Secondly, as M is odd, we could replace M by a multiple $M' = mM$ with the property $mM \equiv 1 \pmod{2^t}$. However, the result using the scaled modulus M' will need some further minor postprocessing to reduce it modulo the original M. Alternatively, the modulus can be chosen to satisfy $M \equiv 1 \pmod{2^t}$ directly. The modulus used in the RSA cryptosystem is a product p_1p_2 of two primes, each typically of around 100 decimal digits in length. These primes are obtained by considering a sequence of numbers until one is found that, using an algorithm such as that of Solovay and Strassen [4], is likely to be prime with a given very high probability. Any suitable choice for the first prime p_1 will determine the congruence which p_2 must satisfy, namely $p_2 \equiv p_1^{-1} \pmod{2^t}$. The same algorithm can then be used to search for an appropriate value for the second prime.

A consequence of these simplifications is that the bottom t digits of R are determined merely by shifting down the bottom $t+1$ digits of its previous value. Because these digits do not change when S is added, they will be the digits q. Thus the digits q are indeed produced when required. Moreover, they can be obtained in nonredundant binary form: because the lowest t digits of R are initially 0, they have nonredundant form initially, and thereafter, the digit at position $t+1$ can be converted to nonredundant form, with its carry moving upwards, so that the nonredundancy property of the lowest digits is maintained.

Conclusion: To sum up, for any number n of binary digits in the modulus of the modular multiplication, we have described how to generate the digits required for the modular reduction steps without delaying the formation of the product. Thus modular multiplication suited for RSA may be implemented in $n+O(\log n)$ clock cycles using the algorithm of Montgomery and a clock cycle determined by an adder with a critical path length of only three gates. This adder has just half the depth of those used previously in the literature, and so leads to significantly faster performance.

© IEE 1995 *22 December 1994*
Electronics Letters Online No: 19950217

C.D. Walter (*Computation Department, UMIST, PO Box 88, Sackville Street, Manchester M60 1QD, United Kingdom*)

References

1 RIVEST, R.L., SHAMIR, A., and ADLEMAN, L.: 'A method for obtaining digital signatures and public-key cryptosystems', *Commun. ACM*, 1978, **21**, pp. 120–126

2 BRICKELL, E.F.: 'A fast modular multiplication algorithm with application to two-kwy cryptography' *in* CHAUM *et al.* (Eds.): 'Advances in Cryptology - CRYPYO '82' (Plenum, New York, 1983), pp 51–60

3 MONTGOMERY, P.L.: 'Modular multiplication without trial division', *Math. Comput.*, 1985, **44**, pp. 519–521

4 SOLOVAY, R., and STRASSEN, V.: 'A fast Monte-Carlo test for primality', *SIAM J. Comput.*, 1977, **6**, pp. 84–85

5 WALTER, C.D.: 'Faster modular multiplication by operand scaling'. Advances in Cryptology - CRYPTO '91, Lecture Notes in Comp. Sci, vol. **576**, 1992, pp. 131–323 (Springer-Verlag)

6 WALTER, C.D., and ELDRIDGE, S.E.: 'Hardware implementation of Montgomery's modular multiplication algorithm', *IEEE Trans.*, 1993, **C-42**, pp. 693–699

Noncontacting optical generation of focused surface acoustic waves using a customised zoneplate

M. Liu, H.P. Ho, M.G. Somekh and J.M.R. Weaver

Indexing terms: Surface acoustic wave devices, Computer-generated holograph, Holograph optical elements

The use of computer generated holographic zoneplates to enhance the generation of laser ultrasound is described. An amplitude grating capable of focusing laser light onto an arc which in turn generates a near diffraction limited focus of 82MHz Rayleigh surface waves is also described. The application of zoneplates for ultrasonic nondestructive evaluation and imaging is considered.

Introduction: Laser generation and detection of ultrasound is becoming increasingly important. This Letter describes the fabrication of specially designed zoneplates, to produce controlled ultrasonic field distributions which can be tailored for specific applications. To demonstrate the approach, this Letter describes the design, fabrication and testing of a zoneplate capable of producing tightly focused high frequency surface acoustic waves (SAWs).

Focusing of SAWs is important because the signal to noise ratio for a given illumination intensity on the sample surface is improved, and the confinement gives improved lateral resolution, necessary for imaging applications. Focusing of SAWs on a sample surface occurs naturally in the scanning acoustic microscope [1] because the leaky surface waves are excited on a ring. Furthermore Koymen *et al.* [2] have used SAWs generated on an arc to image surface defects. This Letter describes the implementation of similar ideas in a noncontacting system.

Design of zoneplate: To focus the SAWs on an isotropic surface it is necessary to illuminate the sample surface in the form of the arc of a circle. The focusing element was designed to focus incident light from a distance of 80mm to an arc whose half angle was 30°, with a radius of curvature of 2mm.

