Sankhyā : The Indian Journal of Statistics
2010, Volume 72-A, Part 1, pp. 226-236

On the Number of Solutions of the Equation $Rx^2 + Sy^2 = 1 \pmod{N}$

Rana Barua and Mahabir P. Jhanwar
Indian Statistical Institute, Kolkata, India

Abstract

We find by elementary methods the number of solutions of the equation $RX^2 + SY^2 \equiv 1 \pmod{N}$, where N is an RSA composite and R, S are given integers coprime to N . When S (or R) is a square modulo N and its square root is known, our approach gives a very simple randomized algorithm for finding a solution. We also find the number of solutions in terms of Legendre and Jacobi symbols.

AMS (2000) *subject classification.* Primary 11D79, 11D45; Secondary 11T71.
Keywords and phrases. Congruences, number of solutions, randomized algorithm, Jacobi and Legendre symbols.

1 Introduction and preliminaries

In this article we shall consider the following equation in x, y

$$Rx^2 + Sy^2 \equiv 1 \pmod{N}, \tag{1.1}$$

where N is a product of two primes p, q and R and S are given integers coprime to N. Such equations have found several uses in crytography. Ong, Schnorr and Shamir (1984) considered the equation

$$x^2 + ky^2 \equiv m \pmod{N} \tag{1.2}$$

to obtain an efficient digital signature, where k, N are public and the factorization of N is kept secret. A valid signature of a message $m, 0 < m < N$, is a solution (x, y) of the above equation. However, Pollard and Schnorr (1987) have shown that there is a polynomial-time probabilistic algorithm to solve equation (1.2) even when the factorization of N is not known, thereby breaking the Ong-Schnorr-Shamir signature scheme. In FOCS 2008, Boneh, Gentry and Hamburg (2007) obtained a secure space-efficient identity-based encrytion scheme without pairing, using equations of the form (1.1). (The first ID-based encrytion without pairing was, however, obtained by Cocks, 2001). In Boneh et al. (2007), efficient algorithms to solve (1.1) are discussed based on the algorithms of Cremona and Rusin (2003). (See Boneh et al., 2007, for details.) In this article, we shall obtain a count of the number of solutions of equation (1.1) using very elementary properties of congruences. In the special case when R or S is a quadratic residue modulo N and its square root known, our approach gives a very simple probabilistic algorithm to obtain a solution of (1.1). Finally, we shall also give a count of the number of solutions of (1.1) in terms of Jacobi symbols.

For a natural number n, let $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ denote the ring of integers modulo n and let $\mathbb{Z}_n^*$ denote the multiplicative group of integers modulo n. An integer a is said to be a square or quadratic residue modulo N if $a \equiv b^2 \pmod N$ for some integer b. The set of quadratic residues modulo N is denoted by $\mathbf{QR}(\mathbf{N})$. Non-squares are called quadratic non-residue and $\mathbf{QNR}(\mathbf{N})$ denotes the set of quadratic non-residues. The Euler's function is denoted by ϕ and $\phi(n)$ counts the number of positive integers less than n which are coprime to n. For integers a, b let $gcd(a, b)$ denote the greatest common divisor of a and b.

2 Number of solutions when S is a square

We first consider the case when N is prime and S is a quadratic residue modulo N. We shall find solutions (x, y) of equation (1.1) where x is coprime to N.

LEMMA 2.1. *Suppose N is* prime*, S is a quadratic residue modulo N and $s^2 \equiv S \pmod N$. Then any solution (x_0, y_0) of equation (1.1) where $gcd(x_0, N) = 1$, is of the form*

$$\left(\frac{-2st}{R + St^2}, \frac{R - St^2}{s(R + St^2)}\right) \in \mathbb{Z}_N \times \mathbb{Z}_N,$$

for some $t \in \mathbb{Z}_N^*$ such that $R + St^2 \in \mathbb{Z}_N^*$.

Consequently, there is a 1-1 correspondence between the set $A_N \overset{def}{=} \{t \in \mathbb{Z}_N^* : gcd(R + St^2, N) = 1\}$ and all solutions of equation (1.1) of the form (x_0, y_0), with $gcd(x_0, N) = 1$. Hence the number of solutions in this case is $N - 1$, unless $-R \in QR(N)$ in which case it is $N - 3$.

