Table 3: Number of operations for complex data

Algorithm in [5]			Proposed algorithm ($q=1$)		
$N=$	$M_c(N\times N)$	$A_c(N\times N)$	$N=$	$M_c(N\times N)$	$A_c(N\times N)$
8	48	816	8	48	816
16	720	4496	16	528	4432
32	4175	22928	32	3600	22736
64	24720	111568	64	21072	110352
128	123216	525712	128	111120	521680
256	614928	2421072	256	555984	2401424
Proposed algorithm ($q=3$)			Proposed algorithm ($q=5$)		
$N=$	$M_c(N\times N)$	$A_c(N\times N)$	$N=$	$M_c(N\times N)$	$A_c(N\times N)$
6	32	464	15	5040	900
12	128	2432	30	23760	3600
24	944	12464	60	109440	14400
48	6800	60368	120	506040	68400
96	40592	286544	240	2287320	349200
192	222416	1320848	480	10275000	1731600

Compared to Chan's algorithm, however, savings on both additions and multiplications are achieved by our algorithm. Fig. 1 shows that the additive complexity required by the proposed algorithm is increased with q. However, Fig. 2 shows that the multiplicative complexity is substantially reduced for $q > 0$. Fig. 3 shows a comparison of overall computational complexity (i.e. additions plus multiplications) needed by various algorithms. The proposed algorithm requires the smallest number of operations when $q = 3$. For real input, our algorithm achieves exactly the same number of additions as that in [1] and fewer additions than that in [5]. Fig. 3 also shows that when $q = 3$, our algorithm for real data needs fewer f operations than others.

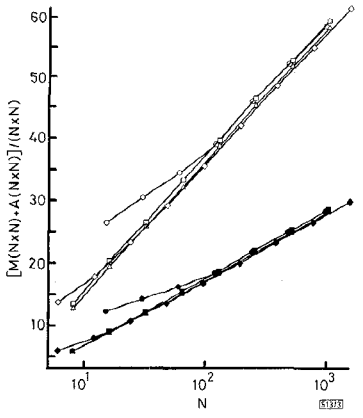

Fig. 3 *Overall complexity for complex and real input*

□ $N = 2^m$ [5], △ $N = 2^m$ [2] and [proposed], ◇ $N = 3 \times 2^m$ [proposed], ○ $N = 15 \times 2^m$ [proposed], ■ $N = 2^m$ [5], ▲ $N = 2^m$ [1] and [proposed], ◆ $N = 3 \times 2^m$ [proposed], ● $N = 15 \times 2^m$ [proposed]

Because the proposed algorithm has the same computational structure as other split-radix ones, it preserves all the desirable properties, such as in place computation, regular permutation and simple memory requirements.

Conclusion: A general split-radix algorithm is proposed for the 2D discrete Fourier transform. Compared to other algorithms ([1] for real data and [2] for complex data), the proposed algorithm achieves a better computational complexity and naturally provides a wider choice of sequence lengths.

Acknowledgment: The authors acknowledge the financial support of PR 24/92 provided by NTU.

26 November 1996

Electronics Letters Online No: 19970170

Guoan Bi and Yanqiu Chen (*School of Electrical and Electronic Engineering, Block S1, Nanyang Technological University, Nanyang Avenue, Singapore 939798, Republic of Singapore*)

E-mail: egbi@ntuvax.ntu.ac.sg

References

1 MOU, Z.J., and DUHARNEL, P.: 'In-place butterfly-style FFT of 2-D real sequences', *IEEE Trans. Acoust., Speech, Sig. Process.*, 1988, **36**, pp. 1642–1650

2 WU, H.R., and PAOLONI, F.J.: 'On the two-dimensional vector-radix FFT algorithm', *IEEE Trans. Acoust., Speech Sig. Process.*, 1989, **37**, pp. 1302–1304

3 KUMARESAN, R., and GUPTA, P.K.: 'Vector-radix algorithm for a 2-D discrete Fourier transforms', *Proc. IEEE*, 1986, **74**, pp. 755–757

4 PEI, S.C., and WU, J.L.: 'Split vecter-radix 2D Fourier transform'. Proc. ICASSP'87, 1987, Dallas, pp. 1987–1990

5 CHAN, M.S.C., and HO, K.L.: 'Split vector radix fast Fourier transform', *IEEE Trans. Sig. Process.*, 1992, **40**, (8), pp. 2029–2039

Fast digital signature scheme based on the quadratic residue problem

DaeHun Nyang and JooSeok Song

Indexing terms: Digital arithmetic, Residue arithmetic, Cryptography

The authors propose a new, fast digital signature scheme which is based on the quadratic residue problem. Only a few computations are needed to obtain and verify a legal signature in the scheme. Moreover, a signature generated in the proposed scheme is very short.

