Defect-free (denuded) zones are formed at the top layers.[5,6] The removal of impurities and defects from the surface region results in an increase of surface Hall mobility. So, the mobility in the two samples increases a lot after proton implantation and annealing. Comparing Figs. 1 and 2, we observe that the maximum resistivity value of the polycrystalline layer in the annealed sample B is nearly one order of magnitude higher than that in the annealed sample A. To explain the results, we suggest a model in which substitutional phosphorus atoms in grains are gettered by grain boundaries. Furthermore, we assume that phosphorus atoms in grain boundaries do not act as electrically active atoms. During growth of CZ silicon, phosphorus was doped into silicon to control the resistivity of silicon. Substitutional phosphorus atoms act as electrically active atoms. A few substitutional phosphorus atoms in the grains were gettered by grain boundaries during annealing which was at 1000°C for 15 h. Therefore, the number of the electrically active phosphorus atoms within the polycrystalline layer decreased a little and an increase of resistivity occurred in the polycrystalline layer. As a result, the annealing at 1000°C for a long period is effective for increasing resistivity in the polycrystalline layer and a good SOPL substrate is formed by using three-step annealing.

In this study, high-resistivity polycrystalline layers were buried beneath the surface top layers and the surface Hall mobility increased by about 25% compared with the original mobility. The high-resistivity layer beneath the top layer results in low parasitic capacitance of devices fabricated on the layer of the top silicon single crystal.[1] Parasitic capacitance and carrier mobility are the two most important material properties which affect the speed of ICs. The two material properties have been improved by using SOPL substrate. The low parasitic capacitance and the high electron mobility of GaAs result in substantially higher operating speed for GaAs ICs. But silicon and GaAs are getting close together in terms of the two properties owing to the SOPL technique. Silicon is cheap and will most likely remain as the sole material for VLSI. SOPL substrate will be a new material for the manufacture of high-speed integrated circuits.

Acknowledgment: I am grateful to C. Hai, W. Wang, J. Zhu, D. Li, L. Yang and L. Tian for their assistance.

JIANMING LI

5th September 1989

Department of Public Technology
Institute of Semiconductors
Chinese Academy of Sciences
Beijing, People's Republic of China

References

1 LIAW, H. M.: 'Trends in semiconductor material technologies for VLSI and VHSIC applications', *Solid-State Technol.*, 1982, **25**, pp. 65–73
2 PINIZZOTTO, R. F.: 'Silicon on insulator by ion implantation'. Proc. Mater. Res. Soc., 1984, **27**, pp. 265–269
3 LI, J.: *Chinese Phys. Lett.* (English edition), to be published October 1989
4 LI, J.: 'Stable defects in silicon implanted with hydrogen ions', *Chinese J. Semicond.* (English edition), 1988, **9**, pp. 459–462
5 GEIPEL, H. J., and TICE, W. K.: 'Reduction of leakage by implantation gettering in VLSI circuit', *IBM J. Res. Dev.*, 1980, **24**, pp. 310–317
6 JASTRZEBSKI, L.: 'Origin and control of material defects in silicon VLSI technologies', *IEEE J. Solid-State Circuits*, 1982, **SC-17**, pp. 105–117

2-BIT, CHAINED, PROBABILISTIC ENCRYPTION SCHEME

Indexing terms: Information theory, Codes, Encoding, Algorithms

In this letter we present a new probabilistic encryption algorithm based on the scheme proposed by Jingmin and Kaicheng in 1988. This algorithm utilises the public key concept and recursively encrypts two bits at a time. The message bit expansion is very low and is the same as in their scheme. At the same time, this new scheme is twice as fast.

