A small secret exponent attack on cryptosystems using Dickson polynomials

Akihiko Onishi[1], Yukihiro Uchida[1] and Shigenori Uchiyama[1]

[1] Tokyo Metropolitan University, 1-1 Minami-Osawa, Hachioji, Tokyo 192-0397, Japan

E-mail *onishi-akihiko@ed.tmu.ac.jp*

Received November 10, 2014, Accepted January 8, 2015

Abstract

The Dickson cryptosystem is a modification of the RSA and LUC based on the Dickson polynomial. In this paper, we consider Wiener's attack and Boneh-Durfee's algorithm on RSA to the Dickson cryptosystem. We then efficiently apply them when the secret exponent d is sufficiently small compared to public modulus n. We show that if $d < (1/3\sqrt{2})n^{0.5}$, then Wiener's attack works. Furthermore, the bound on Boneh-Durfee's algorithm is extended up to $d < n^{0.585}$.

Keywords Dickson polynomial, RSA, LLL-algorithm, small inverse problem

Research Activity Group Algorithmic Number Theory and Its Applications

1. Introduction

A classical attack, called Wiener's Attack [1], to the RSA scheme with small secret exponent uses a continued fraction. In this attack, it is shown that the prime factor of the RSA modulus n and secret exponent d can be determined in polynomial time when $d < (1/3)n^{0.25}$. Boneh and Durfee [2] improved the bound of Wiener's attack on RSA. They proposed using Coppersmith's method [3], which is based on the LLL-lattice reduction algorithm, and showed that secret exponent d can be efficiently found with given public exponent e and n when $d < n^{0.292}$. However, the analysis for this bound is complicated in general. Herrmann and May [4] proposed another simpler algorithm which used a full-rank lattice and achieved the same bound $d < n^{0.292}$.

In this paper, we apply the above attacks to the Dickson cryptosystem and analyze them. The plan of the paper is as follows: In Section 2, we recall the definition, a proposition, and method of calculation of the Dickson polynomials. In Section 3, we explain the attacks to the RSA scheme with the small secret exponent and show that these attacks can be applied to Dickson cryptosystems. Our results are summarized in Section 4.

2. The Dickson polynomials

2.1 Definition and Proposition

Definition 1 (Dickson [5]) *For $n \geq 0$, the Dickson polynomials in the indeterminate x and with parameter a are given by*

$$\begin{cases} D_0(x,a) = 2 \\ D_n(x,a) = \displaystyle\sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n}{n-i}\binom{n-i}{i}(-a)^i x^{n-2i}. \end{cases}$$

Here, $\lfloor n/2 \rfloor$ is the largest integer not greater than $n/2$. Each term $(n/n-i)\binom{n-i}{i}$ is an integer.

Dickson polynomials with parameter $a = 0$ give the power functions x^n. If $a \in \mathbb{F}_q^*$, then this polynomial in two variables induces a permutation polynomial of $\mathbb{F}_q^*$ if and only if $GCD(n, q^2 - 1) = 1$, where $\mathbb{F}_q$ denotes the finite field with q-elements. Then Waring's formula yields the following equation

$$D_n(u_1 + u_2, u_1 u_2) = u_1^n + u_2^n. \qquad (1)$$

The following three equations for the Dickson polynomials can be derived from equation (1).

Proposition 2 *Let k, l be positive integers. Then the Dickson polynomials satisfy the following recurrence relations*

$$D_{2n}(x,a) = (D_n(x,a))^2 - 2a^n, \qquad (2)$$

$$D_{2n+1}(x,a) = D_n(x,a)D_{n+1}(x,a) - a^n x, \qquad (3)$$

$$D_{kl}(x,a) = D_k(D_l(x,a), a^l). \qquad (4)$$

The recurrence relations (2), (3) lead to a fast algorithm, similar to exponentiation by the squaring method, for evaluating $D_n(x,a)$ when n, x, a are given. The recurrence relation (4) is used when decrypting Dickson cryptosystems.

