direction and have reverse-mesa shape (115°) along the [110] direction. However, the behaviour observed in AlInAs is more general, resulting also in the Br_2–CH_3COOH system.[5] Experiments on the dependence of the shape from the nature of the mask were also made using a PECVD Si_3N_4 masking material, but no clear crystal habits were obtained also in this case. The absence of a crystallographic habit can thus be attributed to a higher reactivity of the material, owing to the presence of the aluminium. In any case, as shown in Fig. 4 uniform morphologies can be obtained with a quasi-rectangular shape in both crystallographic directions, resulting, for a second-order grating, in a good feedback coupling coefficient.

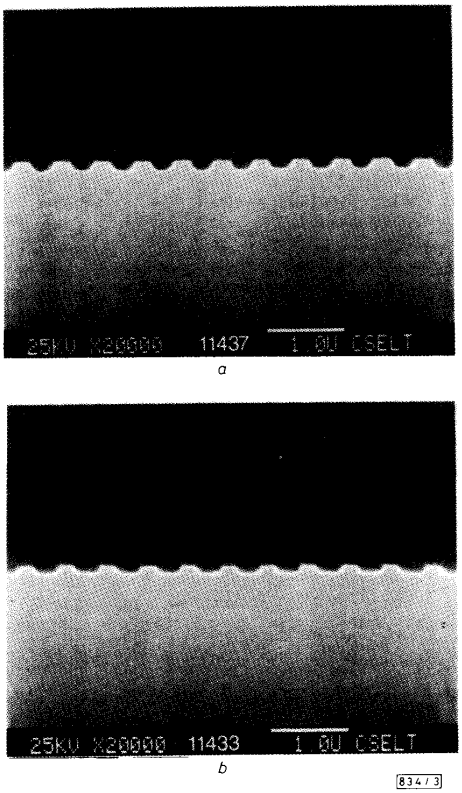

Fig. 3 *470 nm grating cross-section*
a [$1\bar{1}0$] direction *b* [110] direction

Conclusion: Uniform, large-area second-order gratings were realised in AlInAs MBE layers parallel to the [$1\bar{1}0$] and [110] directions, suitable for DFB laser devices, using a chemical etching based on saturated bromine water system. The solution SBW : H_2O : H_3PO_4 has been characterised for reproducible results, and is suitable also for first-order grating formation.

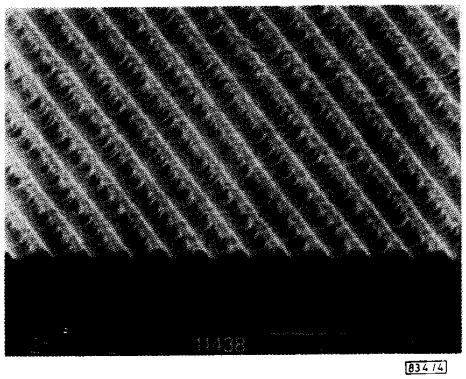

Fig. 4 *Tilted view of 470 nm grating along* [$1\bar{1}0$] *direction*

Acknowledgments: I wish to thank C. Rigo for the growth of the MBE materials and R. De Franceschi for SEM observations. This work was supported in part by the European Economic Community under Race 1057 Project.

G. MENEGHINI *10th April 1989*

CSELT—Centro Studi e Laboratori Telecomunicazioni SpA
Via G. Reiss Romoli 274
10148 Torino, Italy

References

1 TSANG, W. T.: '$Ga_{0.53}In_{0.47}As$/InP double-heterostructure and multiquantum well laser grown by chemical beam epitaxy', *IEEE J. Quantum Electron.*, 1987, **QE-23**, pp. 936–942
2 KAWAMURA, Y., NONAKA, K., and MIKAMI, O.: 'Low threshold current GaInAs/AlInAs ridge MQW laser with InP cladding layers', *Electron. Lett.*, 1988, **24**, pp. 637–638
3 SAITOH, T., MIKAMI, O., and NAKAGOME, H.: 'New chemical etching solution for InP and GaInAsP gratings', *Electron. Lett.*, 1982, **18**, pp. 408–409
4 GATOS, H. C., and LAVINE, M. C.: 'Etching and inhibition of the {111} surfaces of the III-V intermetallic compounds: InSb', *J. Phys. Chem. Solids*, 1960, **14**, pp. 169–174
5 STANO, A.: 'Chemical etching characteristics of InGaAs/InP and InAlAs/InP heterostructures', *J. Electrochem. Soc.*, 1987, **134**, pp. 448–452