Introduction: Rabin proposed a digital signature scheme in [4], which is based on the square root finding problem in the composite field. This scheme requires redundant information in the signing process and also has non-deterministic characteristics. Harn solved the problems in [3], but his scheme cannot encrypt a message and write a signature when a message a satisfies $gcd(a, pq) \neq 1$. Recently, many signature schemes derived from Rabin's scheme have been proposed. However, they require a large public key and signature [2, 3], and require iterative checks to verify a signature [3, 5].

The signature in the proposed scheme is composed of one integer and one bit flag. Also, a private key consists of just two large primes and an integer, and the public key is composed of the multiplication of two primes and an integer. Because only four multiplications are needed to verify a signature, the proposed scheme is appropriate for applications which require quite a fast verification.

Our signature scheme is based on the fact that the computation used in deciding whether a message is a quadratic residue or not and finding its square root are infeasible in the finite field Z_{pq}^* without knowing the factorisation. In addition, this scheme can be easily extended to the blind signature scheme. For an explanation, we shall denote $J(p/q)$ as the Jacobi symbol and $L(p/q)$ as the Legendre symbol.

$\sqrt{x}$ in Z_p^*, where p is prime: In the finite field Z_p^*, where p is a prime, there are $(p-1)/2$ quadratic residues and $(p-1)/2$ quadratic nonresidues. Thus, for $(p-1)/2$ elements $a \in Z_p^*$, $\sqrt{a}$ does not exist.

Lemma 1: Let p be an odd prime, $a \in Z_p^*$, and $L(a/p)$ is the Legendre symbol. If $p \equiv 3 \bmod 4$, then one of a, $-a$ is a quadratic residue and the other is a quadratic nonresidue.

Proof: From $L(-a/p) = L(-1/p)L(a/p)$ and $L(-1/p) = -1$, $L(-a/p)L(a/p) = -1$. □

We can perform one-to-one mapping of the message a whose quadratic residue does not exist into an unused quadratic residue using Lemma 1. If a message a is a quadratic nonresidue, we map this message into $-a$, which is the quadratic residue by Lemma 1. We assume that $1 \leq a \leq n$, where $p-1 > 2n$. The reason why we make the finite field's size p larger than two times the message's size is that the number of quadratic residues in Z_p^* is exactly $(p-1)/2$.

Using the law of quadratic reciprocity, one can determine in $O(\log p)$ whether a is a quadratic residue or nonresidue modulo p.

$\sqrt{x}$ in Z_m^*, where m is Blum integer: In this Section, we extend the one-to-one mapping of quadratic nonresidue to quadratic residue in Z_m^*, where m is a Blum integer.

Let $m = pq$, where p,q are distinct odd primes and $p \equiv q \equiv 3 \bmod 4$, is called a Blum integer. The $(p-1)(q-1)$ elements a in Z_m^* call be divided into four types based on $L(a/p) = \pm 1$ and $L(a/q) = \pm 1$: (+, +), (+, –), (–, +) and (–, –).

Theorem 1: Let $m > 1$ be an odd integer and the factorisation of m be $\Pi_{i=1}^{r} p_i^{e_i}$. An element $a \in Z_m^*$ is a quadratic residue modulo m iff $L(a/p_i) = 1$ for all $1 \le i \le r$.

Lemma 2: Let $m = pq$, where p, q are distinct odd primes and $p \equiv q \equiv 3 \bmod 4$. (1) If a is a quadratic residue in Z_p^* and Z_q^*, then a is also a quadratic residue in Z_m^*. (2) If a is a quadratic nonresidue in Z_p^* and Z_q^*, then $-a$ is a quadratic residue in Z_m^*.

Proof: $J(a/pq) = L(a/p)L(a/q)$. Because $L(a/p) = L(a/q) = -1$ in (1), a is a quadratic residue by Theorem 1. Because $L(a/p) = L(a/q) = -1$ in (2), $L(-a/p) = L(-a/q) = 1$ by Lemma 1. Therefore, $-a$ is a quadratic residue modulo m by Theorem 1. □

Lemma 3: Let $m = pq$, where p, q are distinct odd primes and $p = q = 3 \bmod 4$. If a is a quadratic residue in Z_p^* and quadratic nonresidue in Z_q^*, then there exists x in Z_m^* such that $x^2 = a \bmod p$ and $x^2 = -a \bmod q$.