Proof. Here we work in $\mathbb{Z}_N$. Let s be a square root of S modulo N and let (x_0, y_0) be a solution of equation (1.1), where $gcd(x_0, N) = 1$. Let $t = \frac{(y_0 - 1/s)}{x_0}$. Then

$$R + St^2 = R + S\frac{(y_0 - 1/s)^2}{x_0^2} = \frac{Rx_0^2 + Sy_0^2 + 1 - 2y_0 s}{x_0^2} = \frac{2(1 - y_0 s)}{x_0^2}. \quad (2.1)$$

If $R + St^2 \equiv 0 \pmod{N}$, then by (2.1), $y_0 \equiv 1/s \pmod{N}$. But (x_0, y_0) is a solution of $Rx^2 + Sy^2 = 1 \pmod{N}$ and this implies $x_0 \equiv 0 \pmod{N}$, contradicting the fact that $gcd(x_0, N) = 1$. Thus we must have, $gcd(R + St^2, N) = 1$. Also

$$\begin{aligned} R - St^2 = R - S\frac{(y_0 - 1/s)^2}{x_0^2} &= \frac{Rx_0^2 - Sy_0^2 - 1 + 2y_0 s}{x_0^2} \\ &= \frac{2y_0 s(1 - y_0 s)}{x_0^2} = y_0 s(R + St^2). \end{aligned}$$

Hence, $y_0 = \frac{R - St^2}{s(R + St^2)}$. Further,

$$-2st = -2s\frac{(y_0 - 1/s)}{x_0} = \frac{2(1 - y_0 s)}{x_0} = \frac{1}{x_0}.2(1 - y_0 s) = \frac{1}{x_0}(R + St^2)x_0^2,$$

by equation (2.1). This yields

$$x_0 = \frac{-2st}{R + St^2}.$$

Incidentally, we also have $gcd(t, N) = 1$. With such a solution we associate the $t \in \mathbb{Z}_N^*$ thus obtained. Plainly, $R + St^2$ is coprime to N. This forms a 1-1 correspondence with the set A_N. For, corresponding to such a $t \in A_N$, the pair $(\frac{-2st}{R+St^2}, \frac{R-St^2}{s(R+St^2)})$ is a solution. Moreover, if

$$\frac{-2st}{R + St^2} = \frac{-2st'}{R + S(t')^2} \quad \text{and} \quad \frac{R - St^2}{s(R + St^2)} = \frac{R - S(t')^2}{s(R + S(t')^2)},$$

then from the second equation we have $t^2 = (t')^2$. Hence, the first equation yields $t = t'$.

To see the last part, note that if $-R \in QNR(N)$ for any $t \in \mathbb{Z}_N^*, R + St^2 \not\equiv 0 \pmod{N}$ and hence $|A_N| = N - 1$. If $-R \in QR(N)$, then for $t = \pm\sqrt{-R/S}$, $R + St^2 \equiv 0 \pmod{N}$. Otherwise, $R + St^2 \not\equiv 0 \pmod{N}$. Hence in this case, the number of solutions is $N - 3$. □

REMARK 2.1. An analogous result can be proved when R is a quadratic residue modulo N.

As an immediate consequence of this, we have

COROLLARY 2.1. *Let $N = pq$, where p, q are primes. Then any solution (x_0, y_0) of equation (1.1), with $gcd(x_0, N) = 1$, is of the form*

$$\left(\frac{-2st}{R+St^2}, \frac{R-St^2}{s(R+St^2)}\right) \in \mathbb{Z}_N \times \mathbb{Z}_N,$$

for some $t \in \mathbb{Z}_N^*$, such that $R + St^2 \in \mathbb{Z}_N^*$.

PROOF. Since (x_0, y_0) is a solution to both the equations

$$Rx^2 + Sy^2 \equiv 1 \pmod{p},$$

$$Rx^2 + Sy^2 \equiv 1 \pmod{q},$$

we have by Lemma 2.1

$$x_0 \equiv \frac{-2st_1}{R+St_1^2} \pmod{p}, \quad y_0 \equiv \frac{R-St_1^2}{s(R+St_1^2)} \pmod{p},$$

$$x_0 \equiv \frac{-2st_2}{R+St_2^2} \pmod{q}, \quad y_0 \equiv \frac{R-St_2^2}{s(R+St_2^2)} \pmod{q},$$

where $t_1 \in \mathbb{Z}_p^*, t_2 \in \mathbb{Z}_q^*$ and $gcd(R + St_1^2, p) = 1, gcd(R + St_2^2, q) = 1$.