2.2 The computation of Dickson polynomials

To evaluate $D_n(x,a)$, consider the following steps.

```
**Input:** $n, t \in \mathbb{N}$, $x, a \in (\mathbb{Z}/t\mathbb{Z})^*$
**Output:** $D_n(x,a) \pmod{t}$
  $n = (n_{k-1}n_{k-2}\dots n_1 n_0)_2$, $b \leftarrow a$, $(d1, d2) \leftarrow (x, x^2 - 2a)$, $k \leftarrow k - 1$
  while $k > 0$ do
    $k \leftarrow k - 1$
    if $n_k = 1$ then
      $d1 \leftarrow d1d2 - xb \pmod{t}$
      $d2 \leftarrow d2d2 - 2ab \pmod{t}$
      $b \leftarrow b^2 a \pmod{t}$
    else
```

```
            $d2 \leftarrow d1d2 - xb \pmod t$
            $d1 \leftarrow d1d1 - 2b \pmod t$
            $b \leftarrow b^2 \pmod t$
        end if
    end while
    return $d1$
```

This algorithm outputs a Dickson polynomial in time $O(\log(n))$.

2.3 Dickson cryptosystems

Here, we introduce public-key cryptosystem based on Dickson polynomials. Let n be a product of large distinct odd primes p, q. The public exponent e is chosen relatively prime to $v(n)$, where $v(n) = (p^2-1)(q^2-1)$. The secret exponent d is defined to be the multiplicative inverse of $e \pmod{v(n)}$. An integer a chosen such that a and n are coprime or $a = 0$, and let $b = a^e \bmod n$. Then a, b, n, e are published as a public key, and d is kept as a secret key.

To encrypt a message m

$$c = D_e(m, a) \bmod n.$$

To decrypt a ciphertext c

$$m = D_d(c, b) \bmod n.$$

This cryptosystem is regarded as a generalization of the RSA scheme (when $a = 0$) and LUC (when $a = 1$).

3. Small secret exponent attack

3.1 Wiener's attack

We now review Wiener's attack [1] to the RSA scheme, and analyze it to the Dickson cryptosystem. This attack requires the following classical theorem of continued fractions.

Theorem 3 ([6]) *Let x be a positive real number and a, b be coprime positive integers. If*

$$\left| x - \frac{a}{b} \right| < \frac{1}{2b^2}$$

then a/b is a convergent to x obtained by the continued fraction expansion.

Theorem 4 (Wiener [1]) *Let $n = pq$, e be published with $GCD(e, \varphi(n)) = 1$, where $\varphi(n) = (p-1)(q-1)$, and d be kept with $ed \equiv 1 \pmod{\varphi(n)}$. If $q < p < 2q$, $1 \le e < \varphi(n)$, and $d < (1/3)n^{1/4}$, then p, q, and d can be determined in polynomial time by the continued fraction expansion of e/n.*

We apply this attack to the Dickson cryptosystem.

Theorem 5 *Let $n = pq$, e be published with $GCD(e, v(n)) = 1$, where $v(n) = (p^2-1)(q^2-1)$, and d be kept with $ed \equiv 1 \pmod{v(n)}$. If $q < p < 2q$, $1 \le e < v(n)$, and $d < (1/3\sqrt{2})n^{1/2}$, then p, q, and d can be determined in polynomial time by the continued fraction expansion of $e/(n+1)^2$.*

Proof There is a positive integer k such that $ed - kv(n) = 1$. Since $e < v(n)$, we see that $k < d < (1/3\sqrt{2})n^{1/2}$. Hence, we obtain

$$\begin{aligned} \left| \frac{e}{(n+1)^2} - \frac{k}{d} \right| &< \frac{k(p+q)^2}{n^2 d} \\ &< \frac{9k}{nd} \\ &< \frac{1}{2d^2}. \end{aligned}$$

Since e, d, k are given, it follows that the prime factor of n can be found for $ed - kv(n) = 1$.

(QED)

3.2 Boneh-Durfee's algorithm

A substantial improvement to Theorem 4 was proposed by Boneh and Durfee [2], who used Coppersmith's method based on the LLL-lattice reduction algorithm. By introducing the "*small inverse problems*" which reduced to finding small roots of a bivariate modular equation, they showed that when d was less than $n^{0.292}$, then the system is insecure. However, the method of proof in [2] relies on a detailed analysis of the determinant of a lattice basis matrix. On the other hand, Herrmann and May used a related, but difficult method in [2], which simplifies the analysis of the bound. In the following, we review the necessary ideas to explain the analysis and proof on the bound given in [4]. We assume e is the same order of magnitude as n for $e < n$, and d satisfies $d < n^\delta$. We have $ed = k\varphi(n) + 1 = k(n + 1 - (p+q)) + 1$. Letting $s = -(p+q)$ and $A = n+1$, we have $k(A+s) + 1 \equiv 0 \pmod e$, where $|k| < d < n^\delta \approx e^\delta$, $|s| < 3\sqrt{n} \approx e^{1/2}$. We end up with the following problem.

