+1} \\ &\leq 2^{-(m/2)\cdot(t-m-1/2)n/2} + 2^{-(t-m-1/2)n/4+1} \qquad (3) \end{aligned}$$

From eqns. 2 and 3, we conclude that the success probability of such an active attack is upper-bounded by

$$\delta \leq 2^{-(m/2)\cdot(t-1/2)n} + 2^{-(m/2)\cdot(t-m-1/2)n/2} + 2^{-(t-m-1/2)n/4+1} = 2^{-\Omega(n)}$$

Conclusion: We have improved Wolf's protocol by using string S both for authentication and input of an extractor. Analysis of the improved protocol shows that strong privacy amplification by communication over an insecure and non-authentic channel is possible for sufficiently large n when the adversary's Rényi entropy about S exceeds only $n/2$ rather than $2n/3$.

© IEE 1999 *4 February 1999*
Electronics Letters Online No: 19990262
DOI: 10.1049/el:19990262

Liu Shengli and Wang Yumin (*National Key Laboratory on ISN of Xidian University, Xi'an 710071, People's Republic of China*)

References

1 BENNETT, C.H., BRASSARD, G., and ROBERT, J.-M.: 'Privacy amplification by public discussion', *SIAM J. Comput.*, 1988, **17**, (2), pp. 210–229

2 BENNETT, C.H., BRASSARD, G., CREPEAU, C., and MAURER, U.M.: 'Generalized privacy amplification', *IEEE Trans.*, 1995, **IT-41**, (6), pp. 1915–1923

3 WOLF, S.: 'Strong security against active attacks in information-theoretic secret-key agreement'. Advances in Cryptology-ACIACRYPT'98, Lecture Notes in Computer Science, (Springer-Verlag, 1998), Vol. 1514, pp. 405–419

4 NISAN, N., and ZUCKERMAN, D.: 'Randomness is linear in space', *J. Computer Syst. Sci.*, 1996, **52**, (1), pp. 43–52

5 COVER, T.M., and THOMAS, J.A.: 'Elements of information theory' (Wiley Series in Telecommunications, New York, 1992)

Circuit model for mode conversion in coplanar waveguide asymmetric shunt impedances

M. Ribó and L. Pradell

A new 'circuit model' for the conversion between even and odd modes in coplanar waveguide asymmetric shunt impedances is presented. The model is based on the separation of modes into two input and two output ports. In contrast to previous work, it allows a quantitative analysis of the energy exchange between modes.

Introduction: Uniplanar guiding structures, such as coplanar waveguides (CPWs) and slotlines, are widely used in hybrid and monolithic (MMIC) microwave integrated circuits, due to the fact that discrete shunt components are easily mounted without the need for via holes. A CPW is multimoded, supporting two fundamental modes; the coplanar even-mode (CEM), or coplanar-mode, and the coplanar odd-mode (COM), or slotline-mode. Applications of CPWs include amplitude and phase modulators [1 – 3], frequency multipliers [4, 5] and mixers [3, 6 – 8]. These functions are achieved by an energy exchange between the CEM and the COM which takes place at two shunt-mounted Schottky or *pin* diodes.

A number of models for the mode conversion at CPW shunt diodes, represented by two general impedances Z_A and Z_B in Fig. 1*a*, have been proposed. In [1, 2, 4], the CPW is modelled by two uncoupled slotlines supporting only one (slotline) mode, whereas the model in [3] allows the CEM to be separated from the COM. Although these models are useful in the particular case of shunt diodes excited by a slotline, they cannot be applied to a more general situation, in which either CPW mode (CEM or COM) is exciting the impedances. Furthermore, they do not provide a quantitative analysis of the energy exchange between CEM and COM. In [9], a two-port CPW asymmetric discontinuity is modelled as an equivalent four-port 'black box', each port corresponding to a mode (either even or odd). Since this method requires measurements, it is not easily applicable to CAD.