Proof: $L(a/p) = 1$, $L(-a/q) = 1$ by Lemma 1. According to the Chinese remainder theorem, there exists such an x. □

By Lemma 2 and 3, we can perform one-to-one mapping of any message a which satisfies $1 \le a \le n$, where $n < (p-1)(q-1)/4$ into a quadratic residue. Using the mapping, we define the pseudo-root.

Definition: Let $s \in Z_m^*$, where $m = pq$ is a Blum integer, $1 \le a \le (p-1)(q-1)/4$. When s satisfies the following, s is called a pseudo-root of a, and denoted $PR(a)$.

If $L(a/p) = L(a/q) = 1$ then $s \equiv \sqrt{a} \bmod m$
else if $L(a/p) = 1$ and $L(a/q) = -1$ then
$s \equiv x \bmod m$ such that $x \equiv \sqrt{a} \bmod p$ and $x \equiv \sqrt{\{-a\}} \bmod q$
else if $L(a/q) = 1$ and $L(a/p) = -1$ then
$s \equiv x \bmod m$ such that $x \equiv \sqrt{a} \bmod q$ and $x \equiv \sqrt{\{-a\}} \bmod p$
else if $L(a/p) = L(a/q) = -1$ then $s \equiv \sqrt{\{-a\}} \bmod m$.

Our digital signature scheme uses the pseudo-root of a message when a signature is written. Thus, a proper oneway perturbation function should be applied before signing a message [1].

New digital signature scheme: We assume the finite field Z_m^*, where $m = pq$ is a Blum integer. For a message $1 \le a \le n$, we choose the field size m such that $(p-1)(q-1) > 4n$. It is assumed that a message to be signed will be perturbed by a oneway function.

In our signature scheme, a (m,B) pair is a public key and a (p,q,b) triple consists of a private key, where $b^4 \equiv B \bmod m$. A signature (s, f) pair is written and verified by the following procedures.

(i) The signing procedure:
if $L(a/p) = L(a/q)$ then $s \equiv PR(a) \bmod m$ and $f = 0$
else $s \equiv b \times PR(a) \bmod m$ and $f = 1$
(ii) The verifying procedure: if $s^4 = b^f a^2 \bmod m$ then PASS
else FAIL

No one can perform the quadratic residue test, the one-to-one mapping and find the square root of a message without prior knowledge of the factorisation. However, when $L(a/p)L(a/q) = -1$, $gcd(s^2 \pm a, m)$ are nontrivial factors of m, so we use a mask b not to expose s^2 to a verifier.

x satisfying $x^2 \equiv a \bmod pq$ can be found in $O(\log pq)$ with probability $\ge 1/2$, provided p and q are known [6]. Especially when p is an odd prime of the form $4n+3$, $\sqrt{a} \equiv a^{(p+1)/4} \bmod p$. Thus the signing of our scheme can be performed deterministically in $O(\log pq)$.

The signature s is verified by simply comparing s^4 with $B^f a^2$. When $s \equiv \sqrt{a} \bmod m$ or $s \equiv \sqrt{\{-a\}} \bmod m$, $f = 0$. Hence, it is trivial that $s^4 \equiv B^f a^2 \bmod m$. In the other cases, the following theorem indicates that a signature can be verified by comparing s^4 with $B^f a^2$.

Theorem: If x satisfies the condition that $x^2 \equiv -a \bmod p$ and $x^2 \equiv a \bmod q$, then $(bx)^4 \equiv B^f a^2 \bmod pq$.

Proof: $x^2 \equiv a' \bmod pq$, where $a' \equiv -a \bmod p$ and $a' \equiv -a \bmod q$. $a'^2 \equiv a^2 \bmod p$ and $a'^2 \equiv a^2 \bmod q$. This relationship can be expressed as $a'^2 \equiv a^2 \bmod pq$. Thus, $x^4 \equiv a'^2 \equiv a^2 \bmod pq$. $b^4 x^4 \equiv b^4 a^2 \equiv B^f a^2 \bmod m$, because $b^4 \equiv B \bmod m$ and $f = 1$. □

Now, we shall prove that two different messages have their own unique signatures.

Theorem: No two messages which the same signature in the proposed scheme.

