where $t = \lfloor \log_3 P \rfloor$. If $P \simeq 2^{512}$, then at most 36027 stored values are needed.

Future work: This point leads us to wonder whether an optimum HTQNS representation exists such that time and space is further reduced. For example, take two bases k and h, where $k > h$ and $h \neq 2$. We can construct the following recurrent relations:

$$p_s^t = \frac{1}{k} p_{s-1}^{k(t \bmod h)} + \frac{1}{h} \sum_{\substack{u=0 \\ (u+ht) \bmod k \neq 0}}^{h-1} p_{s-1}^{h(t \bmod k)+u}, t=0,1,2,\ldots,kh-1$$

These asymptotic solutions will estimate the average number of modular multiplications. Conversely, the amount of storage is at most $t + \Sigma_{j=0}^{t} \lfloor \log_k(P/h^j) \rfloor$, where $t = \lfloor \log_h P \rfloor$. In our view, searching proper bases k and h such that both time and space are reduced is an open problem.

© IEE 1996 *2 January 1996*
Electronics Letters Online No: 19960345

C.-Y. Chen and W.-P. Yang (*Department of Computer and Information Science, National Chiao Tung University, Hsinchu, Taiwan 300, Republic of China*)

C.-C. Chang (*Institute of Computer Science and Information Engineering, National Chung Cheng University, Chiayi, Taiwan 621, Republic of China*)

References

1 BRICKELL, E.F., GORDON, D.M., McCURLEY, K.S., and WILSON, D.B.: 'Fast exponentation with precomputation'. Proceedings of Eurocrypt' 92 (Springer-Verlag, 1993), pp. 200–207

2 DIMITROV, V., and COOKLEV, T.: 'Two algorithms for modular exponentiation using nonstandard arithmetics', *IEICE Trans. Fundam.*, 1995, **E78-A**, (1), pp. 82–87

3 EL-GAMAL, T.: 'A public key cryptosystem and signature scheme based on discrete logarithms', *IEEE Trans. Inf. Theory*, 1985, **IT-31**, (4), pp. 469–472

Analogue squarer and multiplier based on MOS square-law characteristic

S.-I. Liu and D.-J. Wei

Indexing terms: Multiplying circuits, CMOS analogue integrated circuits, MOSFET

A simple CMOS squarer based on MOS square-law characteristic is presented. This circuit was fabricated in a 0.8μm single-poly double-metal *n*-well CMOS process. Experimental results show that the nonlinearity of the squarer can be kept below 2% across the entire differential input voltage range of ±1V. The total harmonic distortion is < 2% with the input range up to ±0.8V. Moreover, a four-quadrant multiplier can be also realised using the proposed squarers. The proposed circuits are expected to be useful in analogue signal-processing applications.

Introduction: Many CMOS analogue signal-processing building blocks which exploited the square-law model of the MOS transistors have been developed in the literature [1 – 6], e.g. CMOS multipliers, transconductors and resistors based on the square-algebraic identity can be easily realised since the squaring function can be obtained from the well known square-law model of the MOS transistors operated in saturation [1 – 6]. In this Letter, we propose a simple CMOS squarer which can also be used for realising a four-quadrant multiplier. Experimental results are given to verify the theoretical analysis.

Circuit description: The proposed CMOS squarer and its symbol are shown in Fig. 1. Assume that all the devices in Fig. 1 are biased in the saturation region without the body effect. Let the transconductance parameter and the threshold voltage of M_1 to M_8 be equal to K and V_T, respectively. I_B is the DC current. By describing the source currents of M_1 to M_4, the following relations in Fig. 1 can be obtained i.e.

$$I_1 + I_2 = I_2 + I_3 = I_3 + I_4 = I_B \qquad (1)$$

where I_i is the source current of the PMOS transistor M_i (for $i = 1$ to 4). From eqn. 1 and after some algebraic calculations, the voltage v_S can be expressed as

$$v_S = \frac{v_M + v_N}{2} \qquad (2)$$

The voltage v_S is the averaging value of the voltages v_M and v_N [2, 5]. From the transistors, M_5 to M_8, it is also found that

$$v_M = \frac{v_1 + V_{DD}}{2} \qquad (3)$$

and

$$v_N = \frac{v_2 + V_{DD}}{2} \qquad (4)$$

Assume that the aspect ratio of M_9 is twice that of M_5 (and M_7). According to the proposed squarer in Fig. 1, the output voltage V_o can be expressed as

$$\begin{aligned}\frac{V_o}{R} &= I_5 + I_7 - I_9 \\ &= K(V_{DD} - v_M - V_T)^2 + K(V_{DD} - v_N - V_T)^2 \\ &\quad - 2K(V_{DD} - v_S - V_T)^2 \qquad (5)\end{aligned}$$

where I_i is the source current of the PMOS transistor M_i (for $i = 5$, 7 and 9). Substituting eqns. 2 – 4 into eqn. 5, the output voltage V_o in Fig. 1 can be obtained as

$$V_o = \frac{K}{8} R(v_1 - v_2)^2 \qquad (6)$$

A simple CMOS squarer can be realised. For proper operation, it is required that all the devices operated in the saturation i.e.