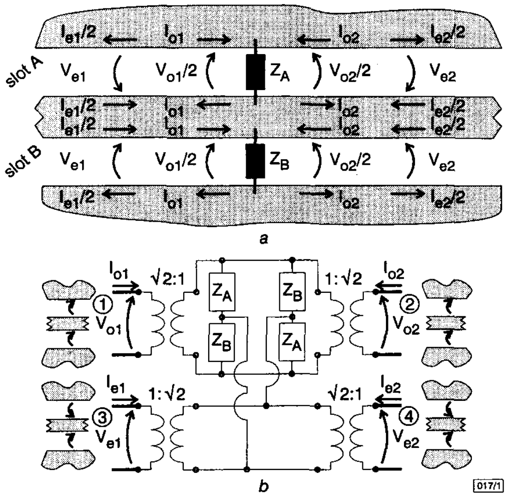

Fig. 1 *Asymmetric shunt-impedances in coplanar waveguide (CPW)*

a Voltages and currents of CPW even and odd-modes at impedance plane
b Four-port circuit model that separates input and output even and odd-modes into different ports

In this Letter, a new four-port 'circuit model' for the energy exchange between even and odd modes at the CPW shunt impedances, is proposed. In contrast to [9], the model is not a 'black box', but a four-port circuit which does not require measurements. Therefore, it can be easily implemented in microwave CAD. Since the circuit separates the modes into different ports, it overcomes the limitations of previous models [1 – 4] in that it provides a quantitative analysis of mode conversion, enables the shunt-impedances in a CPW section loaded with (coplanar) structures presenting different responses to each mode to be analysed, and allows the CPW shunt-impedances to be excited with either mode (CEM or COM). Validation of the model is achieved through its application to CPW circuits designed at K-band (18–26.5GHz).

Model derivation: Consider the structure shown in Fig. 1*a*, composed of a symmetrical CPW section with two shunt impedances, Z_A and Z_B, connected across the slots *A*, *B*, respectively. Each slot can be seen as a transmission line propagating both the CEM and COM. We denote the left and right sides of the slots by subscripts $i = 1, 2$, respectively. The slot voltages and currents at the impedance plane, V_{Ai}, V_{Bi}, I_{Ai}, I_{Bi} $(i = 1, 2)$ are written as functions of the CEM and COM voltages and currents V_{oi}, V_{ei}, I_{oi}, I_{ei}, $(i = 1, 2)$:

$$V_{Ai} = (V_{oi}/2) - V_{ei} \qquad V_{Bi} = (V_{oi}/2) + V_{ei} \qquad (1)$$

$$I_{Ai} = I_{oi} - (I_{ei}/2) \qquad I_{Bi} = I_{oi} + (I_{ei}/2) \qquad (2)$$

By substituting eqns. 1 and 2 into the boundary conditions (Kirchoff laws) $V_{A1} = V_{A2}$, $V_{B1} = V_{B2}$, $I_{A2} + I_{A1} = V_{A1}/Z_A$, $I_{B2} + I_{B1} = V_{B1}/Z_B$, imposed by the impedances Z_A and Z_B, the following equation system is obtained:

$$\begin{bmatrix} V_{o1} \\ V_{o2} \\ V_{e1} \\ V_{e2} \end{bmatrix} = \frac{1}{4}\begin{bmatrix} 4(Z_A{+}Z_B) & 4(Z_A{+}Z_B) & 2(Z_A{-}Z_B) & 2(Z_A{-}Z_B) \\ 4(Z_A{+}Z_B) & 4(Z_A{+}Z_B) & 2(Z_A{-}Z_B) & 2(Z_A{-}Z_B) \\ 2(Z_A{-}Z_B) & 2(Z_A{-}Z_B) & (Z_A{+}Z_B) & (Z_A{+}Z_B) \\ 2(Z_A{-}Z_B) & 2(Z_A{-}Z_B) & (Z_A{+}Z_B) & (Z_A{+}Z_B) \end{bmatrix}\begin{bmatrix} I_{o1} \\ I_{o2} \\ I_{e1} \\ I_{e2} \end{bmatrix} \qquad (3)$$

