New weak findings upon RSA modulo of type $N = p^2 q$

ABSTRACT

This paper proposes new attacks on RSA with the modulus $N = p^2 q$. The first attack is based on the equation $eX - NY = p^2 u + q^2 v + Z$ such that u is an integer multiple of 2 and v is an integer multiple of 3. If

$$|p^2 u - q^2 v| < N^{1/2},$$

$$|Z| \frac{|p^2 - q^2|}{3(p^2 + q^2)} < N^{1/3}$$

and

$$X < \frac{\sqrt{3(p^2 u + q^2 v)}}{3(p^2 u + q^2 v)}$$

then N can be factored in polynomial time using continued fractions. For the second and third attacks, this paper proposes new vulnerabilities in k RSA Moduli $N_i = p_{ii}^2 q_i$ for $k \geq 2$ and $i = 1,...,k$. The attacks work when k RSA public keys (N_i, e_i) are related through

$$e_i x - N_i y_i = p_{ii}^2 u + q_{ii}^2 v + z_i$$

or

$$e_i x_i - N_i y = p_{ii}^2 u + q_{ii}^2 v + z_i$$

where the parameters x, xi, y, yi and zi are suitably small.

Keyword: RSA; Factorization; Continued fraction; LLL algorithm; Simultaneous diophantine approximations