Note that the second rule cannot be translated into a single FIP, for it uses the 'or' operator. Replacing 'and' by 'or' and 'or' by 'and' we obtain a flat dilation. Using weighted rules, more elaborate operators can be built. The output image of the program below is depicted in Fig. 4 and the processing time was 14s:

```
var d: real;
d := abs(x[1]-x[2])+abs(x[1]-x[3])+abs(x[1]-x[4]);
if d is black then y is +1.14 weight 1;
if d is white then y is -0.14 weight 5.1;
```

Conclusion: In this Letter, a new technique to construct grey-scale morphological operators using fuzzy expert systems was presented. A new representation scheme for morphological operators was introduced. Some application examples were presented.

© IEE 1997

Electronics Letters Online No: 19971268

4 July 1997

H.Y. Kim and F.A.M. Cipparrone (Lab. Proc. Sinais e Sistemas, Dept. Eng. Eletrônica, Escola Politécnica, Univ. São Paulo, Av. Prof. Luciano Gualberto, tr. 3, 158, CEP 05508-900, São Paulo, SP, Brazil)

M.T.C. Andrade (Dept. Eng. Comp. e Sist. Digitais, Escola Politécnica, Univ. São Paulo, Av. Prof. Luciano Gualberto, tr. 3, 158, CEP 05508-900, São Paulo, SP, Brazil)

E-mail: hae@lps.usp.br

References

- 1 SINHA, D., and DOUGHERTY, E.R.: 'Fuzzy mathematical morphology', *J. Vis. Commun. Image Represent.*, 1992, 3, (3), pp. 286-302
- 2 SINHA, D., and DOUGHERTY, E.R.: 'A general axiomatic theory of intrinsically fuzzy mathematical morphologies', *IEEE Trans. Fuzzy Systems*, 1995, 3, (4), pp. 389-403
- 3 MATHERON, G.: 'Random sets and integral geometry' (Wiley, New York, 1975)
- 4 KIM, H.Y.: 'Quick construction of efficient morphological operators by computational learning', *Electron. Lett.*, 1997, 33, (4), pp. 286-287
- 5 ZADEH, A.L.: 'Outline of a new approach to the analysis of complex systems and decision processes', *IEEE Trans. Syst. Man. Cybern.*, 1973, SMC-3, (1), pp. 28-44

Improvement to Nyang-Song fast digital signature scheme

Wei-Hua He and Tzong-Chen Wu

Indexing terms: Cryptography, Security of data

The authors present an improvement to the Nyang-Song scheme which achieves the same security level without increasing the cost of signature generation, and which offers two significant advantages.

Introduction: In 1979, Rabin [1] proposed a digital signature whose security is based on the difficulty of finding square roots modulo a composite number. Rabin's scheme provides a fast signature verification, which only requires one calculation of the adopted one-way hash function, one multiplication and one addition modulo a composite number n , where n is the product of two large primes. Note that in Rabin's scheme, the signer cannot generate the valid signatures for some messages if their corresponding signature equations are not solvable. Whenever the signature equation is solvable, it has four solutions (square roots) in which the signer can choose one of them as the signature of the message. Since then, several signature schemes derived from Rabin's scheme have been proposed in the literature [2-8]. However, they require a large public key [2-4, 7], and need iterative checks to verify a signature [7, 8].

Recently, Nyang and Song [9] proposed a fast digital signature scheme derived from Rabin's scheme. The Nyang-Song scheme has the following characteristics: (i) all signature equations are

solvable; (ii) it requires no more iterative checks for signature verification. Moreover, in the Nyang-Song scheme, each of the public key and the secret key is shortened to $2|n|$ bits, and it requires one calculation of the adopted one-way hash function and four modular multiplications (in Z_n) for signature verification.

In this Letter, we propose an improvement to the Nyang-Song fast digital signature. The improvement achieves the same security level as the original Nyang-Song scheme, without increasing the cost of signature generation. The improvement preserves the characteristics inherent in the Nyang-Song scheme. In addition, it has two significant advantages: (i) it is faster for signature verification than the Nyang-Song scheme, since two modular multiplications are eliminated; (ii) each of the public key and the secret key for each user is shortened to $|n|$ bits, while the Nyang-Song scheme needs $2|n|$ bits. However, the size of a digital signature generated by the improvement is one bit longer than the original one.