The 4 × 4 *Z*-matrix in eqn. 3 leads to the circuit model proposed in Fig. 1*b*, composed of impedances Z_A and Z_B connected to ideal transformers in an impedance-bridge configuration. The new model relevant features are:

(i) It separates the CEM contribution from the COM contribution in the multimode CPW, into different monomode CPWS (ports) with characteristic impedances Z_{oe} (for CEM) and Z_{oo} (for COM). Therefore, planar structures that present different responses to each mode (such as slotline-to-CPW transitions and air-bridges) can easily be connected by loading the four ports in Fig. 1*b* with proper impedances.

(ii) It allows the energy transfer from one mode to the other to be quantitatively analysed.

In particular, whenever $Z_A = Z_B$, it can be seen (from eqn. 3 or Fig. 1*b*) that there is no energy conversion from the even-mode to odd-mode and vice versa. Conversely, whenever $Z_A \neq Z_B$, a mode conversion takes place. Since the model contains circuit elements, it can be used to analyse or design any application with shunt impedances, such as those presented in [1 – 8], provided that the impedance values are well known. Whenever a mode is cut off, its effect is also easily included by terminating the appropriate ports in Fig. 1*b* with reactive impedances.

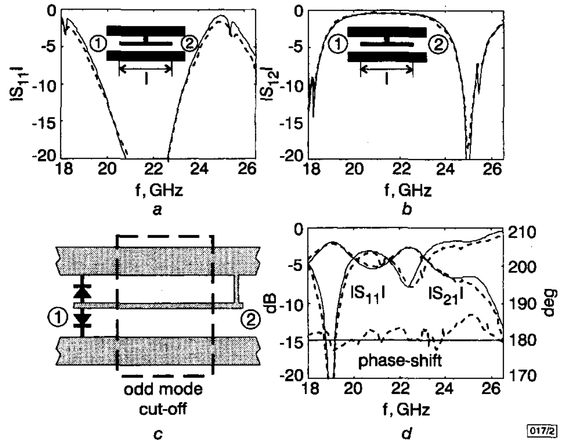

Fig. 2 *Experimental validation of circuit model in Fig. 1b*

- - - - measurement
——— simulation
CPW section with centred asymmetric short-circuit in one of slots:
a $|S_{11}|$
b $|S_{12}|$ BPSK modulator
c Outline
d $|S_{11}|$, $|S_{21}|$ and phase shift
CPW slot and central conductor widths: 0.1mm (*a*, *b*); 0.25mm (*c*)
CPW section lengths: l = 33.53mm (*a*, *b*); l = 32.2mm (*c*)

