A Comment on "Cryptographic Applications of Brahmagupta–Bhãskara Equation"

Amr M. Youssef

***Abstract*—Murthy and Swamy proposed a symmetric key encryption system based on Brahmagupta–Bhãskara equation over $\mathrm{GF}(p)$. In this comment, we show that breaking this system is equivalent to solving a set of linear equations over the field of rational numbers. Our attack, typically, requires as low as three known plaintext–ciphertext pairs and allows the cryptanalyst to fully recover the secret key.**

***Index Terms*—Brahmagupta–Bhãskara (BB) equation, communication and network security, cryptography, digital encryption.**

I. Introduction

THE Brahmagupta–Bhãskara (BB) equation [1] is a quadratic Diophantine equation of the form

$$NX^2 + k = Y^2$$

where k is an integer and N is a positive integer such that N is irrational. A particular case of the above BB equation with $k = 1$ is known as Pell equations.

Recently, Murthy and Swamy [2] proposed a symmetric key cryptosystem [3] based on the Pell equations over $\mathrm{GF}(p)$.

In this comment, we show that breaking this system is equivalent to solving two sets of four linear equations over the field of rational numbers. Our attack, typically, requires as low as three known plaintext–ciphertext pairs and allows the cryptanalyst to fully recover the secret key.

Throughout the rest of this section, we briefly describe the aspects of the encryption algorithm related to our attack. For further details about the system, the reader is referred to [2]. The role of the various parameters of the BB equation in the proposed encryption process is as follows.

- n corresponds to the plaintext in a block that is being encrypted.
- p is an odd prime number which corresponds to the primary secret key.
- Let (q_{x_i}, q_{y_i}) be a valid solution of the corresponding BB equation

$$n_i q_{x_i} + k = q_{y_i} \bmod p.$$

Then, the ciphertext c_i corresponding to n_i is the pair (s_{q_i}, d_{q_i}) derived from q_{x_i} and q_{y_i} as follows:

$$s_{q_i} = (a q_{x_i} + b q_{y_i}) \bmod p \tag{1}$$

and

$$d_{q_i} = (a q_{x_i} - b q_{y_i}) \bmod p \tag{2}$$

where $p > n$, and $a, b > 0$. The parameters a and b are referred to as secondary keys.

II. Proposed Attack

Schneier [4] provides a nice introduction to different types of cryptanalytic attacks. A mathematical treatment can be found in [3]. For a background about number theory, the reader is referred to [5].

Before we present our attack, we briefly review some of the definitions and mathematical background required by our attack.

Definition 1: A rational number r is a number that can be expressed as a fraction $r = m/n$ where m and n are integers and $n \neq 0$.

The set of all rational numbers are referred to as the *rationals* and forms a field $\mathcal{Q}$ defined as

$$\mathcal{Q} = \left\{ \frac{m}{n} : m \in \mathcal{Z}, n \in \mathcal{Z}, n \neq 0 \right\}$$

where $\mathcal{Z}$ denotes the ring of integers.

Lemma 1: Let $x_1, x_2 \in \mathcal{Z}$. If $x_1 = x_2 \bmod p$, then $p|(x_1 - x_2)$.

Our attack is a known plaintext attack in which the cryptanalyst is assumed to know at least three plaintext–ciphertext pairs. In particular, we assume that the cryptanalyst knows n_1, n_2 and n_3 and their corresponding (s_{q1}, d_{q1}), (s_{q2}, d_{q2}) and (s_{q3}, d_{q3}), respectively. By adding (1) and (2) over $\mathcal{Z}$, we get

$$s_{q_i} + d_{q_i} = 2 a q_{x_i}, \qquad i = 1, 2, 3.$$

Similarly, by subtraction, we get

$$\begin{aligned} s_{q_i} - d_{q_i} &= 2 b q_{y_i} \\ &= 2b\,(n_i q_{x_i} + 1), \qquad i = 1, 2, 3. \end{aligned}$$

The above seemingly nonlinear equations (with indeterminates (a, b, q_{x_i})) can be linearized by rewriting them as follows:

$$\begin{aligned} a^{-1}\,(s_{q_i} + d_{q_i}) &= 2 q_{x_i} \\ b^{-1}\,(s_{q_i} - d_{q_i}) &= 2\,(n_i q_{x_i} + 1) \end{aligned} \tag{3}$$