Review of Nyang-Song scheme: Denote by QR_p the set which contains all quadratic residues modulo p , and NQR_p the set which contains all quadratic nonresidues modulo p . The Legendre symbol $L(a, p)$, for $a \in Z_p$, is defined as

$$L(a, p) = \begin{cases} 0 & \text{if } a \text{ divides } p \\ 1 & \text{if } a \in QR_p \\ -1 & \text{if } a \in NQR_p \end{cases}$$

Theorem 1 [10]: Let p be an odd prime with $p \equiv 3 \pmod{4}$. Then $a \in QR_p$ if only if $-a \in NQR_p$.

Theorem 2 [10]: Let p be an odd prime.

- (i) If $a, b \in QR_p$ or $a, b \in NQR_p$, then $a \cdot b \in QR_p$.
- (ii) If $a \in QR_p$ and $b \in NQR_p$, or $a \in NQR_p$ and $b \in QR_p$, then $a \cdot b \in NQR_p$.

Theorem 3 [10]: Let p and q be distinct primes, and $n = p \cdot q$. If $a \in QR_p$ and $a \in QR_q$, then $a \in QR_n$.

The Nyang-Song scheme works as follows.

System initialisation: Initially, each user selects two large primes p and q that satisfy $p \equiv 3 \pmod{4}$ and $q \equiv 3 \pmod{4}$, and computes $n = p \cdot q$. Next, the user selects a random integer $b \in (0, n)$ and computes $B = b^4 \pmod{n}$. After that, the user publishes (n, B) as his public key and keeps (b, p, q) as his secret key.

Signature generation: Suppose user U_a wants to sign a message m for the verifier U_b . First, U_a uses a predefined one-way hash function f to compress m into $m' = f(m)$. Then, U_a generates the signature (s, t) for m according to the following four cases:

- Case 1: If $L(m'/p) = L(m'/q) = 1$, then let $t = 0$ and compute s satisfying $s \equiv \sqrt{m'} \pmod{n}$.
- Case 2: If $L(m'/p) = 1$ and $L(m'/q) = -1$, then let $t = 1$ and compute $s = b \cdot x \pmod{n}$, where x satisfies $x \equiv \sqrt{m'} \pmod{p}$ and $x \equiv \sqrt{-m'} \pmod{q}$.
- Case 3: If $L(m'/p) = -1$ and $L(m'/q) = 1$, then let $t = 1$ and compute $s = b \cdot x \pmod{n}$, where x satisfies $x \equiv \sqrt{-m'} \pmod{p}$ and $x \equiv \sqrt{m'} \pmod{q}$.
- Case 4: If $L(m'/p) = L(m'/q) = -1$, then let $t = 0$ and compute s satisfying $s \equiv \sqrt{-m'} \pmod{n}$.

Signature verification: The verifier U_b verifies the signature (s, t) of m with respect to U_a by checking the following congruent equality:

$$s^4 \equiv B^t \cdot (m')^2 \pmod{n}$$

where $m' = f(m)$. If the equality holds, then (s, t) is an authentic signature.

Note that like the Harn-Kiesler scheme [7], the compressed message m' shall be restricted to the condition that $\gcd(m', n) = 1$ for protecting p and q from being disclosed.

Improvement: We first introduce some preliminaries, which will be used in the improvement, with respect to the quadratic residue problem.

Lemma 1 [10]: Let p be an odd prime.

- (i) If $p \equiv \pm 3 \pmod{8}$, then $2 \in NQR_p$.
- (ii) If $p \equiv \pm 1 \pmod{8}$, then $2 \in QR_p$.

Theorem 4: Let p be an odd prime.

(i) If $p \equiv 3 \pmod{8}$, then $-2 \in QR_p$ and $2 \in NQR_p$.