Model application and experimental validation: The proposed model has been applied to two K-band (18–26.5GHz) CPW circuits fabricated on CuClad 217, ε_r = 2.17, thickness = 0.254mm (see Fig. 2) and placed in the E-plane of a WR-42 rectangular waveguide. Both circuits include two slotline-to-CPW transitions at their input and output ports, respectively, because excitation is performed through slotline sections. The first circuit (Fig. 2*a*, *b*) is a CPW section with a centred asymmetric shunt load (short-circuit) in one of the slots, corresponding to $Z_A \simeq 0$, $Z_B \to \infty$ in Fig. 1*a*. The slotline-to-CPW transitions add a small parasistic shunt susceptance for the COM, but they act as an open circuit for the CEM. Consequently, according to the model proposed (Fig. 1*b*), the circuit is equivalent to a COM transmission line (length *l*) loaded at its centre with two CEM open-ended transmission lines (length *l*/2). Fig. 2*a*, *b* show the simulated *S*-parameters, obtained from the model, and the measured *S*-parameters, showing excellent agreement. The second circuit (Fig. 2*c*) is a CPW BPSK-modulator. Two shunt-connected beam-lead *pin* diodes (MA4P800 from MACOM) are biased asymmetrically (bias circuits are not shown) and their bias states are switched from on/off to off/on. Therefore, according to the model proposed (Fig. 1*b*) the incoming slotline-mode is converted into the COM and CEM, the CEM being phase-modulated (0°/180°) at the same rate as the diodes are switched. Both waves propagate forward along the CPW section. The COM is cut off (by placing metal planes very close to both sides of the dielectric substrate) at the appropriate distance from the diode plane. The CEM reaches the other end of the CPW section, being partially converted into COM forward and backward waves by the upper slot short-circuit. The COM forward-wave propagates out to the output slotline section. The COM backward-wave is cutoff at the appropriate distance. Modulator S-parameters and the phase-shift (both simulated using eqn. 3 and measured) are shown in Fig. 2*d*. Again, their agreement is excellent, demonstrating the validity of model and its applicability.

Conclusions: A new 'circuit model' that enables a quantitative analysis to be carried out of the energy exchange between even and odd modes at asymmetric shunt impedances in CPW, has been proposed, and applied to the simulation of CPW microwave circuits. The excellent agreement between simulated results and S-parameter measurements demonstrates the validity of the model and its usefulness as a CAD tool in the design and optimisation of hybrid/MMIC microwave CPW circuits.

Acknowledgment: This work has been supported by the research project TIC97-1129-C04-04 financed by the Spanish Government CICYT.

© IEE 1999 *18 March 1999*
Electronics Letters Online No: 19990507
DOI: 10.1049/el:19990507

M. Ribó (*Enginyeria La Salle, Ramon Llull University* (*URL*), *Dept. CTS, Pg. Bonanova 8, 08026 Barcelona, Spain*)

L. Pradell (*Polytechnic University of Catalunya* (*UPC*), *Dept. TSC, Campus Nord UPC, 08034 Barcelona, Spain*)

References

1 OGAWA, H., AIKAWA, M., and AKAIKE, M.: 'Integrated balanced BPSK and QPSK modulators for the Ka-band', *IEEE Trans.*, 1982, **MTT-30**, pp. 227–234

2 TARUSAWA, Y., OGAWA, H., and HIROTA, T.: 'A new constant-resistance ASK modulator using double-sided MIC', *IEEE Trans.*, 1987, **MTT-35**, pp. 819–822

3 CALLSEN, H., MEINEL, H.H., and HOEFER, W.: 'p-i-n diode control devices in E-plane technique', *IEEE Trans.*, 1989, **MTT-37**, pp. 307–316

4 OGAWA, H., and MINAGAWA, A.: 'Uniplanar MIC balanced multiplier-A proposed new structure for MICs', *IEEE Trans.*, 1987, **MTT-35**, pp. 1363–1368

5 YANEV, A.S., TODOROV, B.N., and RANEV, V.Z.: 'A broad-band balanced HEMT frequency doubler in uniplanar technology', *IEEE Trans.*, 1998, **MTT-46**, pp. 2032–2034

6 RAMAN, S., RUCKY, F., and REBEIZ, G.M.: 'A high-performance W-band uniplanar subharmonic mixer', *IEEE Trans.*, 1997, **MTT-45**, pp. 955–962

7 MAO, S.G., CHIOU, H.K., and CHEN, C.H.: 'Design and modeling of uniplanar double-balanced mixer', *IEEE Microw. Guid. Wave Lett.*, 1998, **8**, pp. 354–356

8 HSU, P.C., NGUYEN, C., and KINTIS, M.: 'A new uniplanar broad_band singly balanced diode mixer', *IEEE Trans.*, 1998, **MTT-46**, pp. 1782–1784