$$\max\left(v_1, v_2, \frac{v_1 + v_2}{2}\right) < V_{DD} - 2V_T \qquad (7)$$

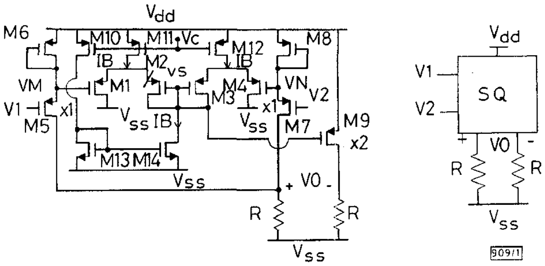

Fig. 1 *Proposed CMOS squarer*

Moreover, based on the square-difference identity ($[a+b]^2 - [a-b]^2 = 4ab$), one squarer with input voltages v_1 and v_2 and the other with input voltages v_1 and $-v_2$ can be used to realise a four-quadrant multiplier as shown in Fig. 2. The output voltage V_o of the multiplier in Fig. 2 can be expressed as

$$V_o = \frac{K}{2} R v_1 v_2 \qquad (8)$$

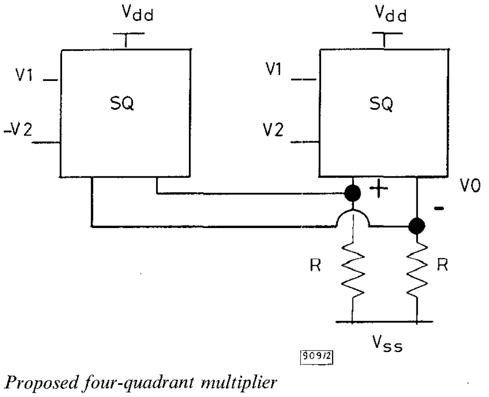

Fig. 2 *Proposed four-quadrant multiplier*

Table 1: Aspect ratios of devices in Fig. 1

Transistor	M_1-M_8	M_9	$M_{10}-M_{14}$
W/L (µm/µm)	5/5	10/5	25/5

Experimental results: The circuit was fabricated in a standard 0.8 µm single-poly double metal *n*-well CMOS process. The aspect ratios of all the devices in Fig. 1 are listed in Table 1. Fig. 3 shows the layout diagram of the proposed squarer. The measurement conditions are : R = 100 kΩ and the supply voltage = +2.5V. The input range of the squarer with the nonlinearity < 2% is within 1V. Fig. 4 shows a typical output waveform of the squarer where v_1 (= $-v_2$) is a sinusoidal signal. The measured –3dB bandwidth of this squarer was ~1MHz. The proposed multiplier was also demonstrated as working properly.

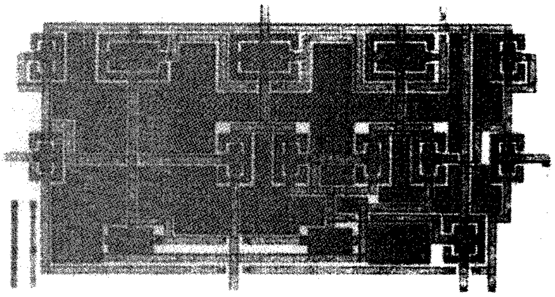

Fig. 3 *Layout diagram of Fig. 1*

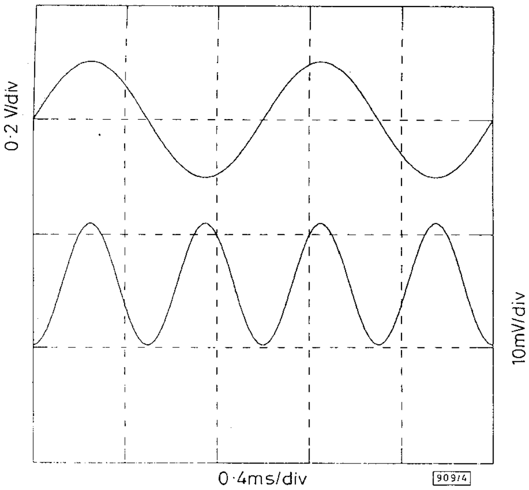

Fig. 4 *Typical output waveform of squarer when a 0.2 V sinusoidal signal of 1kHz was applied to $v_1(= -v_2)$*

Conclusions: In this Letter, a CMOS squarer and a four-quadrant multiplier which were based on the square-law of the MOS transistors have been presented. Experimental results have demonstrated their feasibility. The proposed circuits are expected to be useful in the analogue signal-processing applications.