(ii) If $p \equiv -1 \pmod{8}$, then $2 \in QR_p$ and $-2 \in NQR_p$.

Proof of (i): From lemma 1 (i), we have $2 \in NQR_p$. From theorem 1, we have $-2 \in QR_p$ and $2 \in NQR_p$, since $p \equiv 3 \pmod{8}$ implies $p \equiv 3 \pmod{4}$.

Proof of (ii): From lemma 1 (ii), we have $2 \in QR_p$. From theorem 1, we have $-2 \in NQR_p$ and $2 \in QR_p$, since $p \equiv -1 \pmod{8}$ implies $p \equiv 3 \pmod{4}$.

From theorems 3 and 4, we have the following results.

Theorem 5: Let p and q be distinct primes satisfying $p \equiv 3 \pmod{8}$ and $q \equiv -1 \pmod{8}$, and $n = p \cdot q$.

(i) If $a \in QR_p$ and $a \in QR_q$, then $a \in QR_n$.

(ii) If $a \in QR_p$ and $a \in NQR_q$, then $-2a \in QR_n$.

(iii) If $a \in NQR_p$ and $a \in QR_q$, then $2a \in QR_n$.

(iv) If $a \in NQR_p$ and $a \in NQR_q$, then $-a \in QR_n$.

Now, the improvement of the Nyang-Song scheme is described in the following.

System initialisation: Initially, each user selects two large primes p and q satisfying $p \equiv 3 \pmod{8}$ and $q \equiv -1 \pmod{8}$, and computes $n = p \cdot q$. After that, the user publishes n as his public key and keeps (p, q) as his secret key.

Signature generation: Suppose user U_a wants to sign a message m for the verifier U_b . First, U_a uses a predefined one-way hash function f to compress m into $m' = f(m)$. Then, U_a performs the following steps to generate the signature (s, t) for m :

(i) Choose t according to the following four cases:

Case 1: If $L(m'/p) = L(m'/q) = 1$, then let $t = 1$.

Case 2: If $L(m'/p) = 1$ and $L(m'/q) = -1$, then let $t = -2$.

Case 3: If $L(m'/p) = -1$ and $L(m'/q) = 1$, then let $t = 2$.

Case 4: If $L(m'/p) = L(m'/q) = -1$, then let $t = -1$.

(ii) Compute s satisfying:

$$s \equiv \sqrt{t \cdot m'} \pmod{n}$$

Signature verification: The verifier U_b verifies the signature (s, t) of m with respect to U_a by checking the following congruent equality:

$$s^2 \equiv t \cdot m' \pmod{n}$$

where $m' = f(m)$. If the equality holds, then (s, t) is an authentic signature.

Again, in the improved version, the compressed message m' shall be restricted to the condition that $\gcd(m', n) = 1$ for protecting the secret parameters p and q from being disclosed. From theorem 5, it can be seen that all signature equations used in the improvement are solvable.

Performance and storage requirement: The following notations are used for analysing the computational complexity and storage requirement of the improvement:

T_L : the time for obtaining the value of Legendre symbol

T_{SR} : the time for finding square roots modulo n .

T_f : the time for executing one calculation of the adopted one-way hash function f .

T_m : the time for executing one modular multiplication.

The computational complexity of signature generation in both the Nyang-Song scheme and the improvement is $2T_L + T_{SR} + T_m$, on average. The computational complexity of signature verification in the improvement is $2T_m + T_f$, while two extra modular multiplications are needed in the Nyang-Song scheme.

In the Nyang-Song scheme, each of the public key and the secret key is $2|n|$ bits, and the size of a signature is $|n|+1$ bits. However, in the improvement, each of the public and the secret keys is shortened to $|n|$ bits, and the size of a signature is $|n|+2$ bits.

Security analysis: We will look at some ways in which an adversary may attempt the attacks on the improvement, just as he attempts the attacks on the Nyang-Song scheme.

Attack 1: An adversary attempts an attack by revealing the secret key for any user from public information.

