This typical example shows that the analysis method is very efficient and considerably simpler than other known methods. Although it is presently restricted to stray-insensitive SC networks, it can easily be extended, as will be described in a forthcoming comprehensive publication. There it will be shown that this method can readily be used for general SC networks, including those with unity-gain buffer amplifiers.

A. DąBROWSKI
Institute of Electronics & Telecommunication
Technical University of Poznań
ul. Piotrowo 3a, PL-60 965 Poznań, Poland

G. S. MOSCHYTZ
Institute of Signal & Information Processing
Swiss Federal Institute of Technology
ETH Centre, CH-8092 Zurich, Switzerland

References

PUBLIC-KEY ENCRYPTION ALGORITHM INCORPORATING ERROR DETECTION

Indexing terms: Information theory, Codes and coding, Public-key cryptography, Error-detecting codes, Quadratic residue, Authentication

Owing to their mathematical properties, quadratic residues have been used successfully in designing a number of cryptographic applications, such as oblivious transfer protocol and coin flipping protocol. In the letter we propose an encryption scheme based on quadratic residue theory. In particular, we incorporate the encrypting procedure and error-detecting code into a complete communication system.

Introduction: In 1976, Diffie and Hellman introduced the concept of public-key cryptography, which provides a proper solution to the problem of key distribution. Since then many implementations of public-key cryptography have been proposed. For example, the Rivest-Shamir-Adelman (RSA) scheme depends on the difficulty of factoring large integers, and Elgamal's scheme depends on the difficulty of computing discrete logarithms.

In this letter we propose a public-key encryption/decryption scheme that incorporates into it an error-detecting code. The public/private keys are based on quadratic residue theory. The oblivious transfer protocol proposed by Blum is one application based on the same theory. The security of our system is based on the difficulty of factoring large integers, as in the RSA scheme.

Diffie and Hellman observed that if an error is propagated by an encryption/decryption algorithm, then applying error-detecting codes before encryption and after decryption (as shown in Fig. 1) provides a way to achieve message authenticity (to the extent of detecting active tampering). The reason for this is that any altering of the ciphertext will be detected by the error-detecting device.

![Fig. 1](image)

Since we use the block cipher for encryption, the error does propagate. One special feature of our proposed encryption scheme is that we incorporate error detection within our decryption technique. The result is that our scheme provides not only data secrecy but also, as a bonus, error detection and message authenticity.

Quadratic residues: We now summarise those facts about quadratic residue theory (cf. Denning's summary (Reference 6, pp. 111-117)) needed to understand our encryption algorithm presented later. Those facts are as follows:

1. **Definition:** A number $a$ is a quadratic residue modulo $n$ iff $a$ and $n$ are relatively prime (gcd $(a, n) = 1$), and the equation $x^2 \equiv a \pmod{n}$ has a solution.

2. **Notation:** We define $QR_n$ to be the set of all integers between 1 and $n - 1$ that are quadratic residues modulo $n$, and $NQR_n$, those that are not, called quadratic nonresidues.

3. Since $(n - a)\equiv (a - 1)\equiv (n - 1)/2 \pmod{n}$, $QR_n$ can be found by evaluating $x^2 \pmod{n}$ for only $x = 1, 2, \ldots, (n - 1)/2$. If $n$ is a prime, these $(n - 1)/2$ values will all be distinct. If $n > 2$ and prime, then $QR_n$ contains exactly half of these $n - 1$ elements.

4. For prime $n = p > 2$, and $0 < a < p$, $a^{(p-1)/2} \equiv 1 \pmod{p}$, depending on whether $a \in QR_p$ or $a \in NQR_p$, respectively.

5. If $n = p^s q$, where $p$ and $q$ are large primes, then $a \in QR_n$ iff $(a \in QR_p)$ and $(a \in QR_q)$. If $a \in QR_n$, then $a$ has exactly 2 or 4 square roots. Since square roots come in additive inverse pairs, half of these roots are even and half odd. We call the even root(s) the primary square root(s) of $a$.

6. In this letter we make the further assumption that, for $n = p^s q$, $p$ and $q$ are large primes such that $(p + 1)$ and $(q + 1)$ are each evenly divisible by 4. This assumption considerably simplifies the calculations required for finding square roots (see Reference 6, p. 116).

The reason why quadratic residues, and primary square roots of quadratic residues, play a significant role in our secrecy scheme is threefold:

(i) Quadratic residues modulo $n$ within the integer interval $[1, n - 1]$ fall randomly in that interval.

(ii) Primary square roots of a quadratic residue modulo $n$ are independent of each other.