A design procedure akin to that used for binary holograms [3] was employed. To compute the appropriate zoneplate design, light from the arc, C, was propagated to the plane of the zoneplate, where the amplitude and phase distribution at this plane is calculated. The ideal field distribution was then approximated by dividing the optical field into an array of pixels; if the calculated phase lay between 0 and $-\pi$, the transmissivity of the pixel was set to zero, if, on the other hand, the phase lay between 0 and π the transmissivity of the pixel was set to a value proportional to the amplitude at this point. The amplitude weighting factor was controlled by adjusting the opening width. The pixel was fully open at the position of maximum amplitude.

This approximation to the desired surface distribution was improved further by a process of iteration. The field distribution arising from the approximation was then calculated and if the surface distribution along C differs from the desired distribution by a factor $R(C)$, the design procedure described in the previous paragraph was repeated by weighting the arc C by the factor $1/R(C)$. This procedure was repeated until no material improvements in the arc profile were obtained. The binary zoneplates designed by the procedure described above were then fabricated using an electron beamwriter capable of nanometre lithography.

Results: Testing of the zoneplates was carried out in two stages. First the optical focusing was tested and secondly the resulting SAW distribution was measured. Zoneplates designed for illumination with 532 and 1064nm radiation were fabricated for each stage of the testing.

A plate designed for 532 nm operation was illuminated with laser light and the focal arc was projected onto a CCD camera. The resulting focal arc had a measured width of ~45μm, which is within 10% of the predicted width. The binary nature of the zoneplate is such that there is considerable zero order background, which will be removed in future implementations using phase gratings. The zoneplate designed for 1064nm could not be readily tested with the CCD camera but scanning a point detector confirmed that the line width was double the value obtained for the 532nm zoneplate (to within 5%). The width of the arc is wider than optimum for efficient SAW generation and higher numerical aperture plates are currently being designed.

To generate SAWs, an Nd:YAG laser which emitted short pulses whose approximate duration was 400ps with a repetition frequency of 82MHz was used. The simultaneous operation of the Q-switch operating with a repetition frequency of 500Hz limited the emission of the modelocked pulses to a period corresponding to ~30 pulses, this greatly increased the peak power, thus improving the SAW generation efficiency. The mean power from the laser was ~1W giving an average energy per pulse of 70μJ. This is extremely modest, and no damage could be observed from close examination in the optical microscope. The pump beam was then focused onto the sample through the zoneplate so that the arc could be projected onto the sample surface. The displacement produced by the pump beam was detected with a phaselocked interferometer whose probe position could be varied by scanning the focusing optics. The output signal was passed via amplification and filter stages to a digital storage scope, which was triggered by the optical beam.

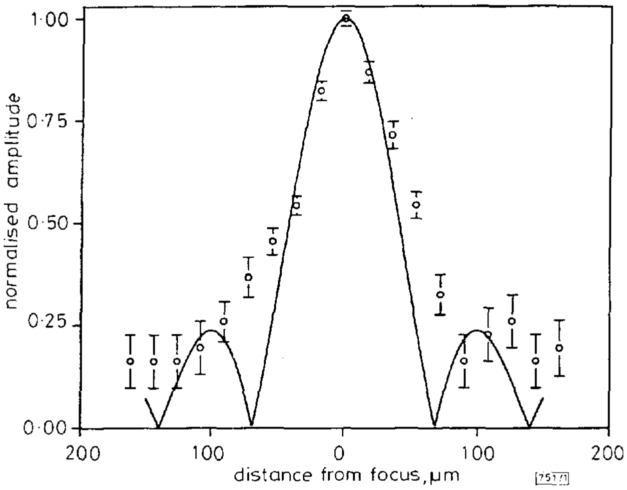

Fig. 1 *Surface wave amplitude against position on SAW focal line*

—— theoretical
O experimental

Fig. 1 shows the variation in the amplitude of the 82MHz SAW on a silicon nitride sample as the probe is scanned across the focal plane. The overlaid theoretical plot was obtained using a SAW velocity of 5800ms^{-1}. It can be seen that the zoneplate produces surface waves focused to a near diffraction limited focus.