Thus, from the knowledge of n_1, n_2 and their corresponding ciphertexts (s_{q1}, d_{q1}), (s_{q2}, d_{q2}), the cryptanalyst can construct a system of 4 linear equations over $\mathcal{Q}$ with 4 indeterminates $(a^{-1}, b^{-1}, q_{x1}, q_{x2})$ as follows:

$$\begin{pmatrix} s_{q_1} + d_{q_1} & 0 & -2 & 0 \\ s_{q_2} + d_{q_2} & 0 & 0 & -2 \\ 0 & s_{q_1} - d_{q_1} & -2n_1 & 0 \\ 0 & s_{q_2} - d_{q_2} & 0 & -2n_2 \end{pmatrix} \begin{pmatrix} a^{-1} \\ b^{-1} \\ q_{x_1} \\ q_{x_2} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 2 \\ 2 \end{pmatrix}.$$

Let $(a_{11}/a_{12}, b_{11}/b_{12})$ denote the values obtained for a^{-1} and b^{-1} by solving the above system of equations over the field of rational numbers. Similarly, let $(a_{21}/a_{22}, b_{21}/b_{22})$ denote the values obtained for a^{-1} and b^{-1} by solving the above system of equations corresponding to (n_1, n_3) [or (n_2, n_3)] over $\mathcal{Q}$. Thus, we have

$$\begin{aligned} a_{11} \times a_{22} &= a_{12} \times a_{21} \bmod p \\ b_{11} \times b_{22} &= b_{12} \times b_{21} \bmod p. \end{aligned}$$

Manuscript received May 19, 2006; revised August 28, 2006. This work was supported inpart by the Natural Sciences and Engineering Research Council of Canada (NSERC) under Grant N00930. This paper was recommended by Associate Editor C.-W. Wu.

The author is with the Concordia Institute for Information Systems Engineering, Concordia University, Montreal, QC H3G IM8, Canada (e-mail: youssef@ciise.concordia.ca).

Digital Object Identifier 10.1109/TCSI.2007.893508

From Lemma 1, the attacker can recover p (or an integer multiple of p) by calculating

$$p' = gcd(a_{11} \times a_{22} - a_{12} \times a_{21}, b_{11} \times b_{22} - b_{12} \times b_{21}) \quad (4)$$

where $gcd(\cdot,\cdot)$ denotes the greatest common divisor of the enclosed arguments and which can be efficiently calculated using the Euclidean algorithm [3]. The two solutions obtained for q_{x_1} can also be used in (4).

Note that p' can also be a multiple of p. This can be tested by checking the primality of p'. If p' turns out to be a composite number, then we can either factor it or use more known plaintexts-ciphertext pairs to directly recover p by passing more arguments to the gcd function above.

Once p is recovered, the secondary keys (a, b) can be recovered by evaluating the solution of the above system of equations over $\mathrm{GF}(p)$.

One should note that the claimed requirements of 3 plaintext–ciphertext pairs represents a lower bound. Developing an upper bound on the number of plaintext–ciphertext pairs required for the success of of attack seems to be a hard number-theoretic problem. On the other hand, our experimental results show that three plaintext–ciphertext pairs are typically enough for the success of our attack even for large sized keys, i.e., even for large values of p.

The following example illustrates the above attack.

Example 1: Let $p = 17$, $a = 3$, and $b = 2$. For $n_1 = 8$, a possible solution for the corresponding Pell equation is $(q_{x_1}, q_{y_1}) = (1, 9)$ and hence we have $c_1 = (s_{q_1}, d_{q_1}) = (4, 2)$. For $n_2 = 6$, a possible solution for the corresponding Pell equation is $(q_{x_2}, q_{y_2}) = (8, 15)$ and hence we have $c_2 = (s_{q_2}, d_{q_2}) = (3, 11)$. For $n_3 = 5$, a possible solution for the corresponding Pell equation is $(q_{x_3}, q_{y_3}) = (16, 13)$ and hence we have $c_3 = (s_{q_3}, d_{q_3}) = (6, 5)$.

