New squaring architecture: A block diagram of the new squaring architecture is shown in Fig. 1. This architecture consists of an LSD-multiplier, such as that introduced in [5], and a squaring adapter. The multiplier is used to compute products and sums and the squaring adapter is used to generate and propagate operands to the multiplier.

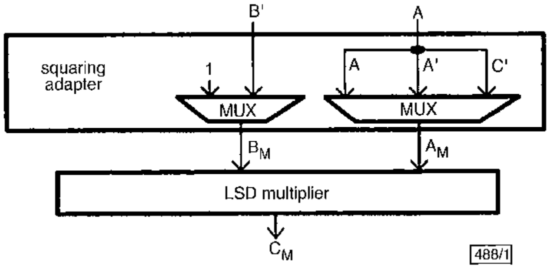


Fig. 1 *New squaring architecture*

LSD-multipliers implement variations of the multiplication algorithm, such as algorithm 1. The inputs to this algorithm are the field elements $A = \Sigma_{i=0}^{m-1} a_i \alpha^i$ and $B = \Sigma_{i=0}^{k_B \le \lceil m/D \rceil - 1} B_i \alpha^{Di}$, where $B_i = \Sigma_{j=0}^{D-1} b_{Di+j} \alpha^j$. Note that the field element B is expressed in at most $\lceil m/D \rceil$ digits, where each digit is represented by D bits. Also, note that the multiplication finishes when the most significant nonzero digit of B, B_{k_B}, is processed.

```
Algorithm 1: LSD multiplication:
  For $i = 0$ to $k_B$ do
      $C = B_i * (A * \alpha^{Di} \bmod F(\alpha)) + C$
  $C = C \bmod F(\alpha)$
```

From algorithm 1 it is evident that an LSD-multiplier can compute the operation described by eqn. 2 by first multiplying A' and B' and then adding to it the product of C' and 1. For the computation of these products, the host system provides the squaring adapter with operands A and B'. During the computation of the product of A' and B', the squaring adapter generates A' according to eqn. 3 and forwards it along with B' to the multiplier. During the accumulation of C', the squaring adapter generates C' according to eqn. 5 and forwards it along with the 1 operand to the multiplier.

The computation of a square requires a multiplication and a sum. The computation of the sum requires one clock cycle and the computation of the multiplication requires $\lceil(\deg(B') + 1)/D\rceil$ clock cycles. The squaring operation requires $\lceil(k+1)/D\rceil+1$ clock cycles when m is even, $\lceil(k+2)/D\rceil+1$ clock cycles when m is odd and $k < m - 1$, and $\le\lceil(k+1)/D\rceil+1$ clock cycles when m is odd and $k = m - 1$.

The complexity of the squaring adapter is approximately $3.5m + D$ two-input gates and its critical path delay is four gates. The complexity of an LSD-multiplier depends on its architecture and irreducible polynomial support. As a reference, the realisation of an LSD-multiplier documented in [5] that supports field polynomials of order $k < m - D$ with h programmable coefficients requires approximately $2Dm + 7m + 4Dh$ gates and $3m + D + h$ registers. (This estimate considers the system I/O and accumulator reset, which are not considered in [5].)

Table 1: Distribution of squaring-to-multiplication processing time ratios for fields in range m = 160–1024

T_{sq}/T_{mul}	Distribution	Cumulative distribution
	%	%
0.05–0.10	32	32
0.10–0.20	23	55
0.20–0.30	16	71
0.30–0.50	29	100

Squaring processing time for cryptosystems: We conclude by analysing the suitability of the squarer architecture for cryptographic applications. Table 1 summarises the squaring-to-multiplication processing time ratio, T_{sq}/T_{mul}, for the field polynomials suggested by the cryptographic standard [6], assuming the use of an LSD-multiplier with D = 1. The Table can be interpreted as follows: 32% of all fields in the range considered allow squaring at least 10 times (1/0.1) as fast as multiplication, 23% between 5 times and 10 times (1/0.2) as fast, etc.

Acknowledgment: This research was supported in part through NFS CAREER award CCR-9733246.