Let t be the unique integer in $\mathbb{Z}_N^*$ such that $t \equiv t_1 \pmod{p}$ and $t \equiv t_2 \pmod{q}$. Clearly for this t, we have $gcd(R + St^2, N) = 1$. Also, one can easily see that

$$x_0 \equiv \frac{-2st}{R+St^2} \pmod{N}, \quad y_0 \equiv \frac{R-St^2}{s(R+St^2)} \pmod{N}.$$

□

We now look at solutions (x, y) when x is not co-prime to N.

LEMMA 2.2. *Suppose N is prime. The number of solutions (x_0, y_0), where $x_0 \equiv 0 \pmod{N}$ is 2, if $S \in QR(N)$, and is 0, if $S \in QNR(N)$.*

PROOF. We work in $\mathbb{Z}_N$. If $S \in QNR(N)$, then $(0, y_0)$ cannot be a solution to equation (1.1). For otherwise, $S = 1/y_0^2$, which is not possible.

Now suppose, $S \in QR(N)$ and let s_1, s_2 be the two square roots of S. If $(0, y_0)$ is a solution, then clearly $y_0 = 1/s_i$ for some $i = 1, 2$. □

Lemmas 2.1 and 2.2 yield the number of solutions of (1.1) in the case when N is prime.

Theorem 2.1. *Let N be prime and S a square modulo N. Let η_N denote the number of solutions of equation (1.1). Then*

$$\eta_N = \begin{cases} N-1 & \text{if } -R \in QR(N), \\ N+1 & \text{if } -R \in QNR(N). \end{cases}$$

The above theorem gives us the count at least when S is a square.

Theorem 2.2. *Let $N = pq$, where p and q are primes. Suppose S is a quadratic residue modulo N. Let η_N denote the number of solutions of equation (1.1). Then*

$$\eta_N = \begin{cases} (p-1)(q-1) = \phi(N) & \text{if } -R \in QR(N), \\ (p-1)(q+1) & \text{if } -R \in QR(p) \text{ and } -R \in QNR(q), \\ (p+1)(q-1) & \text{if } -R \in QNR(p) \text{ and } -R \in QR(q), \\ (p+1)(q+1) & \text{if } -R \in QNR(p) \text{ and } -R \in QNR(q). \end{cases}$$

Proof. Using the Chinese Remainder Theorem, it is not hard to show that $\eta_N = \eta_p \times \eta_q$. Now η_p (resp. η_q) is $p-1$ or $p+1$ (resp. $q-1$ or $q+1$) according as $-R$ is square or non-square modulo p (resp. q). The result now follows immediately. □

Corollary 2.1 above yields a simple algorithm for obtaining a solution of equation (1.1), when S is a quadratic residue and its square root is known or can be computed. (See also Jhanwar and Barua, 2009).

Algorithm $\mathcal{A}$:

1. Compute $s \in \mathbb{Z}_N^*$ such that $s^2 = S \bmod N$.
2. Choose randomly a point $t \in \mathbb{Z}_N^*$.
3. If $gcd(R + St^2, N) \neq 1$ then report **failure**.
4. **Else** compute

$$x = \frac{2st}{R + St^2}, \; y = \frac{R - St^2}{s(R + St^2)}.$$

Output (x, y).
It is clear from Corollary 2.1 that (x, y) is a solution of equation (1.1). Also by Lemma 2.1, the algorithm succeeds with probabilty at least $\frac{(p-3)(q-3)}{N}$.

REMARK 2.2. For step 1, one needs the factorization of N. Then s can be efficiently computed using standard methods. Otherwise, the square root s needs to be given as input.

Analogously, if R is a quadratic residue and its square root r is given, then we have the following algorithm.

