test antenna and the probe array and their associated electronic equipment.

For an electrically modulated array, each diode is connected to the LF multiplexer that sequentially applies modulation via a resitive line. Thus for each diode, two such lines are needed. As the frequency increases, the space between diodes will become smaller, the wires will be very close, and in addition they have to be perpendicular to the electric field. In most cases, it is again difficult to predict the error caused by these wires.

The following describes a new free space laser beam modulated array technique. Instead of using an ordinary diode load at the centre of the dipole element, a photodiode is placed at the centre of each dipole element. A laser scanning system is used to scan the elements, so the photodiodes in the array can be illuminated sequentially by a modulated laser beam and the local field in the plane of the array can be sampled effectively at the location of the elements to produce a two dimensional representation of the field in that plane.

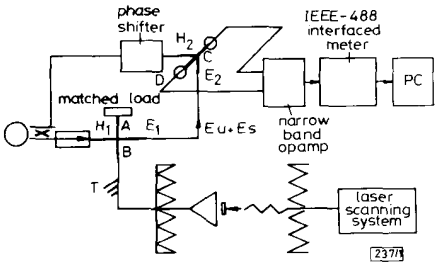

Fig. 1 *General arrangement for 8·5 GHz modulated scatter measurement*

Use of modulated diode as dipole to measure field: There are many types of system that can be adopted for measurement of fields using modulated scatterers. The system used here is shown in Fig. 1. The 3 dB coupler is used to convey the reference signal to the H arm of the second magic T, thus avoiding the disturbance to the signal channel. Because of the imperfection of the magic T, and reflection from surrounding objects, an unmodulated RF signal will leak to arm E_1 together with modulated back scattered signal from the photodiode detector. By using a coherent system as shown in Fig. 1, these unwanted signals would not be detected. Thus the final signal is not affected by the unmodulated component. The output from the operational amplifier is the coherent response of the system [1]

$$V = GE_f E_s \cos \alpha$$

E_f is the reference signal, E_s is the backscattered signal from the photodiode and α is the phase angle between E_s and E_f. Shifting the reference signal by 90°, we have

$$V = GE_f E_s \sin \alpha$$

Therefore, if the array is scanned twice, shifting the reference by 90° in between, the full vector state will be available. Fig. 2 shows the field aperture amplitude distribution of the horn antenna, measured with a single photodiode detector.

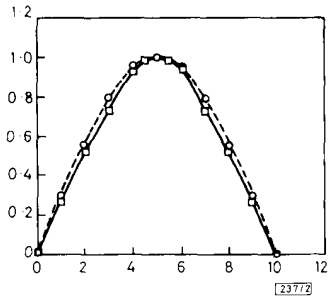

Fig. 2 *Aperture amplitude distribution of 10 cm wide horn at 8·5 GHz*
□ single probe
○ array

Having established a single photodiode measurement, an array was constructed. Each element of the array was calibrated to have the same response; each was set at $\lambda/2$ separation. Six identical dipoles were attached to dry balsa wood which was fixed to a three-dimensional positioner. The laser scanner was preprogrammed to scan 11 points horizontally. Because only six elements can be arranged over 10 cm aperture, the measurement was carried out by scanning twice with the array shifted a distance of $\lambda/4$ between scans. The results are shown in Fig. 2.

Conclusions: An array technique using isolated photodiode modulated scatterers has been demonstrated. It has been shown that providing simple criteria are met, a laser scanning system can be used to probe the array at a distance. Results have been presented which illustrated the relative simplicity of the system compared with electrical modulation. Mutual coupling, although a problem in limiting the resolution of these arrays, does not prevent the functioning of the system providing the element spacing is of the order of a half wavelength. The approach also lends itself to very high frequency measurements where semiconductor large scale integration techniques can be used to fabricate the array.

Acknowledgment: We acknowledge the help and advice of B. Minachovic during the device measurement stage of this work and also other members of the Microwave and Communications Research group. The support of the UK SERC is also gratefully acknowledged.

