International Journal of Cryptology Research 11(1): 28 - 32 (2021)

A Comment on "Key Generation Using Generalized Pell's Equation in Public Key Cryptography Based on the Prime Fake Modulus Principle to Image Encryption and Its Security Analysis"

Zahari Mahad[1]

[1]*Lab. of Cryptography, Analysis and Structure, Institute for Mathematical Research, Universiti Putra Malaysia, 43400 UPM Serdang, Selangor, Malaysia.*

E-mail: zaharimahad@upm.edu.my
**Corresponding author*

ABSTRACT

This write-up shows that the public key system proposed by (Rao et al., 2020) is insecure, even by using the concept of fake modulus and generalized Pell's equation.

Keywords: Public Key Cryptography, RSA Cryptosystem, Pell's Equation

1 INTRODUCTION

In (Rao et al., 2020), the authors present the RSA cryptosystem using the concept of fake modulus and generalized Pell's equation. By using that concept, the authors assume that their public key system is secure and the security of the RSA cryptosystem is enhanced.

2 THE PROPOSED METHOD BY Rao et al. (2020)

We have simplified the details of the proposed method such as Key Generation, Encryption and Decryption Processes here based on the description in (Rao et al., 2020) into Algorithm 1, Algorithm 2 and Algorithm 3, respectively.

Algorithm 1: Key Generation Process

```
Input: Size of prime $k$
Output: Public key, $(A, z)$ and Private key, $(B, z)$
Choose 4 distinct primes $p$, $q$, $r$ and $s$          // same $k$-bits size
Compute $N = p \times q \times r \times s$
Compute $\phi(N) = (p-1) \times (q-1) \times (r-1) \times (s-1)$
Select an integer $u$ and generate $R$, $x$ and $y$ that satisfying
  $x^u - Ry^u = 1$
Choose integer $e$ with the gcd$(e, \phi(N)) = 1$
Compute $d \equiv e^{-1} \pmod{\phi(N)}$
Compute $\beta = (x + \phi(N))^u - R(y+e)^u$
Compute public exponent, $A = (\beta + R(y+e)^u - Ry^u) \cdot d^u$
  $\pmod{\phi(N)}$
Compute private exponent, $B = e^u \pmod{\phi(N)}$
Compute Fake modulus, $z = \frac{ed-1+k}{k}$
Return Public key, $(A, z)$ and Private key, $(B, z)$
```

Algorithm 2: Encryption Process

```
Input: Plaintext, $m$
Output: Ciphertext, $c$
Compute ciphertext, $c = m^A \pmod{z}$
Return Ciphertext, $c$
```

Algorithm 3: Decryption Process

```
Input: Ciphertext, $c$
Output: Plaintext, $m$
Compute plaintext, $m = c^B \pmod{z}$
Return Plaintext, $m$
```

Example 2.1.

Key Generation:
$u = 5$, $R = 31$, $x = 2$ *and* $y = 1$
$N = p \cdot q \cdot r \cdot s = 43 \cdot 53 \cdot 61 \cdot 47 = 6533893$
$\phi(N) = (p-1)(q-1)(r-1)(s-1) = 42 \cdot 52 \cdot 60 \cdot 48 = 6027840$
$e = 1032301$ *and* $d \equiv e^{-1} \pmod{\phi(N)} = 2003941$
$\beta = 79217574417786619090624925163302 40$
Public exponent $A = 5061781$
Private exponent $B = e^u \pmod{\phi(N)} = 3740221$
Fake modulus $z = \frac{ed-1+k}{k} = 413734059649$

Encryption:
Plaintext, $m = 12345$
Ciphertext, $c \equiv m^A \pmod{z} \equiv 12345^{5061781} \equiv 379529689509 \pmod{413734059649}$

Decryption:
Plaintext, $m \equiv c^B \pmod{z} \equiv 379529689509^{3740221} \equiv 12345 \pmod{413734059649}$

Based on observation, using Fake modulus z as a prime number instead of N as modulus will allow a trapdoor in the decryption process. We show in the next section that this method produces an insecure cryptosystem.

3 CRYPTANALYSIS

Definition 3.1. *We say two integers A and z are relative prime or co-prime if $gcd(A, z) = 1$.*

Proposition 3.1. *Let two integers A and Z are relative prime with $gcd(A, Z) = 1$ then $A \cdot B \equiv 1 \pmod{Z}$ for some integer B.*

Proof. Suppose $\gcd(A, Z) = 1$, then the Extended Euclidean Algorithm tell us that we can find the integers B and Y such that $AB - ZY = 1$. It means that $AB - 1 = ZY$ is divisible by Z for some integer Y. So $A \cdot B \equiv 1 \pmod{Z}$. □

Using this proposition, we show that it is possible to decrypt the ciphertext without knowing the private exponent. By referring to (Rao et al., 2020), it is a **BIG MISTAKE** when the authors set the Fake modulus, z must be a prime number. Due to that setting, anyone can decrypt and read the original plaintext. Considering the public exponent A is a odd number and z is a prime number with gcd$(A, \phi(z)) = 1$, then absolutely there exist a multiplicative inverse of A. This is trivally solved using the extended Euclidean algorithm.

Example 3.1. *Based on the Example 2.1, we have the public key* $(A, z) = (5061781, 413734059649)$. *From that information, we know that the gcd*$(A, z-1) = 1$. *Therefore, by using Proposition 3.1 above, we can compute the multiplicative inverse of the public exponent* A *where denoted as* $\hat{B} \equiv A^{-1} \pmod{z} \equiv 5061781^{-1} \equiv 210782838205 \pmod{413734059649}$. *As we can see,* $B \neq \hat{B}$. *However, we still can get the plaintext by decrypting the ciphertext using the* $\hat{B}$ *as* $m \equiv c^{\hat{B}} \pmod{z} \equiv 379529689509^{210782838205} \equiv 12345 \pmod{413734059649}$.

4 CONCLUSION

We finally conclude that this system is insecure even the authors claim that by using concept of fake modulus and generalized Pell's equation, they can enhanced the security of RSA cryptosystem. However, based on our observation it is proven that their scheme not secure.

ACKNOWLEDGMENTS

I want to thank Prof. Dr. Muhammad Rezal Kamel Ariffin and Dr. Muhammad Asyraf Asbullah for their encouragement to write this write-up.

REFERENCES

Rao, R., Ganesh, A., Surendra, S., and Kallapu, B. (2020). Key Generation Using Generalized Pell's Equation in Public Key Cryptography Based on the Prime Fake Modulus Principle to Image Encryption and Its Security Analysis. *Cybernetics and Information Technologies*, 20(3):86–101.