IMPROVED RABIN'S SCHEME WITH HIGH EFFICIENCY

Indexing terms: Information theory, Public-key cryptosystems, Rabin's scheme, Quadratic residues

The letter proposes a modified public-key cryptosystem based on the Rabin scheme. It can provide simultaneously both private encryption and digital signatures for network users. In the cases where it provides only encryption or only digital signatures, the scheme provides that the bit ratio between plaintext and ciphertext is 1 : 1, i.e. equivalent to that of the RSA scheme.

The scheme here builds on the Rabin scheme[1] presented in 1979. That scheme includes both an encryption algorithm and a digital signature algorithm, both based on quadratic residue theory. It requires that redundant information be used in the encryption scheme, and that a non-deterministic technique be used to select an appropriate ciphertext, corresponding to a message, to be signed.

The goal of our scheme is twofold: (i) to eliminate the need for using redundant information in the encryption scheme, and to replace the non-deterministic method of selecting the ciphertext to sign by a deterministic one; and (ii) to make the bit ratio between the plaintext and the ciphertext 1 : 1 and so comparable to that in the RSA scheme.

We first make some comments about the notation we have used. We use the symbol QR_n to represent the set of all integers between 1 and $n-1$ inclusive that are quadratic residues modulo n, and the symbol QNR_n to represent those that are quadratic non-residues modulo n. We use the symbol $L(a/p)$ for the Legendre symbol, and the symbol $J(a/n)$ for the Jacobi symbol. For $n = p * q$, with p and q odd primes, $J(a/n) = L(a/p) * L(a/q)$. However, $J(a/n)$ can be evaluated without knowing the factors of n.[2]

Some necessary features of quadratic residue theory are the following:

(*a*) For $n = p * q$, with p and q odd primes and integer a relatively prime to n, $a \in QR_n$ iff $[(a \in QR_p)$ and $(a \in QR_q)]$.

(*b*) Given any message M relatively prime to n, and three fixed constants α, β and γ ($\alpha \in QR_p \cap QNR_q$, $\beta \in QNR_p \cap QR_q$ and $\gamma \in QNR_p \cap QNR_q$), M can be mapped to a quadratic residue modulo n as follows: $M \rightarrow M' = m * M$, where $m = 1, \alpha, \beta$ or γ according to whether $M \in QR_p \cap QR_q$, $M \in QR_p \cap QNR_q$, $M \in QNR_p \cap QR_q$ or $M \in QNR_p \cap QNR_q$, respectively.

(c) For p prime, congruent to 3 modulo 4, $a \in QR_p$ iff $(-a) \in QNR_p$.[3]

We now present our new theorem.

Theorem: For any integer $n = p * q$, with p and q primes congruent to 3 modulo 4, and any integer $a \in QR_n$, the four square roots (r) of a are distinguishable according to four exhaustive, nonoverlapping cases, in either of the following ways:

case 1a: $J(r/n) = 1$ and $1 < r < n/2$ — case 1b: $r \in QR_p \cap QR_q$

case 2a: $J(r/n) = 1$ and $n/2 < r < n$ — case 2b: $r \in QR_p \cap QNR_q$

case 3a: $J(r/n) = -1$ and $1 < r < n/2$ — case 3b: $r \in QNR_p \cap QR_q$

case 4a: $J(r/n) = -1$ and $n/2 < r < n$ — case 4b: $r \in QNR_p \cap QNR_q$

Proof: According to Knuth[4] the four square roots of a can be expressed as follows: x, $-x$, $(f * x) \bmod n$ and $-(f * x) \bmod n$, where $f = (p^{q-1} - q^{p-1}) \bmod n$. Without loss of generality, assume that $x \in QR_p \cap QR_q$ (i.e. case 1b). Then, by theorem 3, $(-x) \in QNR_p \cap QNR_q$ (case 4b). Since $J(x/n) = J(-x/n) = 1$, x and $(-x)$ fall into cases 1a and 2a. Since $L(f/p) = -1$ and $L(f/q) = 1$, $J(f/n) = -1$. Similarly, $L(-f/p) = -1$ and $L(-f/q) = 1$, so $J(-f/n) = -1$. Therefore $(f * x) \bmod n$ and $-(f * x) \bmod n$ belong to the two cases corresponding to sets $QR_p \cap QNR_q$ and $QNR_p \cap QR_q$ (i.e. cases 2b and 3b), as well as to cases 3a and 4a. (Note that the cases 1a–4a do not correspond, respectively, to the cases 1b–4b.)

Our algorithms follow. All use public keys $(n, \alpha, \beta, \gamma)$ and corresponding secret keys (p, q), where $\alpha \in QR_p \cap QNR_q$, $\beta \in QNR_p \cap QR_q$ and $\gamma \in QNR_p \cap QNR_q$.

Data encryption scheme:

Encryption: For any message m, where $0 < m < n_i$ and $\gcd(m, n_i) = 1$, to send it secretly to user i, the sender needs to access the public keys $(n_i, \alpha_i, \beta_i, \gamma_i)$ of the recipient user i. The encryption procedure can be classified into the following four different cases according to the properties of m:

1	case 1: if $J(m/n_i) = 1$ and $0 < m < n_i/2$
α_i	case 2: if $J(m/n_i) = 1$ and $n_i/2 < m < n_i$
$C = \{(m)^2 * \beta_i\} \bmod n_i$	case 3: if $J(m/n_i) = -1$ and $0 < m < n_i/2$
γ_i	case 4: if $J(m/n_i) = -1$ and $n_i/2 < m < n_i$

Recall that the Jacobian can be calculated without knowing the factorisation of n_i. The ciphertext C can then be sent to user i over a public channel.

Decryption: For every received ciphertext C, there are four possible solutions in modulo n_i. However, since user i knows the secret keys, p and q, he/she can remove the ambiguity. The reason is that $(m)^2 \bmod n_i$ is always a quadratic residue modulo n_i and according to the theorem the ciphertext generated from the four different possible cases during the encryption procedure can be distinguished, knowing p and q, as follows:

C comes from encryption case i:
- $i = 1$, if $C \in QR_p \cap QR_q$
- $i = 2$, if $C \in QR_p \cap QNR_q$
- $i = 3$, if $C \in QNR_p \cap QR_q$
- $i = 4$, if $C \in QNR_p \cap QNR_q$

Therefore, the legitimate receiver can first multiply C by the appropriate multiplicative inverse, modulo n_i, to obtain $(m)^2 \bmod n_i$, and then the one and only one plaintext which is the correct one of the four possible square roots can be uniquely specified by the following decryption procedure:

case 1: if $C \in QR_p \cap QR_q$		1	such that $J(m/n_i) = 1$, $0 < m < n_i/2$
case 2: if $C \in QR_p \cap QNR_q$	choose	α_i^{-1}	such that $J(m/n_i) = 1$, $n_i/2 < m < n_i$
case 3: if $C \in QNR_p \cap QR_q$	$m = \sqrt{\{C * \beta_i^{-1}\}}$		such that $J(m/n_i) = -1$, $0 < m < n_i/2$
case 4: if $C \in QNR_p \cap QNR_q$		γ_i^{-1}	such that $J(m/n_i) = -1$, $n_i/2 < m < n_i$

Digital signature scheme:

Digital signature: For any message m, where $0 < m < n_i$ and $\gcd(m, n_i) = 1$, user i wants to generate a unique signature S. First, owing to one possible attack suggested by Shamir,[5] the message m itself, before being signed, needs to be perturbed in a totally unpredictable way that affects most of the message bits. We define this bit-perturbing one-way function as P, and therefore $m' = P(m)$ and $m' \in [1, n_i - 1]$. Then user i needs to access his/her own secret keys, p_i and q_i, for calculating square roots, following four different procedures for selecting the signature S, depending on the nature of the value m', as follows:

case 1: if $m' \in QR_p \cap QR_q$		1	such that $J(S/n_i) = 1$, $0 < S < n_i/2$
case 2: if $m' \in QR_p \cap QNR_q$	choose	α_i	such that $J(S/n_i) = 1$, $n_i/2 < S < n_i$
case 3: if $m' \in QNR_p \cap QR_q$	$S = \sqrt{\{m' * \beta_i\}}$		such that $J(S/n_i) = -1$, $0 < S < n_i/2$
case 4: if $m' \in QNR_p \cap QNR_q$		γ_i	such that $J(S/n_i) = -1$, $n_i/2 < S < n_i$

Signature verification: To verify that the signature S is a valid signature for message m transmitted from user i, any receiver needs to access the public keys $(n_i, \alpha_i, \beta_i, \gamma_i)$ of user i. First, the receiver applies the publicly known perturbing function P to the message m to obtain $m' = P(m)$. Then, there are four different verification procedures as follows:

1	for case 1: if $J(S/n_i) = 1$, $0 < S < n_i/2$
α_i	for case 2: if $J(S/n_i) = 1$, $n_i/2 < S < n_i$
$(S)^2 \bmod n_i = m' * \beta_i$	for case 3: if $J(S/n_i) = -1$, $0 < S < n_i/2$
γ_i	for case 4: if $J(S/n_i) = -1$, $n_i/2 < S < n_i$

Data encryption and digital signature scheme:

Encryption and digital signature: Suppose user A wants to transmit the message m to user B. User A needs to ensure that $n_A > n_B > m$. This condition can be easily achieved using either the arrangement suggested by Rivest *et al.*[6] or that suggested by Kohnfelder.[7] Then, using the data encryption scheme, user A needs to generate the intermediate result C as follows:

$$C = \{(m)^2 * \beta_B\} \bmod n_B \quad \begin{cases} 1 & \text{for case 1: if } J(m/n_B) = 1,\ 0 < m < n_B/2 \\ \alpha_B & \text{for case 2: if } J(m/n_B) = 1,\ n_B/2 < m < n_B \\ \gamma_B & \text{for case 3: if } J(m/n_B) = -1,\ 0 < m < n_B/2 \\ & \text{for case 4: if } J(m/n_B) = -1,\ n_B/2 < m < n_B \end{cases}$$

Next, applying the perturbing function P to C to obtain $C' = P(C)$, user A then generates and selects the signature S for C', as

case 1: if $C' \in QR_{p_A} \cap QR_{q_A}$	1	such that $J(S/n_A) = 1,\ 0 < S < n_A/2$
case 2: if $C' \in QR_{p_A} \cap QNR_{q_A}$	choose α_A	such that $J(S/n_A) = 1,\ n_A/2 < S < n_A$
case 3: if $C' \in QNR_{p_A} \cap QR_{q_A}$	$S = \sqrt{\{C' * \beta_A\}}$	such that $J(S/n_A) = -1,\ 0 < S < n_A/2$
case 4: if $C' \in QNR_{p_A} \cap QNR_{q_A}$	γ_A	such that $J(S/n_A) = -1,\ n_A/2 < S < n_A$

Since the ciphertext C contains the receiver's public key n_B and the signature S contains the transmitter's secret keys p_A and q_A, data security and the digital signature can be achieved by transmitting (C, S). The bit ratio between the plaintext and the ciphertext is 1 : 2.

Decryption and signature verification: The decryption procedure for ciphertext (C, S) is straightforward.