(iii) Given a quadratic residue $a$ modulo $n$, where $n = p^s q$, with $p$ and $q$ large prime numbers, it is computationally infeasible to calculate the square roots of $a$ without knowing $p$ and $q$.

Encryption scheme: The following cryptosystem, based on the theory of quadratic residues, provides secrecy as well as authentication of the message itself (freedom from active tampering). It also incorporates error detection within the decryption algorithm.

Each user $U$ of the system selects two very large (of the order of 350 bits in length) prime numbers $p_U$ and $q_U$, with the
added property that $p_n + 1$ and $q_n + 1$ are each divisible by 4, and then calculates $n_p = p_n * q_n$. The user then makes $n_p$ public while keeping $p_n$ and $q_n$ secret.

Any message $M$ to be sent is divided into a sequence of block messages of uniform length $L$, $(M_1, M_2, \ldots, M_L)$, each of which can be considered as a large integer in binary form. Individual blocks are then encrypted. We henceforth refer to individual message blocks as $M$.

We need a method for encrypting these individual message blocks $M$. Two earlier papers in particular 5,8 directed our thinking about this problem. In Reference 5 Diffie and Hellman recommended that error-detection encoding and decoding precede and follow, respectively, the encipherment and decipherment of a message, as shown in Fig. 1 (see Reference 6, p. 137).

Our method instead incorporates the encoding and decoding into a system, and in particular requires the use of error-detection decoding in the actual decipherment of the message.

In Reference 8 Koyama presented a method for encrypting messages, which preserves secrecy of the message and requires that the receiver use the quadratic formula to find the roots of a quadratic equation. He appended redundant information to the message, so that this redundant information can be used to select the one of the four solutions to the quadratic equation which includes the plaintext. Instead of using redundant information, we use parity bits already necessary for error-detection encoding and decoding to one special parity bit of our own, to enable us to select the one square root of the ciphertext that contains the plaintext.

The algorithm for deciphering a block of plaintext $M$ is as follows:

1. Find the public value $n_p$ of the receiver $B$, to whom the message is to be sent.

2. Break the message into a sequence of blocks, all of the same length $L$, such that the corresponding parity bit string required for a block of length $L$, being of length 1 to produce an $(L + r, L)$ linear block code for error-detection purposes) is such that $(L + (r + 1)) \leq \log_2 (L) + 1$.

3. For each message block $(M, (a))$ append $M$ to a string of $P$ parity bits and the single bit $0$, as follows to produce $M' = P \oplus 0$ (we use the symbol $\oplus$ for concatenation of strings). $M'$, considered as an integer, is less than $n_p$, because of the restriction imposed in (2) above on $L$; (b) calculate the corresponding ciphertext $C$ as $C = (M')^2 \mod n_p$, and transmit $C$ to user $B$.

Note that, for this scheme, user $A$ needs basically perform only one simple operation other than those already required for communication protocol, including error detection.

User $B$ then deciphers a message block $M$ from a ciphertext $C$, as follows:

1. Find the four (or two) square roots of $C$.

2. Eliminate the odd square roots (root), thus obtaining the primary root(s) $s_1$ and $s_2$.

3. If necessary, select $M'$ from the remaining two primary roots.

4. Remove $0'$ and $P$ from $M'$ to obtain the message block $M$.

Steps (2) and (4) are automatic. Steps (1) and (3) require calculations, which will now be described. Step (3) uses decoding, which would be required in any case. Hence, step (1) is where the computational load is equally divided between the sender and receiver. In our scheme, the sender has a very light load, while the receiver bears a heavy computational load.

Conclusions: In this letter we have presented a new cryptographic scheme. This encryption scheme assures secrecy of a message and message authenticity, while incorporating coding into a single communication system. This scheme is based on the exponential time complexity of factoring a large integer into two large, prime factors, and on quadratic residue theory in number theory. The overall complexity is equivalent to the familiar Rivest-Shamir-Adelman (RSA) scheme. In the RSA scheme, the computational load is equally divided between the sender and receiver. In our scheme, the sender has a very light load, while the receiver bears a heavy computational load.

L. HARN

T. KIESLERS

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

References


3. **ELGAMAL, T.:** 'A public key cryptosystem and a signature scheme based on discrete logarithms', IEEE Trans., 1985, IT-31, pp. 469-472

4. **BLUM, M.:** 'Three applications of the oblivious transfer: 1. Coin flipping by telephone. 2. How to exchange secrets. 3. How to send certified mail'. Dept. EECS, Univ. of California, Berkeley, CA, 1981

5. **DIFFIE, W., AND HELLMAN, M. E.:** 'Privacy and authentication: an introduction to cryptography', Proc. IEEE, 1979, 67, pp. 397-427