6th November 1991

S. Q. Zhang and D. J. Edwards (*University of Oxford, Department of Engineering Science, Parks Road, Oxford OX1 3PJ, United Kingdom*)

References

1 RICHMOND, J. H.: 'A modulated scattering technique for measurement of field distributions', *IRE Trans.*, July 1955, pp. 13–15
2 MING-KUEI HU: 'Measurements of microwave E and H field distributions by using modulated scattering methods', *IRE Trans. Microwave Theory and Techniques*, May 1960, pp. 295–230
3 HAJNAL, J. V.: 'Compound modulated scatterer measuring system', *IEE Proc. H*, August 1987, **134**, pp. 350–356
4 HYGATE, G., and NYE, J. F.: 'Measuring microwave fields directly with an optically modulated scatterer', *Meas. Sci. Technol.*, 1990, **1**, pp. 703–709
5 BOLOMEY, J.-C., and COWN, B. J.: 'Rapid near-field antenna testing via arrays of modulated scattering probes', *IEEE Trans.*, June 1988, **AP-36**, pp. 804–813

CRYPTANALYSIS AND MODIFICATION OF DIGITAL SIGNATURE SCHEME BASED ON ERROR-CORRECTING CODE

L. Harn and D.-C. Wang

Indexing terms: Codes and coding, Error-correcting codes, Information theory

W. Xinmei proposed a digital signature scheme based on the error-correcting code. The Letter points out that in the Xinmei scheme it is possible to combine valid signatures of messages into a valid signature of another message in polynomial time even when the factoring of large matrices is unknown. Some modifications are suggested to improve the security and performance.

Introduction: In 1978, McEliece [2] proposed the first public-key encryption system based on the error-correcting code. However, the McEliece cryptosystem requires the use of Goppa codes with large block lengths and the ability to correct a large number of errors. The very large computational overhead degrades performance. Since then, several

private-key cryptosystems [3, 4] based on error-correcting codes have been suggested to lower the computational overhead. In 1990, W. Xinmei proposed the first digital signature scheme based on an error-correcting code. The security of this scheme relies on the difficulty of factoring large matrices. This scheme also requires the use of Goppa codes with large block lengths and large error-correcting abilities to achieve security.

In this Letter, we point out that in the Xinmei scheme it is possible to combine valid signatures of messages into a valid signature of another message in polynomial time even when the factoring of large matrices is unknown. Some modifications are suggested to improve the security and performance.

Description of Xinmei scheme: User A chooses an (n, k, d) binary Goppa code, with a $(k \times n)$ generator matrix $\boldsymbol{G}$, and an error-correcting capability of t errors. The public keys of user A are given as follows:

$$\boldsymbol{J} = \boldsymbol{P}^{-1}\boldsymbol{G}^*\boldsymbol{S}^{-1} = \boldsymbol{P}^{-1}\boldsymbol{W}$$

$$\boldsymbol{W} = \boldsymbol{G}^*\boldsymbol{S}^{-1}$$

$$T = \boldsymbol{P}^{-1}\boldsymbol{H}^T, t$$

where the private keys are two matrices $\boldsymbol{SG}$ and $\boldsymbol{P}$. $\boldsymbol{H}$ denotes an $(n-k) \times n$ parity check matrix, $\boldsymbol{P}$ is an $n \times n$ full rank permutation matrix and $\boldsymbol{S}$ is a $k \times k$ full rank scrambling matrix. $\boldsymbol{G}^*$ is defined as follows:

$$\boldsymbol{G}\boldsymbol{G}^* = \boldsymbol{I}_{k \times k}$$

The signature $\boldsymbol{C}$ of a k-bit message $\boldsymbol{M}$ is obtained by computing

$$\boldsymbol{C} = (\boldsymbol{E} + \boldsymbol{MSG})\boldsymbol{P}$$

where $\boldsymbol{E}$ is a random n-bit error vector of weight $w(\boldsymbol{E}) = t_a < t$ chosen by user A.

Signature verification procedure: Assume that the receiver receives an n-bit signature $\boldsymbol{C}'$ of the message $\boldsymbol{M}$. The verification procedure is given as follows:

(1) Calculate $\boldsymbol{C}'\boldsymbol{T} = \boldsymbol{Se} = (SE_1, SE_2, \ldots, SE_{(n-k)})$

(2) Using the Berlekamp–Massey algorithm, the receiver can obtain $\boldsymbol{E}'$ from $\boldsymbol{Se}$. If $w(\boldsymbol{E}') > t$, the receiver stops the verification procedure and requests retransmission of the signature of user A.