Analysis of attack 1: First of all, an adversary may factor n directly for finding p and q , however, it is based on the factoring

problem [10, 11]. Next, if the adversary knows the signature (s, t) of m , then he can obtain $s^2 - t \cdot m'$ from the signature verification equation, which implies $s^2 - t \cdot m' = k \cdot p$ and $s^2 - t \cdot m' = k' \cdot q$, for k and k' are some integers. From the Chinese remainder theorem [10], we know that $s^2 - t \cdot m' = c \cdot n$, where c is a constant. Therefore, the adversary cannot obtain p and q with knowing the signature of a message.

Attack 2: An adversary attempts an attack by forging a valid signature for impersonating any user without knowing the secret key for that user.

Analysis of attack 2: Given $m' = f(m)$ for some message m , an adversary may first fix t chosen from $\{\pm 1, \pm 2\}$ and then compute the square roots of $t \cdot m'$ modulo n . However, the adversary will face the difficulty of the quadratic residue problem to compute the square roots of $t \cdot m'$ modulo n without knowing p and q [1–9]. An alternative approach is that the adversary may first fix s and then compute t from the signature verification equation. That is, the adversary could compute $t = s^2 \cdot (m')^{-1} \pmod{n}$, where t should be in $\{\pm 1, \pm 2\}$. However, the probability of finding such t is $4/n$, which approximates to the probability of giving t and m' to choose an s from Z_n satisfying the signature verification equation without knowing p and q .

Conclusion: We have proposed an improvement to the Nyang-Song digital signature scheme based on the quadratic residue problem. The improvement and the original Nyang-Song scheme have the same computational complexity for signature generation, however, the improvement is faster for signature verification. The improvement requires shorter public and secret keys for each user, however, the size of a signature is one bit longer than the original one.

© IEE 1997

14 August 1997

Electronics Letters Online No: 19971243

Wei-Hua He and Tzong-Chen Wu (Department of Information Management, National Taiwan University of Science and Technology, Taipei, Taiwan 107, Republic of China)

E-mail: tcwu@cs.ntust.edu.tw

References

- 1 RABIN, M.O.: 'Digitalized signatures and public key functions as intractable as factorization'. Tech. Rep., MIT/LCS/TR-212, MIT Laboratory for Computer Science, MIT, Cambridge, MA, 1979
- 2 CHANG, C.C., JAN, J.K., and KOWNG, H.C.: 'A digital signature scheme based upon the theory of quadratic residues', *Cryptologia*, 1997, **21**, (1), pp. 55–70
- 3 FAN, C.I., and LEI, C.L.: 'Efficient blind signature scheme based on quadratic residues', *Electron. Lett.*, 1996, **32**, (9), pp. 811–813
- 4 FAN, C.I., and LEI, C.L.: 'Low-computation blind signature schemes based on quadratic residues', *Electron. Lett.*, 1996, **32**, (17), pp. 1569–1570
- 5 FEIGE, U., FIAT, A., and SHAMIR, A.: 'Zero knowledge proofs of identity', *J. Cryptol.*, 1988, **1**, (2), pp. 77–94
- 6 FIAT, A., and SHAMIR, A.: 'How to prove yourself: practical solutions to identification and signature problem'. Adv. Cryptol. CRYPTO '86, (Springer-Verlag, 1987), pp. 186–194
- 7 HARN, L., and KIESLER, T.: 'Improved Rabin's scheme with high efficiency', *Electron. Lett.*, 1989, **25**, (11), pp. 726–728
- 8 SHIMADA, M.: 'Another practical public-key cryptosystem', *Electron. Lett.*, 1992, **28**, (23), pp. 2146–2147
- 9 NYANG, D., and SONG, J.: 'Fast digital signature scheme based on the quadratic residue problem', *Electron. Lett.*, 1997, **33**, (3), pp. 205–206
- 10 ROSEN, K.H.: 'Elementary number theory and its applications' (Addison-Wesley, 1993), 3rd edn.
- 11 RIVEST, R.L., SHAMIR, A., and ADLEMAN, L.: 'A method for obtaining digital signatures and public-key cryptosystems', *Commun. ACM*, 1978, **21**, (2) pp. 120–126