ALGORITHM $\mathcal{B}$:

1. Find $r \in \mathbb{Z}_N^*$ such that $r^2 = R \bmod N$.
2. Choose randomly a point $t \in \mathbb{Z}_N^*$.
3. If $gcd(S + Rt^2, N) \neq 1$, then report **failure**.
4. **Else** compute

$$x = \frac{S - Rt^2}{r(S + Rt^2)}, \; y = \frac{2rt}{S + Rt^2}.$$

Output (x, y).

REMARK 2.3. Algorithm $\mathcal{B}$ can be used to obtain a forgery of the Ong-Schnorr-Shamir signature scheme (Ong, Schnorr and Shamir, 1984) much simpler than that of Pollard and Schnorr (1987). One simply chooses the message $m = \frac{1}{r^2} \in \mathbb{Z}_n^*$ and invoke algorithm $\mathcal{B}$ to obtain a solution of (1.2) which gives the signature of m.

3 The general case

We now consider the case when R or S may not be a quadratic residue. Again, we first assume that N is a prime and that a solution of equation (1.1) is known. (Such a solution can be found by picking a random $y \in \mathbb{Z}_N$ and apply some well-known square root algorithm to $\frac{1-Sy^2}{R}$ to obtain x, cf., Pollard and Schnorr, 1987.) Fix such a solution $(x^*, y^*) \in \mathbb{Z}_N \times \mathbb{Z}_N$ of equation (1.1). (If R(resp. S) is a quadratic residue we may take $(x^*, y^*) = (1/r, 0)$ (resp. $=(0, 1/s)$), where r (resp. s) is a square root of R (resp. S) modulo N.)

Lemma 3.1. *Let $(x_0, y_0) \in \mathbb{Z}_N \times \mathbb{Z}_N$ be a solution of equation (1.1) with $gcd(x_0 - x^*, N) = 1$. Then*

$$x_0 = -\frac{(R - St^2)x^* + 2Sty^*}{R + St^2}, \quad y_0 = \frac{-2Rtx^* + (R - St^2)y^*}{R + St^2}, \tag{3.1}$$

for some $t \in \mathbb{Z}_N^*$ with $gcd(R + St^2, N) = 1$.

Hence, there is a 1-1 correspondence with such solutions and the set A_N of Lemma 2.1.

Proof. Here we work in $\mathbb{Z}_N$. Let (x_0, y_0) be a solution of equation (1.1), where $gcd(x_0 - x^*, N) = 1$. Let $t = \frac{y_0 - y^*}{x_0 - x^*}$. Then

$$R + St^2 = R + S\frac{(y_0 - y^*)^2}{(x_0 - x^*)^2} = \frac{2 - 2(Rx_0x^* + Sy_0y^*)}{(x_0 - x^*)^2}. \tag{3.2}$$

If $R + St^2 \equiv 0 \pmod{N}$, then

$$Rx_0x^* + Sy_0y^* \equiv 1 \pmod{N}. \tag{3.3}$$

Also, we have

$$Rx_0^2 + Sy_0^2 \equiv 1 \pmod{N}, \quad R(x^*)^2 + S(y^*)^2 \equiv 1 \pmod{N}.$$

By subtraction we obtain

$$Rx_0(x^* - x_0) + Sy_0(y^* - y_0) \equiv 0 \pmod{N},$$

$$Rx^*(x^* - x_0) + Sy^*(y^* - y_0) \equiv 0 \pmod{N}.$$

Hence $\frac{x_0}{x^*} \equiv \frac{y_0}{y^*} \equiv k \pmod{N}$, say. So $x_0 \equiv kx^* \pmod{N}$ and $y_0 \equiv ky^* \pmod{N}$. Substitution in equation (3.3) yields $k \equiv 1 \pmod{N}$ which contradicts the fact that $gcd(x_0 - x^*, N) = 1$. Thus we must have $gcd(R + St^2, N) = 1$.