(3) Calculate $\boldsymbol{C}'\boldsymbol{J}$.

(4) Verify whether $\boldsymbol{M} = \boldsymbol{C}'\boldsymbol{J} - \boldsymbol{E}'\boldsymbol{W}$. If it does, then the signature has been verified.

Cryptanalysis: One possible attack on the Xinmei scheme is based on the observation that it is possible to combine valid signatures of messages into a valid signature of another message in polynomial time even when the factoring of large matrices is unknown. For example, if $\boldsymbol{C}_1$, $\boldsymbol{C}_2$, and $\boldsymbol{E}_1$, $\boldsymbol{E}_2$, are two valid signatures and error vectors of $\boldsymbol{M}_1$ and $\boldsymbol{M}_2$, then there exists a possibility that $\boldsymbol{C}_1 + \boldsymbol{C}_2$ is a valid signature of $\boldsymbol{M}_1 + \boldsymbol{M}_2$. This is due to the fact that even if $w(\boldsymbol{E}_1) = t - 1$ and $w(\boldsymbol{E}_2) = t - 1$, there is still a chance that $w(\boldsymbol{E}_1 + \boldsymbol{E}_2) < t$. Because the error vector $\boldsymbol{E}$ is revealed to the public every time during the verification, the attacker can easily select proper message and signature pairs to perform this attack. The cryptanalyst could exploit this relationship to sign an important message $\boldsymbol{M}$ by choosing a proper combination of messages, asking the user to sign them, and then combining these signatures back to $\boldsymbol{C}$.

This attack becomes infeasible if the user perturbs the messages before he signs them. In many applications, the message $\boldsymbol{M}$ needs to be compressed by a one-way function within the range $[0, 2^k - 1]$ before signing them. However, if the compression function is cryptographically strong, the modified scheme can be secure.

Our modified digital signature scheme: Our scheme is very similar to the Xinmei scheme. User A needs to publish the same public keys. In addition, a one-way hash function $h(\ )$ needs to be made public.

The signature $\boldsymbol{C}$ of message $\boldsymbol{M}$ is obtained by computing.

$$\boldsymbol{C} = h(\boldsymbol{M})\boldsymbol{SGP}$$

Signature verification procedure: Assume, owing to the channel noise, $\boldsymbol{E}$ is a random n-bit error vector of weight $w(\boldsymbol{E}) = t'$ and the receiver receives an n-bit signature $\boldsymbol{C}'$ of the message $\boldsymbol{M}$. We can represent $\boldsymbol{C}' = \boldsymbol{C} + \boldsymbol{E}$. The verification procedure is given as follows:

(1) Calculate $\boldsymbol{C}'\boldsymbol{T} = h(\boldsymbol{M})\boldsymbol{SGH}^T + \boldsymbol{EP}^{-1}\boldsymbol{H}^T = \boldsymbol{E}'\boldsymbol{H}^T = \boldsymbol{Se}' = (SE'_1, SE'_2, \ldots, SE'_{(n-k)})$.

(2) Using the Berlekamp Massey algorithm, the receiver can obtain $\boldsymbol{E}'$ from $\boldsymbol{Se}'$. If $w(\boldsymbol{E}') > t$, the receiver stops the verification procedures and requests retransmission of the signature of user A.

(3) Calculate $\boldsymbol{C}'\boldsymbol{J}$.

(4) Verify whether $h(\boldsymbol{M}) = \boldsymbol{C}'\boldsymbol{J} - \boldsymbol{E}'\boldsymbol{W}$. If it does, then the signature has been verified.

Discussions:

(*a*) In the Xinmei cryptosystem, if $t_a < t$, then up to $t - t_a$ errors may occur in the channel and these errors can be corrected by the receiver. Thus the system provides both digital signature and error-correcting ability simultaneously. Because the system becomes less secure if t_a is small, but provides less error-correcting ability if t_a is large, there is a tradeoff between security and error-correcting ability. In our modified digital signature scheme, the security no longer relies on the random error vector that the user added in on purpose; therefore, it provides full error-correcting capability for possible channel errors.