Introduction: Diffie and Hellman introduced the concept of public key cryptographic systems in their classic paper of 1976.[1] Schemes to implement it quickly followed: the RSA scheme of Rivest, Shamir and Adelman in 1978,[2] the knapsack trapdoor scheme of Merkle and Hellman in 1978[3] and the Rabin scheme in 1979.[4]

In 1982, Goldwasser and Micali[5] pointed out some basic problems with all the schemes thus far presented, and proposed a new approach called probabilistic encryption as an alternative approach which assures what they termed polynomial security. Probabilistic encryption algorithms provide that corresponding to every message are many possible encrypted forms, not just one.

The first probabilistic encryption algorithm proposed by Goldwasser and Micali[5,6] was impractical, in that it required the encryption of every bit of message independently, thus utilising a message bit expansion of $1:K$, where K is called the security parameter and constitutes the length of ciphertext used to represent the single bit being transmitted. Blum and Goldwasser[7] proposed a more efficient probabilistic encryption scheme in which every message bit sequence was exclusive-ORed with the output bit sequence of a pseudorandom number generator. More recently Jingmin and Kaicheng[8] proposed an elegant way to chain into a single cipher text a sequence of encryptions of the individual message bits of a long message string of L bits, with a low message bit expansion of $[L + (K - 1)]/L$, where K is the security parameter (length of cipher text).

In this letter we develop a public-key probabilistic encryption algorithm which is very similar to that of Jingmin and Kaicheng.[8] However, this new algorithm chains the cipher texts obtained by recursively encrypting two message bits at a time, with message bit expansion the same as theirs, while providing encryption and decryption operations that are twice as fast.

Quadratic residue theory: In what follows, we use the symbol QR_n to represent the set of all integers between 1 and $n-1$ that are quadratic residues modulo n, and the symbol QNR_n to represent those that are quadratic nonresidues modulo n. Also, for $n = p_1 p_2$, we use the symbol $QR^*_{p_i}$, for $1 \le i \le 2$, for the set $\{a \mid 1 \le a \le n-1,\ a \text{ is a quadratic residue modulo } p_i\}$, and similarly the symbol $QNR^*_{p_i}$. We use the symbol $L(a/p)$ for the Legendre symbol, where p is an odd prime, and $J(a/n)$ for the Jacobi symbol, where n is a product of two large primes.

We utilise the following theorem, proved in Reference 10.

Theorem: For any integer $n = p_1 p_2$, with p_1 and p_2 primes of the form $4n + 3$, and an integer $a \in QR_n$, the four square roots of a are distinguishable among four different cases as specified in any of the following ways:

case (*a*): root $\in QR^*_{p_1} \cap QR^*_{p_2}$
case (*b*): root $\in QR^*_{p_1} \cap QNR^*_{p_2}$
case (*c*): root $\in QNR^*_{p_1} \cap QR^*_{p_2}$
case (*d*): root $\in QNR^*_{p_1} \cap QNR^*_{p_2}$

or

case (*a*): $J(\text{root}/n) = 1$ and $0 < \text{root} < n/2$
case (*b*): $J(\text{root}/n) = 1$ and $n/2 < \text{root} < n$
case (*c*): $J(\text{root}/n) = -1$ and $0 < \text{root} < n/2$
case (*d*): $J(\text{root}/n) = -1$ and $n/2 < \text{root} < n$

or

case (*a*): $J(\text{root}/n) = 1$ and root is even
case (*b*): $J(\text{root}/n) = 1$ and root is odd
case (*c*): $J(\text{root}/n) = -1$ and root is even
case (*d*): $J(\text{root}/n) = -1$ and root is odd

2-bit, chained, probabilistic encryption algorithm:

Secret key: Every user i needs to select two large distinct primes p_{i_1} and p_{i_2}, with p_{i_1} and p_{i_2} of the form $4n + 3$, and calculate their product $n_i = p_{i_1} p_{i_2}$; (p_{i_1}, p_{i_2}) becomes user i's secret key.

Public key: Every user i will select one parameter y_i from the region $[1, n_i - 1]$ and $y_i \in QNR^*_{p_{i(1)}} \cap QNR^*_{p_{i(2)}}$. User i's public key is then (n_i, y_i).