Now, we have

$$Sy_0y^* = Sy^*(y_0 - y^*) + S(y^*)^2 = Sty^*(x_0 - x^*). \tag{3.4}$$

Hence by (3.2) and (3.4) we obtain

$$(x_0 - x^*)^2 = 2\frac{1 - (Rx_0x^* + Sy^*(y_0 - y^*) + S(y^*)^2)}{R + St^2}$$

$$= 2\frac{1 - (Rx_0x^* + St(x_0 - x^*) + S(y^*)^2)}{R + St^2}$$
$$= 2\frac{R(x^*)^2 - Rx_0x^* - St(x_0 - x^*)}{R + St^2},$$

which yields

$$x_0 - x^* = -2\frac{Rx^* + Sty^*}{R + St^2}.$$

On simplification, we obtain,

$$x_0 = -\frac{(R - St^2)x^* + 2Sty^*}{R + St^2}.$$

Also we have, $y_0 - y^* = t(x_0 - x^*)$. Putting the value of x_0 we get

$$y_0 = \frac{-2Rtx^* + (R - St^2)y^*}{R + St^2}.$$

Denote the right-sides of equations (3.1) by x_t, y_t. Suppose $x_t = x_{t'}$ and $y_t = y_{t'}$. Then from the last relation one obtains $y^* + t(x_t - x^*) = y^* + t'(x_{t'} - x^*)$ and hence $t = t'$. This establises the 1-1 correspondence. □

As in Lemma 2.2, the following can easily be proved.

LEMMA 3.2. *Suppose N is prime. Then the number of solutions (x_0, y_0), where $x_0 \equiv x^* \pmod{N}$, is 2.*

Thus we have, as in the previous section, the following

THEOREM 3.1. *Suppose $N = pq$, where p and q are primes. Let η_N denote the number of solutions of equation (1.1). Then*

$$\eta_N = \begin{cases} (p-1)(q-1) = \phi(N) & \textit{if } -R/S \in QR(N), \\ (p-1)(q+1) & \textit{if } -R/S \in QR(p) \textit{ and } -R/S \in QNR(q), \\ (p+1)(q-1) & \textit{if } -R/S \in QNR(p) \textit{ and } -R/S \in QR(q), \\ (p+1)(q+1) & \textit{if } -R/S \in QNR(p) \\ & \quad \textit{and } -R/S \in QNR(q). \end{cases}$$

PROOF. We have $\eta_N = \eta_p \times \eta_q$. But by Lemmas 3.1 and 3.2

$$\eta_p = |A| + 2 = \begin{cases} p-1 & \text{if } -R/S \in QR(p), \\ p+1 & \text{if } -R/S \in QNR(p). \end{cases}$$

Similar expression holds for η_q. The result now follows immediately. □

4 Number of solutions in terms of Jacobi symbols

For prime p, we denote the finite field $\mathbb{Z}/p\mathbb{Z}$ by F_p. We denote by F_p^* the multiplicative group $F_p - \{0\}$.

The Legendre symbol $\left(\frac{a}{p}\right)$ for $a \in F_p^*$ is defined to be $+1$ or -1 according as $a \in QR(p)$ or not and is 0 if $p\,|a$. If $N = \Pi_{i=1}^{k} p_i^{e_i}$, then the Jacobi symbol is defined as

$$\left(\frac{a}{N}\right) = \Pi_{i=1}^{k} \left(\frac{a}{p_i}\right)^{e_i}.$$

Then clearly, the number of solutions of $x^2 = a$ is

$$N_p(x^2 = a) = 1 + \left(\frac{a}{p}\right).$$

We shall need the following result for Legendre symbols which follows as a special case of a result for Jacobi sums (See Ireland and Rosen, 1990).

Lemma 4.1. $\sum_{a+b\equiv 1} \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = -\left(\frac{-1}{p}\right)$

We first compute the number of solutions of $Rx^2 + Sy^2 = 1 \pmod p$ and $Rx^2 + Sy^2 = 1 \pmod q$ respectively. We then apply the Chinese Remainder Theorem to obtain the total number of solutions of $Rx^2 + Sy^2 = 1 \pmod N$.

$N_n(Rx^2+Sy^2 = 1)$ denote the total number of solutions of $Rx^2+Sy^2 = 1 \pmod n$. Thus we have

$$\begin{aligned}
N_p(Rx^2 + Sy^2 = 1) &= \sum_{Ra+Sb=1} N_p(x^2 = a) N_p(y^2 = b) \\
&= \sum_{Ra+Sb=1} (1 + \left(\frac{a}{p}\right))(1 + \left(\frac{b}{p}\right)) \\
&= \sum_{Ra+Sb=1} 1 + \sum_{Ra+Sb=1} \left(\frac{a}{p}\right) + \sum_{Ra+Sb=1} \left(\frac{b}{p}\right) \\
&\quad + \sum_{Ra+Sb=1} \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \\
&= p + 0 + 0 + \sum_{Ra+Sb=1} \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \\
&= p + \sum_{u+v=1} \left(\frac{R^{-1}u}{p}\right)\left(\frac{S^{-1}v}{p}\right)
\end{aligned}$$