(*b*) In the Xinmei cryptosystem, because the security relies on the random error vector, it requires the use of Goppa codes with large block lengths and abilities to correct a large number of errors. This involves very large computational overhead in signature generation and signature verification. In our modified scheme, because the security no longer relies on the random error vector, some simple error-detecting codes, such as the Hamming code or cyclic code, can be used to reduce the computational overhead. However, for those simple codes, $\boldsymbol{H}$ cannot be revealed to the public. In other words, we need to modify steps 2–4 in the signature verification procedure into:

(2′) Check to see if all syndrome bits $\boldsymbol{Se}'$ are zeros. If not, the receiver stops the verification procedures and requests retransmission of the signature of user A.

(3′) Verify whether $h(\boldsymbol{M}) = \boldsymbol{C}'\boldsymbol{J}$. If it does, then the signature has been verified.

The simple error-detecting code that we choose should have syndrome bits sufficiently large to provide good security.

(*c*) The security of our modified scheme is based on the difficulty of factoring large matrices. Just like the Xinmei scheme, by knowing the public keys, it is computationally infeasible to obtain the secret signature key $\boldsymbol{SGP}$.

14th November 1991

L. Harn and D.-C. Wang (*Computer Science Telecommunications Program, University of Missouri—Kansas City, Kansas City, MO 64110, USA*)

References

1 XINMEI, W.: 'Digital signature scheme based on error-correcting codes', *Electron. Lett.*, 1990, **26**, (13), pp. 898–899

2 MCELIECE, R. J.: 'A public-key cryptosystem based on algebraic coding theory', *DSN Progress Report*, 1978, **42–44**, pp. 114–116

3 RAO, T. R. N., and NAM, K. H.: 'Private-key algebraic-coded cryptosystems', *in* 'Advances in cryptology—Crypto '86' (Springer-Verlag, 1986), pp. 35–48
4 HWANG, T., and RAO, T. R. N.: 'Secret error-correcting codes', *in* 'Advances in cryptology—Crypto '88' (Springer-Verlag, 1988), pp. 540–563

SILICON GERMANIUM OPTICAL WAVEGUIDES WITH 0·5 dB/cm LOSSES FOR SINGLEMODE FIBRE OPTIC SYSTEMS

S. F. Pesarcik, G. V. Treyz, S. S. Iyer and J. M. Halbout

Indexing terms: Optoelectronics, Optical waveguides, Silicon

Silicon germanium waveguides with losses of less than 1 dB/cm have been fabricated and characterised at 1·32 μm. Propagation losses are as low as 0·62 dB/cm for TM polarised light and 0·50 dB/cm for TE polarised light.

Silicon waveguides are the foundation for many experimental optical devices: sensors, switches, filters and logic devices. For good device performance in systems, waveguide losses must be reduced to acceptable levels. For waveguide devices that couple to optical fibres, the guides should be singlemode, large in cross-section, and have small losses due to scattering or absorption. Waveguides based on crystalline SiGe are attractive because a small refractive index difference can be achieved and a relatively thick structure can be grown, of the order of 10 μm. The small index step provides a good mode match to optical fibres and reduces scattering losses from imperfections in the guides.

The Si-based waveguides reported until recently suffered from high losses. Soref [1] demonstrated large-mode waveguides fabricated from lightly-doped Si grown epitaxially on heavily-doped Si substrates. These guides suffered high losses of 5–12 dB/cm from free-carrier absorption because of the doped substrate. As an alterative to the doped substrate, Si on insulator has been investigated by several groups. Although Kurdi [2] predicted that the losses could be as low as 1 dB/cm, SIMOX guides typically also suffered from high losses. Recently, Schmidtchen [3] did achieve losses of 0·5 dB/cm in SIMOX material, but the large index step could make coupling to optical fibres difficult. SiGe waveguides have been demonstrated in ridge waveguide configurations, with losses reported as low as 1·9–3·2 dB/cm [4]. We propose and demonstrate that the addition of a Si layer on top of the SiGe layer reduces scattering losses, nearly eliminates absorption losses, and provides good coupling to singlemode optical fibres.