© IEE 2000 *18 April 2000*
Electronics Letters Online No: 20000824
DOI: 10.1049/el:20000824

G. Orlando and C. Paar (*ECE Department, Worcester Polytechnic Institute, 100 Institute Rd., Worcester, MA 01609, USA*)

E-mail: orlandog@wpi.edu

References

1 WU, H.: 'Low complexity bit-parallel finite field arithmetic using polynomial basis' *in* KOC, C., and PAAR, C. (Eds.): 'Workshop on cryptographic hardware and embedded systems (CHES '99), August 1999, (Springer-Verlag), Vol. LNCS 1717

2 PAAR, C., FLEISCHMANN, P., and SORIA-RODRIGUEZ, P.: 'Fast arithmetic for public-key algorithms in Galois fields with composite exponents', *IEEE Trans.*, 1999, **C-48**, pp. 1025–1034

3 JAIN, S.K., SONG, L., and PARHI, K.K.: 'Efficient semisystolic architectures for finite-fields arithmetic', *IEEE Trans. VLSI Syst.*, 1998, **6**, pp. 101–113

4 LIDL, R., and NIEDERREITER, H.: 'Finite fields' *in* 'Encyclopedia of mathematics and its applications, Vol. 20' (Addison-Wesley, Reading, Massachusetts, 1983)

5 SONG, L., and PARHI, K.K.: 'Low-energy digit-serial/parallel finite field multipliers', *J. VLSI Sig. Process. Syst.*, 1997, **2**, (22), pp. 1–17

6 A. X9.62-199x, 'Public key cryptography for the financial services industry: The elliptic curve digital signature algorithm (ECDSA)'. January 1998. Approved January 7, 1999

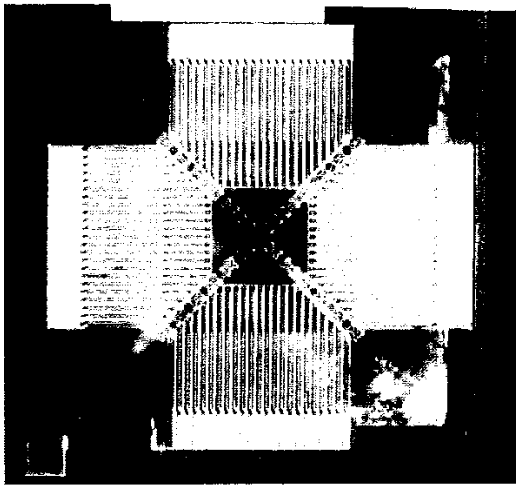
CMOS compatible thermoelectric infrared sensors

Chin-Shown Sheen and Sien Chi

A new structure for CMOS compatible thermoelectric infrared sensors is proposed. By using micro-link structures to connect several floating membranes, the largest floating membrane area yet obtained and large output voltages have been realised. The characteristics of the sensors have been measured, and are compared with those of existing devices.

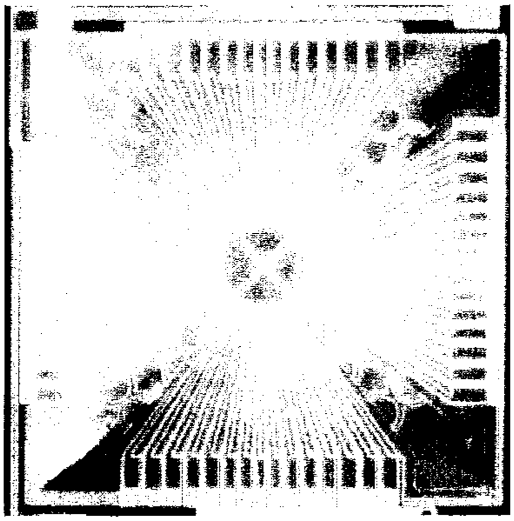
Introduction: Since micromachining using a standard CMOS IC fabrication process was first described [1, 2], a number of sensor applications have been proposed and demonstrated. For CMOS compatible thermoelectric infrared (IR) sensors, to obtain a better performance the aim of the design is to reduce the thermal conductance and increase the active area. In addition to the backside etching technique, the current trend is to create a floating membrane by using a front-side etching technique. For an inherent front-side etching technique, etching windows must be opened in the front-side and the silicon substrate under the membrane etched. Conventionally, using front-side etching techniques, two types of floating structure have been reported: the suspension beam structure and the floating membrane. The membrane is formed and then floats after the silicon substrate underneath is etched. The main drawback of the first structure is that it is easy to bend so that it cannot be made large. For the second structure, the area of membrane is limited by the design consideration that the extended under-cut etching area of opened windows must overlap. This requires long etching times. We propose a micro-link structure for the first time, which enables a larger area of membrane to be realised while reducing the etching time. The detectivity can reach > 2 × 10^8 cm√Hz/W, which is even larger than that obtained using backside etching techniques [3].

Fabrication and measurements: The samples were first fabricated in a 1.2μm CMOS process (UTEK, Taiwan) as a pre-processing step before silicon micromachining. Inherent features of CMOS technology and etching properties of its <100> substrate allow the fabrication of open silicon dioxide microstructures (beams or suspended membranes) by anisotropic silicon etching from the front side of the wafer. The central part of the silicon substrate beneath the masked membrane is removed and only a roughly 2μm thin sandwich layer of SiO_2/Si_3N_4 on top is left. Onto this membrane two standard thermoelectric conducting materials (*n*-poly, Al) are deposited and structured. Both conductors have alternative junctions at the centre of the membrane (hot junctions) and above the edge of the silicon substrate (cold junctions). An IR-absorbing layer covers the hot junctions.