$$\begin{aligned}
&= p + \sum_{u+v=1} \left(\frac{R^{-1}}{p}\right)\left(\frac{u}{p}\right)\left(\frac{S^{-1}}{p}\right)\left(\frac{v}{p}\right) \\
&= p + \left(\frac{R^{-1}}{p}\right)\left(\frac{S^{-1}}{p}\right)\sum_{u+v=1}\left(\frac{u}{p}\right)\left(\frac{v}{p}\right) \\
&= p - \left(\frac{R^{-1}}{p}\right)\left(\frac{S^{-1}}{p}\right)\left(\frac{-1}{p}\right) \text{ by Lemma 4.1} \\
&= p - \left(\frac{R}{p}\right)\left(\frac{S}{p}\right)(-1)^{\frac{p-1}{2}}.
\end{aligned}$$

Similarly

$$N_q(Rx^2 + Sy^2 = 1) = q - \left(\frac{R}{q}\right)\left(\frac{S}{q}\right)(-1)^{\frac{q-1}{2}}.$$

Hence by the Chinese Remainder theorem, we have

$$\begin{aligned}
& N_N(Rx^2 + Sy^2 = 1) \\
= \; & N_p(Rx^2 + Sy^2 = 1)N_q(Rx^2 + Sy^2 = 1) \\
= \; & \left[p - \left(\frac{R}{p}\right)\left(\frac{S}{p}\right)(-1)^{\frac{p-1}{2}}\right]\left[q - \left(\frac{R}{q}\right)\left(\frac{S}{q}\right)(-1)^{\frac{q-1}{2}}\right] \\
= \; & N - p\left(\frac{R}{q}\right)\left(\frac{S}{q}\right)(-1)^{\frac{q-1}{2}} - q\left(\frac{R}{p}\right)\left(\frac{S}{p}\right)(-1)^{\frac{p-1}{2}} \\
& +(-1)^{\frac{p-1}{2}}(-1)^{\frac{q-1}{2}}\left(\frac{R}{N}\right)\left(\frac{S}{N}\right).
\end{aligned}$$

References

Boneh, D., Gentry, C. and Hamburg, M. (2007). Space-efficient identity based encryption without pairings. In *48th Annual IEEE Symposium on Foundations of Computer Science (FOCS'07)*. IEEE Computer Society, Providence, RI, 647–657. Full version is available at `http://crypto.stanford.edu/~dabo/`.

Cocks, C. (2001). An identity based encryption scheme based on quadratic residues. In *Cryptography and Coding*, (B. Honary, ed.). Lecture Notes in Comput. Sci., **2260**. Springer, Berlin, 360–363.

Cremona, J.E. and Rusin, D. (2003). Efficient solution of rational conics. *Math. Comp.*, **72**, 1417–1441.

IRELAND, K. and ROSEN, M. (1990). *A Classical Introduction to Modern Number Theory.* Second Edition. Graduate Texts in Mathematics, **84**. Springer-Verlag, New York.

JHANWAR, M. and BARUA, R. (2009). A semantically secure public key encryption in the standard model. In *Preproceedings of the International Workshop on Coding and Cryptography (WCC'09)*, 181–190.

ONG, H., SCHNORR, C.P. and SHAMIR, A. (1984). An efficient signature scheme based on quadratic equations. *Proc. 16th Annual ACM Symposium on Theory of Computing (STOC'84)*, 208–216.

POLLARD, J. M. AND SCHNORR, C. P. (1987). An efficient solution of the congruence $x^2 + ky^2 = m \pmod n$, *IEEE Trans. Inform. Theory.* **33**, 702–709.

RANA BARUA AND MAHABIR P. JHANWAR
STAT-MATH UNIT
INDIAN STATISTICAL INSTITUTE
203 B.T. ROAD
KOLKATA 700108, INDIA
E-mail: rana@isical.ac.in
mahavir.jhawar@gmail.com

Paper received September 2009; revised January 2010.