Probabilistic encryption: Any user who wants to send binary message string $m = m_1 m_2, \ldots, m_{2t}$ to user i secretly, needs to access user i's public key (n_i, y_i) and randomly select a binary string x within the region $[1, n_i - 1]$ such that $(x, n_i) = 1$:

Set $C_0 = x$
For $j = 1$ to t do
  $C'_j = C^2_{j-1} \bmod n_i \quad$ if $m_{2j-1} = 0$
     $C^2_{j-1}\, y_i \bmod n_i \quad$ if $m_{2j-1} = 1$
  $C_j = C'_j \quad$ if $\{m_{2j} = 0$ and $0 < C'_j < n_i/2\}$
     or $\{m_{2j} = 1$ and $n_i/2 < C'_j < n_i\}$
  $n_i - C'_j \quad$ if $\{m_{2j} = 0$ and $n_i/2 < C'_j < n_i\}$
     or $\{m_{2j} = 1$ and $0 < C'_j < n_i/2\}$
  If $C_j = C'_j$, set $b_j = 0$; otherwise set $b_j = 1$
  If C_j is even, set $d_j = 0$; otherwise set $d_j = 1$
End
Calculate $S_t = C_t^2 \bmod n_i$
Transmit $(S_t, b_1, b_2, \ldots, b_t, d_1, d_2, \ldots, d_t)$ to user i.

Probabilistic decryption: Once user i receives the cipher text, he/she will start to decipher the message m in backward fashion (recursively):

Calculate C_t from S_t using d_t
For $j = t$ to 1 by -1 do
  calculate $C'_j \quad = C_j \quad$ if $b_j = 0$
     $n_i - C_j \quad$ if $b_j = 1$
  calculate $m_{2j} \quad = 0 \quad$ if $0 < C_j < n_i/2$
     $1 \quad$ otherwise
  calculate $m_{2j} - 1 = 0 \quad$ if $L(C'_j/p_{i_1}) = L(C'_j/p_{i_2}) = 1$
     $1 \quad$ if $L(C'_j/p_{i_1}) = L(C'_j/p_{i_2}) = -1$
  If $j > 1$ then calculate the unique quadratic root C_{j-1} of C'_j as follows, using d_j to determine the specified root:
   C_{j-1} = specified root of $C'_j \quad$ if $m_{2j-1} = 0$
     $y_i^{-1} C'_j \quad$ if $m_{2j-1} = 1$
End

Since the parameters 1 and y_i have the property that $J(1/n_i) = 1$ and $J(y_i/n_i) = 1$, then for $1 \le j \le t$ all values C'_j have the property that $J(C'_j/n_i) = 1$; and since further $p_{i_1} \equiv p_{i_2} \equiv 3 \bmod 4$, it follows that $J(C_j/n_i) = 1$.

Security discussion: The secrecy of this algorithm is based on the difficulty of finding square roots of a quadratic residue modulo an integer which is a product of two large primes. Rabin[4] proved that finding such square roots is as difficult as factoring an integer that is a product of two large primes, which latter problem is believed to be computationally infeasible. Although for each two bits (m_{2j-1}, m_{2j}) of a message, we transmit in plain text a bit pair (b_j, d_j), where b_j specifies whether a subtraction operation was applied to C'_j and d_j specifies uniquely C_j as square root of C_{j+1}, knowledge of (b_j, d_j) by an outsider does not reveal any information about the encrypted message bits (m_{2j-1}, m_{2j}). This is due to the fact that each square root has probability 1/2 of being in either the first half or second half of the region $(0, n_i)$, or of being an even number or an odd number. Further, these two Boolean properties are uncorrelated. It also needs to be pointed out that, given cipher text C_t, any user could check the region of C_t without knowing p_{i_1} and p_{i_2} and determine the last bit m_{2t}. It is for this reason that we transmit S_t instead.