673/1

Fig. 1 *Photograph of ML-1 sample*



673/2

Fig. 2 *Photograph of ML-2 sample*

We propose two new membrane structures, which have four large freestanding-like membranes and each is connected to neighbouring membranes by small link structures, termed ML-1 and ML-2, respectively. The use of such small links gives several advantages for the design beyond the inherent geometrical patterns of front-side etching.

The first sample, ML-1, with 90 pairs of thermoelectric elements, is constructed on an 1100 × 1100μm² floating membrane, which is shown in Fig. 1. There are six micro-links between each near-neighbouring membrane with a width of 6μm. The etching windows are opened carefully to allow for silicon substrate etching, and after the etching a pyramid cavity is left.

The second sample, ML-2, with 60 pairs of thermoelectric elements, has a 1300 × 1300μm² floating membrane, which is shown in Fig. 2. Each nearest-neighbour membrane is connected by three micro-links, enabling the largest floating membrane yet realised to be created by a front-side etching technique. The etching windows are opened efficiently so that the silicon substrate beneath is anisotropically etched completely, leaving a pyramid cavity.

A transistor cap with IR filter hermetically seals the sensor chip. The transmission range of the IR filter is chosen to be 5–14μm in accordance with the application for detecting living objects.

Table 1: Characteristics of different thermopiles

Parameter	OTC236 [5]	ML-1	ML-2	Baltes [4]	TPS434 [3]
Chip size [mm²]	1.72×1.95	1.72×1.95	1.72×1.95	–	2.2×2.2
Elements *N*	44	92	60	40	40
Resistance [kΩ]	65	36	35.2	–	40
Sensitivity [V/W]	55	93.7	95.5	30	48
NEP [nW/√Hz]	0.59	0.26	0.25	–	0.54
Detectivity [cm√Hz/W] D^*	8.53×10^7	1.94×10^8	2.01×10^8	3×10^7	9.3×10^7
Time constant [ms]	18	18	18	10	20
Etching method	front-side	front-side	front-side	front-side	back-side

Table 1 lists the characteristics for existing devices and the micro-link samples. For the front-side etched thermopile devices, the detectivity is always small and $< 10^8$cm√Hz/W. For ML-1 and ML-2, the detectivity is the highest yet reported using the front-side etching method [4, 5]. However, they are also good enough to compete with backside-etched devices [3]. The membrane area of ML-2 is larger than that of ML-1 so that a larger active area could be used and the performance of ML-2 is as good as that of ML-1.

Conclusions: We have proposed a new structure for floating membrane devices for the first time, which enables a large area of membrane to be obtained while reducing the etching time. The detectivity can reach $> 2 \times 10^8$ cm√Hz/W, which is even larger than that of existing devices realised using backside etching techniques. A larger membrane structure area could be obtained by using micro-link structures and more flexible structures could be designed by incorporating such structures.

© IEE 2000 27 April 2000
Electronics Letters Online No: 20000823
DOI: 10.1049/el:20000823

Chin-Shown Sheen and Sien Chi (*Institute of Electro-Optical Engineering, National Chiao Tung University, Taiwan, Republic of China*)

Chin-Shown Sheen: Also with Opto Technology Corporation, Hsinchu, Taiwan, Republic of China

E-mail: hilbert@dreamer.com.tw

References

1 LENGGENHAGER, R., and BALTES, H.: 'Improved thermoelectric infrared sensor using double poly CMOS technology'. Tranducers'93, Dig. Tech. Papers, Yokohama, Japan, 1993, pp. 1008–1011

2 SHEEN, CHIN-SHOWN: 'A highly sensitive CMOS compatible thermal-type microsensor'. 16th IEEE Instrumentation and Measurement Technology Conf., Venice, Italy, May 1999

3 SCHIEFERDECKER, J., QUAD, R., HOLZENKÄMPF, E., and SCHULZE, M.: ''. Proc. Eurosensors VIII, Toulouse, 1994, pp. 417–422

4 BALTES, H.: 'CMOS as sensor technology', *Sens. Actuators A*, 1993, **37–38**, pp. 51–56

5 SHEEN, CHIN-SHOWN: 'A new fibre-communication miniature sensor module'. 2000 IEEE Instrumentation and Measurement Technology Conf., Baltimore, Maryland, USA, May 2000