Acknowledgment: The authors would like to thank the National Science Council for financial supporting and thank the Chip Implementation Center (CIC), National Science Council, Taiwan, R. O. C., for the fabrication of the test chip. This work was sponsored by NSC-85-2215-E-002-021.

© IEE 1996 3 January 1996
Electronics Letters Online No: 19960384

S.-I. Liu and D.-J. Wei (*Department of Electrical Engineering, National Taiwan University, Taipei, 10664 Taiwan, Republic of China*)

References

1 SOO, D.C., and MEYER, R.G.: 'A four-quadrant MOS analog multiplier', *IEEE J. Solid-State Circuits*, 1982, **SC-17**, pp. 1174–1178

2 TORRANCE, R.R., VISWANATHAN, T.R., and HANSON, J.V.: 'CMOS voltage to current transconductors', *IEEE Trans. Circuits Syst.*, 1985, **CAS-32**, pp. 1097–1104

3 BULT, K., and WALLINGA, H.: 'A class of analog CMOS circuits based on the square-law characteristics of an MOS transistor in saturation', *IEEE J. Solid-State Circuits*, 1987, **SC-22**, pp. 357–365

4 SINGH, S.P., HANSOM, J.V., and VLACH, J.: 'A new floating resistor for CMOS technology', *IEEE Trans. Circuit Syst.*, 1989, **SC-36**, pp. 1217–1220

5 WILSON, B., and CHAN, P.K.: 'Low-distortion CMOS transconductor', *Electron. Lett.*, 1990, **26**, pp. 720–722

6 LIU, S.I., and HWANG, Y.S.: 'CMOS four-quadrant multiplier using bias-offset crosscoupled pairs', *Electron. Lett.*, 1993, **29**, (20), pp. 1737–1738

Acousto-optic switch with a near rectangular passband for WDM systems

D.A. Smith, H. Rashid, R.S. Chakravarthy,
A.M. Agboatwalla, A.A. Patil, Z. Bao, N. Imam,
S.W. Smith, J.E. Baran, J.L. Jackel and J. Kallman

Indexing terms: Wavelength division multiplexing, Acousto-optical switches

The authors describe the most rectangular passband yet reported for an acousto-optic wavelength-routing switch. The device is a multicycle SAW directional-coupler-weighted AOTF, fabricated on XY lithium niobate, with a –3dB width of 2.52nm and a –20dB width of 0.89nm. For comparison, an ideal apodised AOTF with the same 3dB width would have a –20dB width of only 0.33nm.

Large-scale WDM systems contain wavelength selective elements that ideally need to have a rectangular spectral profile, to allow cascadability, improve wavelength misalignment tolerance and reduce interchannel crosstalk. This Letter describes the most rectangular passband yet reported for an acousto-optic wavelength-routing switch. Sidelobe suppression and peak flattening can be realised by controlling the amplitude and phase of the envelope of the photoelastic grating which constitutes the interaction region of an AOTF [1]. For example, sidelobe suppression can be achieved by embedding the active optical waveguide of the WDM filter in the crossarm of a SAW directional coupler so that the observed interaction strength is apodised with a tapered onset and cutoff. Adjusting the weighting function affects the depth of sidelobe suppression [2]. Theoretical calculations by G. H. Song predicted that a rectangular filter would require a tapered-onset of the AO interaction strength followed by three cycles of an oscillating acoustic interaction strength with an overall exponential decay envelope [3]. Our group designed a filter which maintains the qualitative features of Song's proposal and which coupled-mode theory predicted would have excellent rectangularity (Fig. 1). The filter incorporates a linear-tapered onset, and three full cycles of SAW amplitude in a length of only 39mm by using a zero gap SAW coupler [4].

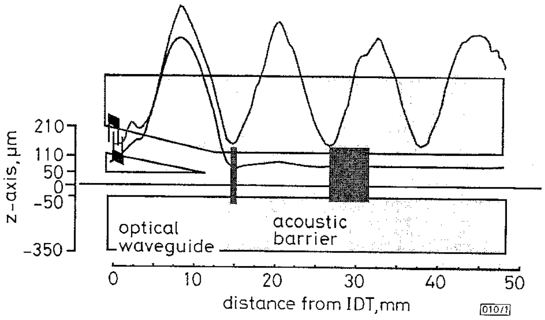

Fig. 1 *Schematic diagram of multicycle SAW-coupler-based AOTF showing measured SAW intensity profile before and after step attenuators were put in place*

Top trace: before
Bottom trace: after