Problem 6 (Boneh and Durfee [2]) *Given positive integers A and e, find the solution $(\overline{x}, \overline{y})$ satisfying*

$$f(x, y) = x(A + y) + 1 \equiv 0 \pmod e$$

where $|\overline{x}| < X = e^\delta$,$|\overline{y}| < Y = e^{1/2}$.

To find the solution, the modular equation must be transformed to an equation over $\mathbb{Z}$. In Coppersmith's method, this is possible because we can use Howgrave-Graham's lemma (as proven in [7]).

Lemma 7 (Howgrave-Graham [7]) *Let X, Y, Z be real numbers, and $h(x,y,z) \in \mathbb{Z}[x,y,z]$ be a sum of ω-monomials. Given a polynomial $h(x,y,z) = \sum_{i,j,k} a_{i,j,k} x^i y^j z^k$, we define $\|h(x,y,z)\|^2 := \sum_{i,j,k} |a_{i,j,k}|^2$. Suppose that*

- *$h(\overline{x}, \overline{y}, \overline{z}) \equiv 0 \pmod{e^m}$ for some positive integer m, where $\overline{x}$, $\overline{y}$, and $\overline{z}$ are integers such that $|\overline{x}| < X$, $|\overline{y}| < Y$, and $|\overline{z}| < Z$.*
- *$\|h(xX, yY, zZ)\| < e^m/\sqrt{\omega}$.*

Then $h(\overline{x}, \overline{y}, \overline{z}) = 0$ holds over the integers.

To configure the lattice for easier analysis, Herrmann and May introduced a concept called the "*unravelled linearization technique*". They defined a polynomial sequence, where the indexing is different from Boneh-Durfee's.

Definition 8 (Herrmann and May [4]) *Let m be a positive integer. For $0 \le k \le m$, $0 \le i \le m-k$, $1 \le j \le$*

Table 1. Herrmann and May basis matrix for $m = 2, \tau = 1/2$.

	1	X	Z	X^2	XZ	Z^2	YZ^2
$g_{0,0}$	e^2	0	0	0	0	0	0
$g_{1,0}$	0	e^2X	0	0	0	0	0
$g_{0,1}$	0	AeX	eZ	0	0	0	0
$g_{2,0}$	0	0	0	e^2X^2	0	0	0
$g_{1,1}$	0	0	0	AeX^2	eXZ	0	0
$g_{0,2}$	0	0	0	A^2X^2	$2AXZ$	Z^2	0
$h_{1,2}$	0	$-A^2X$	$-2AZ$	0	A^2XZ	$2AZ^2$	YZ^2

τk define $g_{i,k}$ and $h_{j,k}$ by

$$g_{i,k}(x,z) = x^i f(x,z)^k e^{m-k},$$

$$h_{j,k}(x,y,z) = y^j f(x,z)^k e^{m-k}$$

where $z = xy+1$, and the parameter τ will be determined later.

They also refer to the polynomials $g_{i,k}$ as x-shifts, and the polynomials $h_{j,k}$ as y-shifts. In their analysis, the first step is to perform a linearization of $f(x,y)$ into $f(x,y) = z + Ax$, where $z = xy + 1$. Second, xy is replaced by $z - 1$ for each occurrence of xy. x-shifts are eventually bivariate polynomials in x and z. Third, a lattice basis is constructed by using coefficient vectors of x-shifts $g_{i,k}(xX, zZ)$ and y-shifts $h_{j,k}(xX, yY, zZ)$. Table 1 shows an example for the parameters $m = 2$, $\tau = 1/2$. Since the lattice basis matrix B is triangular for any m, the analysis of its determinant is easy. From Howgrave-Graham's lemma, the problem can be efficiently solved when $\det(B) < e^{m\omega}$, where ω is the lattice dimension, by ignoring small terms. Here, they use LLL to satisfy this bound on $\det(B)$. Further, solution $(k, -(p+q))$ is obtained by using two short vectors, which are output results. Consequently, Herrmann and May proved the same result (that $d < n^{0.292}$) as Boneh and Durfee.