L. HARN
T. KIESLER

Computer Science & Telecommunications Program
University of Missouri—Kansas City
Kansas City, MO 64110-2499, USA

23rd March 1989

References

1 RABIN, M. O.: 'Digitalized signatures and public key functions as intractable as factorization'. MIT/LCS/TR-212, Jan. 1979
2 DENNING, D. E. R.: 'Cryptography and data security' (Addison-Wesley, Reading, MA, 1982), p. 106
3 SHOCKLEY, J. E.: 'Introduction to number theory' (Holt, Rinehart & Winston, Chicago, 1967), p. 139
4 KNUTH, D. E.: 'The art of computer programming, vol. 2: seminumerical algorithms' (Addison-Wesley, Reading, MA, 1969), p. 389
5 SHAMIR, A., and SCHNORR, C. P.: 'Cryptanalysis of certain variants of Rabin's signature scheme', *Inf. Process. Lett.*, Oct. 1984, pp. 113–115
6 RIVEST, R. L., SHAMIR, A., and ADELMAN, L.: 'A method for obtaining digital signatures and public-key cryptosystem', *Commun. ACM*, Feb. 1978, **21**, pp. 120–126
7 KOHNFELDER, L. M.: 'On the signature reblocking problems', *in* 'Complexity of computer computations' (Plenum Press, NY, 1978), pp. 85–104

ELECTRON WAVE INTERFERENCE DEVICE WITH VERTICAL SUPERLATTICES WORKING IN LARGE CURRENT REGION

Indexing terms: Semiconductor devices and materials, FETs, GaAs, Electron devices, Quantum interference, Vertical superlattices

An electron wave interference device (wash board transistor), consisting of a modulation-doped $Al_{0.3}Ga_{0.7}As$/GaAs heterostructure and a 16 nm $(AlAs)_{0.25}(GaAs)_{0.75}$ vertical superlattice is fabricated. This transistor shows drain current oscillation due to electron wave interference at 4·2 K at large biasing currents. The $(AlAs)_{0.25}(GaAs)_{0.75}$ vertical superlattice improves the biasing current by about 10^5 times compared to the previous wash board transistor with a 500 nm tungsten grating gate.

High-speed field-effect transistors (FETs) are very promising three-terminal devices for ultra-high-speed digital and monolithic millimetre-wave integrated circuits. A high electron mobility transistor (HEMT)[1] has been studied to fulfil this role.

As the performance of these devices is restricted by electron drift velocity, a new concept of device action is needed to fabricate higher-speed, low power dissipation and new functional FETs. Thus the electron wave interference effect,[2–6] the velocity modulation effect[7,8] and the high mobility effect of one-dimensional electrons[9] have been proposed and/or observed as the basis of electron transport.

Electron wave interference between incident electron waves and their waves reflected by a periodic potential in an electron wave interference device, called a wash board transistor (WBT), has been observed by measuring the drain current I_d oscillation.[4,5] The maximum currents, however, during the I_d oscillations are still small (pA ~ nA) owing to the long periodicity of the periodic potential, e.g. 200–500 nm.

This letter reports the production of a WBT, made from III-V semiconductor ultrafine structure materials (vertical superlattices) with 5–16 nm size. A vertical superlattice, called a fractional-layer superlattice (FLS),[10] has a small periodicity perpendicular to the growth direction. This periodicity of the FLS gives this new WBT drain current oscillation at large biasing currents.

A cross-sectional view of the WBT is shown in Fig. 1. The modulation-doped AlGaAs/GaAs heterojunction structure with FLSs was grown by low-pressure metalorganic chemical vapour deposition on (001) vicinal oriented, Cr-doped semi-insulating GaAs substrate.[10] A (001) GaAs substrate with misorientation angle of 1·0° towards the [1$\bar{1}$0] direction was used

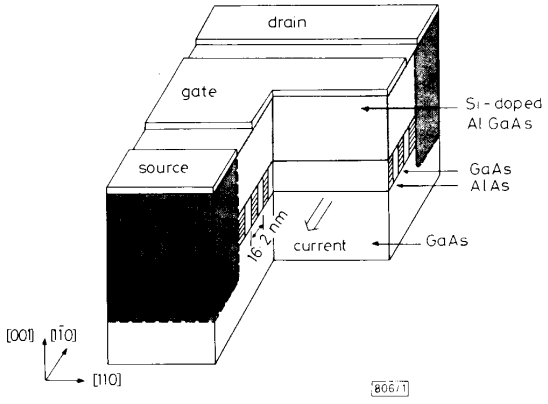

Fig. 1 *Cross-sectional view of electron wave interference transistor (wash board transistor, WBT)*