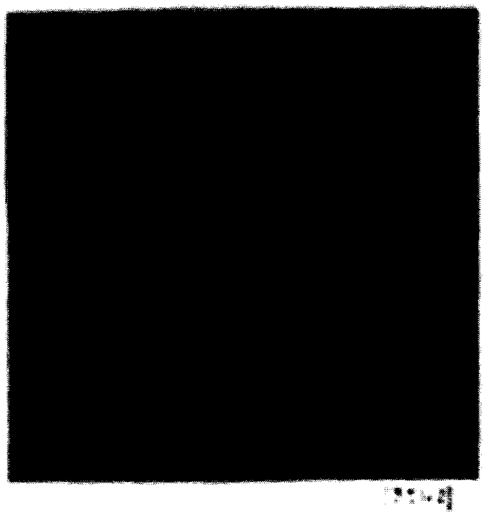

Fig. 2 *Micrograph obtained by scanning sample under generation and detection optics, Rayleigh wave interference fringes formed by reflection from the edge of silicon nitride sample*

Image width = 160µm

To demonstrate the imaging potential of the system, preliminary images were obtained by scanning silicon nitride relative to the optical detection and generation system. Fig. 2 shows a scan taken close to the edge of a silicon nitride sample. A standing wave pattern arising from the reflection of surface waves at the edge of the sample is clearly visible. The periodicity of the standing wave pattern is half the Rayleigh wavelength and is similar to features observed in the scanning acoustic microscope [4]. The system has also been used to image a surface breaking defect which is small compared to the SAW wavelength, where the change in surface wave intensity can be clearly observed; again this is a similar contrast mechanism to that observed in the scanning acoustic microscope [5].

Discussion and further work: This Letter describes the development of simple customised optics to enhance laser ultrasound generation. The power of the method lies in the possibility of designing a surface wave distribution for specific applications. For instance, concentric rings could be produced to combine focusing and surface wave frequency selection. The design of zoneplates to focus on complex component shapes is another important application.

In the present implementation binary zoneplates have been used which give a large zero order background signal. The technology for producing etched phase structures with far greater efficiency will be examined in the future.

The preliminary results indicate that efficient customised zoneplate structures will be extremely valuable in the development of efficient high resolution systems operating with modest laser pump power levels.

Acknowledgments: This work was funded by Brite Euram (project number BE 4398) and the Royal Society.

© IEE 1995 *22 December 1994*
Electronics Letters Online No: 19950216

M. Liu, H.P. Ho and M.G. Somekh (*Department of Electrical and Electronic Engineering, University of Nottingham, University Park, Nottingham NG7 2RD, United Kingdom*)

J.M.R. Weaver (*Department of Electronics and Electrical Engineering, University of Glasgow, Glasgow G12 8QQ, United Kingdom*)

References

1 SMITH, I.R., WICKRAMASINGHE, H.K., FARNELL, G.W., and JEN, C.K.: 'Confocal surface acoustic wave microscopy', *Appl. Phys. Lett.*, 1983, **42**, (5), pp. 411–413

2 KOYMEN, H., ATALAR, A., CILOGLU, T., ONDER, M., UZEL, C., and YAVUZ, H.: 'Imaging flaws close to surface using focused surface acoustic-waves', *IEEE Trans.*, 1987, **UFFC-34**, (3), pp. 399–400

3 BROWN, B.R., and LOHMANN, A.W.: 'Complex spatial filtering with binary masks', *Appl. Opt.*, 1966, **5**, (6), pp. 967–969

4 YAMANAKA, K., and ENOMOTO, Y.: 'Fringe pattern around surface crack observed with scanning acoustic microscope', *Electron. Lett.*, 1981, **17**, (18), pp. 638–640

5 SOMEKH, M.G., BERTONI, H.L., BRIGGS, G.A.D., and BURTON, N.D.: 'A two dimensional imaging theory of surface discontinuities in the scanning acoustic microscope', *Proc. Roy. Soc. Lond.*, 1985, **A401**, pp. 29–51

3V, 28mW Si-bipolar front-end IC for 900 MHz homodyne wireless receivers

HongMo Wang and M. Banu

Indexing terms: Bipolar integrated circuits, Silicon, Radio receivers

A 900MHz homodyne receiver front-end bipolar chip is presented. The circuit consists of a low-noise amplifier and two double-balanced mixers for in-phase and quadrature channels. The power supply voltage is 3V and power dissipation is 28mW. The measured performance includes 33.5dB voltage gain, a 3.1dB noise figure, -13dBm input referred IP3, -95dB LO leakage into the RF port on wafer probing, and less than 0.1dB I/Q magnitude imbalance.

Recently, there has been a renewed interest in developing fully integrated homodyne (direct-conversion) receivers for digital wireless communications [1, 2]. [1] describes a 5V chip which does not include an LNA, and [2] describes a fully integrated design for pagers. The main motivation for a homodyne design is the fact that current radio technology is still far from a single-chip realisation of the successful superheterodyne architecture [3]. High-quality IF filters at practical frequencies are realisable only with discrete components. However, if the IF frequency is reduced to zero, on-chip filtering solutions do exist. Despite this theoretical suitability for integration, IC homodyne receivers are difficult to fabricate due to inherent and severe practical problems such as sensitivity to noise, local oscillator (LO) leakage, I/Q channel imbalances, DC offsets, etc. The design is further complicated if low voltage and low power are also required. In an actual receiver, shown as a block diagram in Fig. 1, many of the difficulties mentioned above are directly related to the front-end stage. In this