Proof: Let (s_a, f_a), $(s_{a'}, f_{a'})$ be signatures of a and a', respectively, where $1 < a, a' < (p-1)(q-1)/4$. Let's assume that $a \ne \pm a' \bmod pq$. If $(s_a, f_a) = (s_{a'}, f_{a'})$, then $s_a^2 \equiv s_{a'}^2 \bmod pq$. From this, $s_a^2 \equiv s_{a'}^2 \bmod p$ and $s_a^2 \equiv s_{a'}^2 \bmod q$. Meanwhile, signature s_a and $s_{a'}$ are determined by the following equations according to f_a. When $f_a = f_{a'} = 0$, $L(a/p) = L(a/q) = 1$, and $L(a'/p) = L(a'/q) = 1$,

$$\begin{cases} s_a \equiv \sqrt{a} \bmod p \\ s_a \equiv \sqrt{a} \bmod q \end{cases} \quad \begin{cases} s_{a'} \equiv \sqrt{a'} \bmod p \\ s_{a'} \equiv \sqrt{a'} \bmod q \end{cases}$$

Because $s_a^2 \equiv s_{a'}^2 \bmod p$ and $s_a^2 \equiv s_{a'}^2 \bmod q$, $a \equiv a' \bmod p$ and $a = a' \bmod q$. Thus, $a \equiv a' \bmod pq$. Similarly, when $L(a/p) = L(a/q) = 1$ and $L(a'/p) = L(a'/q) = -1$, $a \equiv -a' \bmod pq$.

When $f_a = f_{a'} = 1$, $L(a/p) = L(a'/p) = 1$, and $L(a/q) = L(a'/q) = -1$,

$$\begin{cases} s_a \equiv b\sqrt{a} \bmod p \\ s_a \equiv b\sqrt{-a} \bmod q \end{cases} \quad \begin{cases} s_{a'} \equiv b\sqrt{a'} \bmod p \\ s_{a'} \equiv b\sqrt{-a'} \bmod q \end{cases}$$

Because $s_a^2 \equiv s_{a'}^2 \bmod p$ and $s_a^2 \equiv s_{a'}^2 \bmod q$, $b^2 a \equiv b^2 a' \bmod p$ and $-b^2 a \equiv -b^2 a' \bmod q$. Thus, $b^2 a \equiv b^2 a' \bmod pq$, and $a \equiv a' \bmod pq$. Similarly, when $L(a/p) = L(a'/q) = 1$, and $L(a/q) = L(a'/p) = -1$, $a \equiv -a' \bmod pq$. These results contradict the assumption. □

Signature s can be replaced by $\sqrt{\{-1\}} \times s \bmod pq$ or $-s \bmod pq$. In fact, this replacement cannot forge a message or make a false signature. Nevertheless, we show that this replacement does not threaten the security of the digital signature. -1 is a quadratic residue in Z_p^*, where p is an odd prime, if and only if $p \equiv 1 \bmod 4$. Because we choose $m = pq$ as a Blum integer, -1 cannot be a quadratic residue. Thus $\sqrt{\{-1\}}$ does not exist. To prevent an attacker from replacing s by $-s$, a signer makes a signature such that $s < pq/2$, and a verifier checks it.

Conclusion: We have designed a new digital signature scheme based on the quadratic residue problem. Since the verification procedure is composed of only four multiplications, it can be performed very quickly. In the signing procedure, a signature within $O(\log pq)$ can be written by performing a quadratic residue test and a calculation of the square root. In terms of storage requirements, our scheme is superior to other schemes.

Furthermore, our digital signature scheme can be easily extended to the blind signature, and it can be applied to the zero knowledge proof using quadratic residue problem with slight modifications.

8 November 1996
Electronics Letters Online No: 19970124

DaeHun Nyang and JooSeok Song (*Department of Computer Science, Yonsei University, Seoul, 120-749, Korea*)

References

1 SHAMIR, A.: 'Cryptanalysis of certain variants of Rabin's signature scheme', *Inf. Process. Lett.*, 1984, pp. 113–115

2 FAN, , and LEI, : 'Low-computation blind signature schemes based on quadratic residues', *Electron. Lett.*, 1996, **32**, (17), pp. 1569–1570

3 HARN, L., and KIESLER, T.: 'Improved Rabin's scheme with high efficiency', *Electron. Lett.*, 1989, **25**, (11), pp. 726–728

4 RABIN, M.O.: 'Digitalized signatures and public key functions as intractable as factorization'. Technical report, MIT/LCS/TR212, MIT Lab., Computer Science, Cambridge, Mass., January 1979

5 SHIMADA, M.: 'Another practical public-key cryptosystem', *Electron. Lett.*, 1992, **28**, (23), pp. 2146–2147

6 PERALTA, R.C.: 'A simple and fast probabilistic algorithm for computing square roots modulo a prime number', *IEEE Trans.*, 1986, **IT-32**, (6), pp. 846–847