Next, in order to apply this algorithm to Dickson cryptosystems, the coefficients and the upper bound of the solution of the *small inverse problems* are redefined as $A = (n+1)^2$ and $|\overline{x}| < X = e^{\delta/2}$, $|\overline{y}| < Y = e^{1/2}$, respectively, from the equation $ed - kv(n) = 1$. The following theorem is then obtained.

Theorem 9 *Let $n = pq$, e be published with $GCD(e, v(n)) = 1$, where $v(n) = (p^2-1)(q^2-1)$, and d be kept with $ed \equiv 1 \pmod{v(n)}$, and k with $ed - kv(n) = 1$. Then d can be efficiently found by using Boneh-Durfee's algorithm based on Herrmann and May's basis when $d < n^\delta = n^{0.585}$.*

Proof We have to find the solution $(\overline{x}, \overline{y})$ such that $f(x,y) = x(A+y) + 1 \equiv 0 \pmod{e}$, where $|\overline{x}| < X = e^{\delta/2}$, $|\overline{y}| < Y = e^{1/2}$, and $A = (n+1)^2$. Note that we consider the bound X and Y for a solution $(\overline{x}, \overline{y}) = (k, -(p+q)^2)$ with $k < d < n^\delta$, $e < n^2$. We analyze the determinant of the lattice basis matrix B which is constructed by Boneh-Durfee's algorithm. If we ignore the small term, the following values are obtained

$$\det(B) = e^{(1/3+\tau/6)m^3} X^{(1/6)m^3} Y^{(\tau^2/6)m^3} Z^{(1/6+\tau/3)m^3}.$$

To satisfy $\det(B) < e^{m\omega}$, we perform optimization of the parameter τ for arbitrary m. Hence we obtain $\delta < 2 - \sqrt{2} \approx 0.585$ when $\tau = \sqrt{2} - 1$.

(QED)

4. Conclusion

In this paper, we discussed the effect of Wiener's attack and Boneh-Durfee's algorithm for the Dickson cryptosystem. It is shown that the private exponent d can be calculated efficiently if d is smaller than $(1/3\sqrt{2})n^{1/2}$ by applying Wiener's results for the Dickson cryptosystem. Further, it is possible to improve the bound on the Dickson cryptosystem to $n^{0.585}$ by Boneh-Durfee's algorithm.

Further work includes:

- more analysis to exceed the bound $d < n^{0.585}$ by configuring the optimal lattice basis matrix for the Dickson cryptosystem.
- application of general results for the RSA scheme when the knowledge of a few significant bits of p is given.

Acknowledgments

The authors would like to thank the anonymous reviewer for his/her valuable comments, and would also like to thank Stefan Horocholyn at Tokyo Metropolitan University for his helpful comments on the manuscript. This work was supported by Grant-in-Aid for Scientific Research (C) (24540135) and Grant-in-Aid for Young Scientists (B) (25800023).

References

[1] M. J. Wiener, Cryptanalysis of short RSA secret exponents, IEEE Trans. Inform. Theory, **36** (1990), 553–558.

[2] D. Boneh and G. Durfee, Cryptanalysis of RSA with private key d less than $N^{0.292}$, in: Proc. of EUROCRYPT' 99, LNCS, Vol. 1592, pp. 1–11, Springer-Verlag, Berlin, 1999.

[3] D. Coppersmith, Finding a small root of a univariate modular equation, in: Proc. of EUROCRYPT' 96, LNCS, Vol. 1070, pp. 155–165, Springer-Verlag, Berlin, 1996.

[4] M. Herrmann and A. May, Maximizing small roots bounds by linearization and applications to small secret exponent RSA, in: Proc. of PKC2010, LNCS, Vol. 6056, pp. 53–69, Springer-Verlag, Berlin, 2010.

[5] R. Lidl, G. L. Mullen and G. Turnwald, Dickson polynomials, Longman Scientific and Technical, New York, 1993.

[6] G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, 5th ed., Oxford University Press, Oxford, 1979.

[7] N. Howgrave-Graham, Finding small roots of univariate modular equations revisited, in: Proc. of 6th IMA Int. Conf., LNCS, Vol. 1355, pp. 131–142, Springer-Verlag, Berlin, 1997.