We need to point out here that even should a sender encrypt the same message string m repeatedly, since the sender randomly selects x as the starting binary string each time the message is sent, then the corresponding cipher text will be different each time. The bit expansion is $(K + L)/L$, where K is the security parameter and L is the length of the message.

The difference between our scheme and that of Jingmin and Kaiching[8] is that we do not need to require that each C_j lie in the interval $(0, n_i/2)$. Being able to use the entire interval, we can encrypt two bits in the same time that it takes them to encrypt one bit. Thus, for the same message string, our encryption and decryption schemes are twice as fast as theirs.

L. HARN
T. KIESLER

Computer Science Telecommunications Program
University of Missouri
Kansas City, MO 64110, USA

7th August 1989

References

1 DIFFIE, W., and HELLMAN, M. E.: 'New directions in cryptography', *IEEE Inform. Theory*, 1976, **IT-22**, pp. 644–654
2 RIVEST, R. L., SHAMIR, A., and ADELMAN, L.: 'A method for obtaining digital signatures and public-key cryptosystem', *Commun. ACM*, 1978, **21**, (2), pp. 120–126
3 MERKLE, R. C., and HELLMAN, M. E.: 'Hiding information and signatures in trapdoor knapsack', *IEEE Trans. Inform. Theory*, 1978, **IT-24**, (9), pp. 525–530
4 RABIN, M. O.: 'Digitalized signatures and public key functions as intractable as factorization'. MIT/LCS/TR-212, January 1979
5 GOLDWASSER, S., and MICALI, S.: 'Probabilistic encryption & how to play mental poker keeping secret all partial information'. Proceedings of 14th STOC Conference, San Francisco, 1982
6 GOLDWASSER, S., and MICALI, S.: 'Probabilistic encryption', *J. Comput. Syst. Sci.*, 1984, **28**, pp. 270–299
7 BLUM, M., and GOLDWASSER, S.: 'An efficient probabilistic public-key encryption scheme which hides all partial information', *in* 'Advances in Crytology—Crypto '84', 1984, pp. 289–299
8 JINGMIN, H., and KAICHENG, L.: 'A new probabilistic encryption scheme', *in* 'Advances in Cryptology—Eurocrypt '88', 1988, pp. 415–418
9 DENNING, D. E. R.: 'Cryptography and data security' (Addison-Wesley, 1982)
10 HARN, L., and KIESLER, T.: 'Improved Rabin's scheme with high efficiency', *Electron. Lett.*, 1989, **25**, pp. 726–728

PLASMA-HYDROGENATED LOW-THRESHOLD WIDE-BAND 1·3μm BURIED RIDGE STRUCTURE LASER

Indexing terms: Semiconductor lasers, Plasmas, Semiconductor growth

The plasma hydrogenation of *p*-type InP has been applied to the fabrication of buried ridge structure (BRS) lasers. The threshold current, output power and modulation bandwidth of the obtained devices compare favourably with those of more conventional ones fabricated by proton implantation on the same wafer.

Introduction: The use of plasma hydrogenation for decreasing the conductivity of *p*-type InP by several orders of magnitude has been the object of recent reports.[1,2] The physical phenomenon involved is the neutralisation of electrically active acceptors by the in-diffused hydrogen species, with the formation of hydrogen acceptor pairs. An obvious application of this effect is the realisation of electrical isolation in InP-based devices. The BRS laser[3,4] technology makes use of proton implantation to enhance the output efficiency by reducing the current leaks across the InP/InP homojunction. Although proton implantation provides adequate electrical insulation, it is also likely to introduce defects which can act as non-radiative centres. In this letter we report for the first time the realisation and preliminary characterisation of high-performance lasers by plasma hydrogenation instead of proton implantation.

Experimental: Fig. 1 shows the main fabrication steps of the plasma hydrogenated 1·3 μm wavelength BRS laser. This