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.

![Squaring Architecture Diagram](image_url)

**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 $A = \sum_{i=0}^{m-1} a_i \alpha^i$ and $B = \sum_{i=0}^{m-1} b_i \alpha^i$, where $B_i = \sum_{j=0}^{m-1} b_{i+j} \alpha^j$. Note that the field element $B$ is expressed in at least $\lceil mD \rceil$ digits, where each digit is represented by $D$ bits. Also, note that the multiplication finishes when the most significant nonzero digit of $B \times B'$ is processed.

Algorithm 1: LSD multiplication:

For $i = 0$ to $k-1$ do

$$C = B_i \ast (A \ast \alpha^i \mod F(a)) + C$$

$$C = C \mod F(a)$$

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 this product, 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 $\lceil (k+1)D \rceil + 1$ clock cycles when $m$ is odd and $k = m - 1$.

The complexity of the squaring adapter is approximately $3m + D$ 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 realization 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>
<thead>
<tr>
<th>$T_{sq}/T_{add}$</th>
<th>Distribution</th>
<th>Cumulative distribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.05-0.10</td>
<td>32</td>
<td>32</td>
</tr>
<tr>
<td>0.10-0.20</td>
<td>23</td>
<td>55</td>
</tr>
<tr>
<td>0.20-0.30</td>
<td>16</td>
<td>71</td>
</tr>
<tr>
<td>0.30-0.50</td>
<td>29</td>
<td>100</td>
</tr>
</tbody>
</table>

squaring processing time for cryptosystems: We conclude by analysing the suitability of the squaring architecture for cryptographic applications. Table 1 summarises the squaring-to-multiplication processing time ratio, $T_{sq}/T_{add}$ 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 (10.1) as fast as multiplication, 23% between 5 times and 10 times (10.2) as fast, etc.

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

© IEE 2000

Electronics Letters Online No: 20000024

C. Orlando and C. Paar (ECE Department, Worcester Polytechnic Institute, 109 Institute Rd., Worcester, MA 01609, USA)

E-mail: orlandog@wpi.edu

References


CMOS compatible thermoelectric infrared sensors

Chin-Shown Shenc 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 undercut 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 $> 2 \times 10^6$ cm$^2$/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 SiO2/SiN4 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.

The first sample, MI-1, with 90 pairs of thermoelectric elements, is constructed on an 1100 x 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 x 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

<table>
<thead>
<tr>
<th>Parameter</th>
<th>OTC236</th>
<th>ML-1</th>
<th>ML-2</th>
<th>Baltes</th>
<th>TP534</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chip size [mm²]</td>
<td>1.72x1.95</td>
<td>1.72x1.95</td>
<td>1.72x1.95</td>
<td>—</td>
<td>2.2x2.2</td>
</tr>
<tr>
<td>Elements N</td>
<td>44</td>
<td>92</td>
<td>60</td>
<td>40</td>
<td>40</td>
</tr>
<tr>
<td>Resistance [Ω]</td>
<td>65</td>
<td>56</td>
<td>35.2</td>
<td>—</td>
<td>40</td>
</tr>
<tr>
<td>Sensitivity [mV/W]</td>
<td>35</td>
<td>93.7</td>
<td>95.5</td>
<td>30</td>
<td>48</td>
</tr>
<tr>
<td>NEP [nW/Hz]</td>
<td>0.59</td>
<td>0.26</td>
<td>0.26</td>
<td>—</td>
<td>0.54</td>
</tr>
<tr>
<td>Detectivity [cm²/HzW]</td>
<td>8.53x10⁷</td>
<td>1.94x10⁸</td>
<td>2.0x10⁸</td>
<td>3x10⁷</td>
<td>9.3x10⁷</td>
</tr>
<tr>
<td>Time constant [ms]</td>
<td>18</td>
<td>18</td>
<td>18</td>
<td>10</td>
<td>20</td>
</tr>
<tr>
<td>Etching method</td>
<td>front-side</td>
<td>front-side</td>
<td>front-side</td>
<td>back-side</td>
<td></td>
</tr>
</tbody>
</table>

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 < 10⁵cm²/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 x 10⁸cm²/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

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 LIEPMANN, R., and BALTES, H.: 'Improved thermoelectric infrared sensor using double poly CMOS technology', Transducers'93, Dig. Tech. Papers, Yokohama, Japan, 1993, pp. 1008-1011