The system of equations corresponding to n_1, n_2 is given by

$$\begin{pmatrix} 6 & 0 & -2 & 0 \\ 14 & 0 & 0 & -2 \\ 0 & 2 & -16 & 0 \\ 0 & -8 & 0 & -12 \end{pmatrix} \begin{pmatrix} a^{-1} \\ b^{-1} \\ q_{x_1} \\ q_{x_2} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 2 \\ 2 \end{pmatrix}.$$

Solving the above system of equations over $\mathcal{Q}$, we get

$$\begin{pmatrix} a^{-1} \\ b^{-1} \\ q_{x_1} \\ q_{x_2} \end{pmatrix} = \begin{pmatrix} -5/138 \\ 3/23 \\ -5/46 \\ -35/138 \end{pmatrix}.$$

Similarly solving the system of equations corresponding to $n1$, $n3$ over $\mathcal{Q}$ we get

$$\begin{pmatrix} a^{-1} \\ b^{-1} \\ q_{x_1} \\ q_{x_3} \end{pmatrix} = \begin{pmatrix} -1/31 \\ 7/31 \\ -3/31 \\ -11/62 \end{pmatrix}.$$

Then p' can be recovered by calculating

$$p' = gcd(-5 \times 31 + 138, 3 \times 31 - 7 \times 23) = 17 = p.$$

Once p is recovered, a, and b can be recovered as follows:

$$a = -5^{-1} \times 138 \bmod 17 = 3 \text{ or } a = -1 \times 31 \bmod 17 = 3.$$
$$b = 3^{-1} \times 23 \bmod 17 = 2 \text{ or } b = 7^{-1} \times 31 \bmod 17 = 2.$$

III. Conclusion

The symmetric key proposed by Murthy and Swamy is insecure. Both the primary secret key and the secondary keys can be recovered using a very low complexity known plaintext attack.

Acknowledgment

The author would like to thank one of the anonymous reviewers for fixing some typographical errors in the original manuscript.

References

[1] L. E. Dickson, "Diophantine Analysis," in *History of the Theory of Numbers*. New York: Chelsea, 1952, vol. II, ch. XII, p. 341.
[2] N. R. Murthy and M. N. S. Swamy, "Cryptographic applications of Brahmagupta–Bhāskara equation," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 53, no. 7, pp. 1565–1571, Jul. 2006.
[3] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptographic Research*. Boca Raton, FL: CRC, 1996.
[4] B. Schneier, *Applied Cryptography*, 2nd ed. New York: Wiley, 1996.
[5] D. S. Mitrinovic, J. Sandor, and B. Crstici, *Handbook of Number Theory, (Mathematics and Its Applications)*. Norwell, MA: Kluwer.

Authors' Reply

N. Rama Murthy and M. N. S. Swamy

It may be observed that the cryptanalytic attack proposed by the author of [1] uses known plaintext–ciphered text pair in an iterative procedure that terminates after an indefinite number of iteration cycles. Each iteration cycle consists of the following four steps.

- Step 1) Solving a set of four linear equations over the field of rational numbers $\boldsymbol{Q}$ obtained from a pair of known plaintext–ciphered text
- Step 2) Computing the function $\gcd(\cdot,\cdot,\cdot,\ldots)$, where $\gcd$ denotes greatest common divisor of the set arguments enclosed to obtain p' (using Euclid's algorithm)
- Step 3) Primality testing of p' to check if it is a prime (and hence ensure that it is the primary secret key p) and returning to *Step* 1 with a new set of plaintext–ciphered text pair if $p\prime$ is not a prime.
- Step 4) With the knowledge of p, compute secondary keys a and b by solving a set of equations in $\mathrm{GF}(p)$

Assuming the availability of enough computational resources and time (as the steps in the above algorithm besides being complex, are sequential), the algorithm succeeds in recovering secret keys. We do not subscribe to the view expressed in [1], where it is stated that "experimental results show that only 3 plaintext–ciphertext pairs are typically enough for the success of the attack even for a large sized keys i.e., even for large values of p." In the absence of a mathematical proof

Manuscript received October 6, 2006. This paper was recommended by C.-W. Wu.

N. Rama Murthy is with the Centre for Artificial Intelligence and Robotics, Bangalore 560 001, India (e-mail: nr_murthy@hotmail.com).

M. N. S. Swamy is with the Department of Electrical and Computer Engineering, Concordia University, Montreal, QC H3G 1M8, Canada, (e-mail: swamy@ece.concordia.ca).

Digital Object Identifier 10.1109/TCSI.2006.888775