9 DIB, N.I., GUPTA, M., PONCHAK, G.E., and KATEHI, L.P.B.: 'Characterization of asymmetric coplanar waveguide discontinuities', *IEEE Trans.*, 1993, **MTT-41**, pp. 1549–1558

Scalable 10Gbit/s 4 × 2 0.25μm CMOS/SIMOX ATM switch LSI circuit based on distributed contention control

E. Oki, N. Yamanaka, K. Okazaki and Y. Ohtomo

A scalable 10Gbit/s 4 × 2 ATM switch LSI circuit has been fabricated. It employs a new distributed contention control technique that makes the LSI circuit expandable. To increase the LSI circuit throughput, 0.25μm CMOS/SIMOX (separation by implanted oxygen) technology is used. It allows the LSI circuit to offer 221 I/O pins, an operating speed of 1.25Gbit/s and 7W power consumption.

To meet the expected increase in demand for multimedia services, it will be necessary to create asynchronous transfer mode (ATM) switching systems that have a throughput of > 1Tbit/s. For such systems, an appropriate choice is the crosspoint-LSI-type switch architecture, in which identical switch LSI circuits are arranged on a matrix plane. The modularity of the switch design allows the switch to be easily expanded.

The conventional crosspoint-LSI-type switch architecture uses ring arbitration among switch LSI circuits to avoid output-bus-access contention, as shown in Fig. 1*a*. This contention occurs when ATM cells from different switch LSI circuits request transmission to the same output line (bus) during the same ATM cell time. The control signal for ring arbitration must pass through all the switch LSI circuits belonging to the same output line within the ATM cell time [1]. However, as the output-line speed increases, the ATM cell time decreases. In a crosspoint-LSI-type switch with a large number of row switch LSI circuits, ring arbitration cannot be completed within the short ATM cell time. Therefore, conventional switches based on ring arbitration are not scalable due to the centralised contention control mechanism. We have fabricated a scalable 10Gbit/s 4 × 2 switch LSI circuit that employs a new distributed contention control technique, called scalable distributed arbitration (SDA), that allows the LSI circuit to be expanded.

SDA has an ATM output buffer and a transit buffer at each output port in a switch LSI, as shown in Fig. 1*b*. An output buffer sends a request (REQ) to CNTL if there is at least one ATM cell stored in the output buffer. A transit buffer stores several cells that are sent from either the output buffer of the upper switch LSI or the transit buffer of an upper switch LSI circuit. The transit buffer also sends REQ to CNTL if there is at least one cell stored in the transit buffer. If the transit buffer is about to become full, it sends a not-acknowledgment (NACK) to the upper CNTL. If there is an REQ and CNTL does not receive NACK from the next lower transit buffer, then CNTL selects a cell within one ATM cell time. CNTL determines which cell should be sent according to its cell arrival time. To compare the arrival time of competing cells, we use a synchronous counter, which needs S bits. S was set to 8 in the switch LSI circuits. The selected ATM cell is transferred from its output buffer to the output line by way of several transit

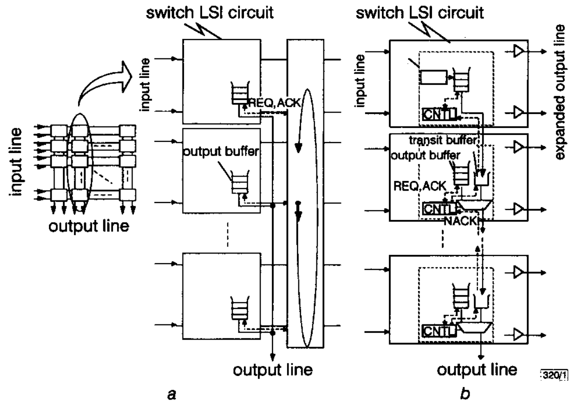

Fig. 1 *Contention control among switch LSIs*

a Ring arbitration (conventional)
b Scalable distributed arbitration (SDA) (proposed)