Structure and fabrication: The waveguide structure consists of a high-resistivity ⟨100⟩ Si substrate, 6·5 μm of undoped $Si_{0.984}Ge_{0.012}$ and 3·0 μm of undoped Si grown epitaxially by chemical vapour deposition. The waveguide rib is 16 μm in width and 4·1 μm in height, extending through the top Si layer and 1·1 μm into the SiGe layer. RBS gives the layer composition as 1·2 ± 0·1% Ge. X-ray diffractometry data from the vendor [5] indicate that this layer is 84% relaxed. Nomarski optical inspection of the layer, revealed by etching, shows a dense, cross-hatched dislocation pattern, confirming that the layer is highly relaxed. The small compositional step produces the desired small step in refractive index.

A single lithographic step and reactive ion etching define the waveguide rib. Following cleaning of the wafer and spinning of the photoresist, proximity lithography with an optically-generated mask defined the features. The waveguides are oriented 1° off of the ⟨011⟩ direction. Reactive ion etching in SF_6 : Freon-115::1 : 1 for 13 min defined ribs with nearly vertical sidewalls and a small outward taper at their bases. SEM inspection revealed some minor roughness in the sidewalls that could contribute to scattering losses.

Cleaving a sample of nominal dimensions 1 × 8 cm^2 provided 70 waveguides for measurement. Lapping and polishing of the input and output facets yielded smooth vertical facets, although a few guides had a scratch visible by optical inspection at × 105 magnification. Following each set of optical throughput measurements, the sample was again cleaved near the output facet, lapped and polished to a shorter length. The five lengths used in this experiment are 7·81, 6·29, 4·42, 3·73 and 3·06 cm.

Measurement of losses: By means of the cut-back technique we determined the waveguide loss and could estimate the insertion loss for coupling to a singlemode fibre. Linearly polarised light at 1·32 μm is launched into the waveguides from a dispersion-shifted, singlemode fibre with an 8 μm diameter core. For every waveguide, the guide and fibre are aligned for maximum throughput of TM polarised light, and this same alignment was also used for measuring transmission of TE polarised light. A microscope objective focused the emission from the output facets onto an aperture. A polarising beam splitter then separated the TE and TM components so that their powers could be measured individually by a pair of germanium photodiodes. Using long sample lengths (> 3 cm) assures us that any light coupled into radiation modes is effectively removed from the waveguide and hence the detection system. Further, the tilt of 1° between the guides and the facets reduces Fabry–Perot effects while introducing negligible changes to the coupling of light from the fibre to the waveguides.

The optical power emitted from the fibre was likewise collected and measured so that the transmission for each guide could be determined. We calculated the total transmission, defined as total power exiting a waveguide divided by the total power exiting the fibre, for a given input polarisation. We also calculated the polarised transmission by using the TE (TM) powers emitted from the waveguides and fibre. Linear regression to the transmission data determined the losses for each waveguide.

Chosen for low loss and good regression correlation (Pearson's $|r| = 0·94$ and 0·99), the best waveguide has losses of 0·58 ± 0·12 dB/cm for TE input light and 0·81 ± 0·08 dB/cm for TM input light. The data are shown in Fig. 1. To our knowledge, these are the lowest losses reported for waveguides in the SiGe system. The waveguide preserved the polarisation of the light, and by considering polarised transmission, the losses are the same to within experimental error: 0·58 and 0·78 dB/cm.

The measurements yielded 53 out of 70 guides with $|r| > 0·90$, indicating a good fit to the TM transmission data. Correlation values for TE transmission are generally lower by 0·05 due to the alignment technique, and only 37 guides have $|r| > 0·90$. The mean losses are 0·73 dB/cm (TE input) and 1·05 dB/cm (TM input), with standard deviations of 0·15 and

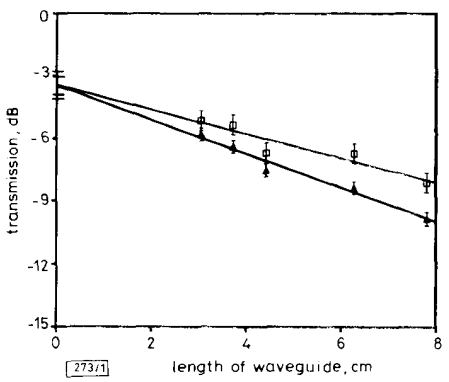

Fig. 1 *Transmission losses of best waveguide for TE and TM input polarisations as function of length*
Losses for this guide are 0·58 and 0·81 dB/cm
□ TE polarisation
△ TM polarisation