Rupert Nöbauer

Cryptanalysis of a public-key cryptosystem based on Dickson-polynomials

Mathematica Slovaca, Vol. 38 (1988), No. 4, 309--323

Persistent URL: http://dml.cz/dmlcz/129130

Math. Slovaca 38, 1988, No. 4, 309—323

CRYPTANALYSIS OF A PUBLIC-KEY CRYPTOSYSTEM BASED ON DICKSON-POLYNOMIALS

RUPERT NÖBAUER[1]

1. Introduction

One of the most important public-key cryptosystems (PKC) is undoubtedly the RSA-scheme (cf. [14]). In this cryptosystem, the plaintext alphabet and the code alphabet are given by $Z/(n)$, the ring of residue classes of the integers Z modulo a natural number n, and the family of encryption functions is given by the group of power permutations $x \to x^k$ of $Z/(n)$. Variants of the RSA-scheme are obtained if the group of power permutations of $Z/(n)$ is replaced by other permutation groups of $Z/(n)$ induced by polynomials or rational functions. So far, three PKCs of this kind have been proposed. The first one (cf. [3], [10]) is based on a class of rational functions which has been introduced by L. Rédei in [13], and the second and third one (cf. [6]) are based on the so-called Dickson-polynomials $g_k(a, x)$ with parameter $a = 1$ or $a = -1$, respectively.

The PKC based on the Rédei-functions has been cryptanalysed in [8], and a cryptanalysis of the PKC based on the Dickson-polynomials with $a = 1$ can be found in [5]. The aim of this paper is to perform a cryptanalysis of the third one of the proposed variants of the RSA-scheme. Having outlined the algebraic background and having given a short description of the scheme, we discuss several possibilities for a cryptanalytic attack, and we formulate requirements to the key parameters which guarantee the system to be secure from the described attacks.

2. Algebraic background

Let a be an integer. The Dickson-polynomial $g_k(a, x) \in Z[x]$ of degree k is given by

[1] The work presented in this paper was supported by the Österreichische Fonds zur Förderung der Wissenschaftlichen Forschung under FWF-Project No. P 5452.

Key words: public-key cryptosystems, cryptanalysis, Dickson-polynomials, fixed points, superencryption.

$$g_k(a,x) = \sum_{t=0}^{[k/2]} \frac{k}{k-t}\binom{k-t}{t}(-a)^t x^{k-2t},$$

where $[k/2]$ denotes the greatest integer $t \leqq k/2$. In $Q(y)$, the field of rational functions over the field Q of rational numbers, the following formula holds (cf. [12]):

$$g_k\left(a, y + \frac{a}{y}\right) = y^k + \left(\frac{a}{y}\right)^k. \tag{1}$$

Since for every $b \in Q$ the equation $u + \dfrac{a}{u} = b$ has solutions u_1, u_2 in a quadratic extension field of Q, we obtain:

$$g_k(a^l, g_l(a,b)) = g_k\left(a^l, u_1^l + \left(\frac{a}{u_1}\right)^l\right) = u_1^{kl} + \left(\frac{a}{u_1}\right)^{kl} =$$

$$= g_{kl}\left(a, u_1 + \frac{a}{u_1}\right) = g_{kl}(a,b). \tag{2}$$

Therefore, if $\circ$ denotes the composition of polynomials, the polynomials $g_k(a^l,x) \circ g_l(a,x)$ and $g_{kl}(a,x)$ have the same function values for infinitely many numbers $b \in Q$, and consequently in $Z[x]$ the functional equation

$$g_k(a^l,x) \circ g_l(a,x) = g_{kl}(a,x) \tag{3}$$

holds.

In this paper we restrict ourselves to the case $a = -1$, and we write $g_k(-1,x) = g_k(x)$. From (3) we obtain $g_k(x) \circ g_l(x) = g_{kl}(x)$ for odd natural numbers k and l.

In the following we write $[a_1, \ldots, a_r]$ for the least common multiple and $(a_1, \ldots, a_r)$ for the greatest common divisor of the integers $a_1, \ldots, a_r$. Let n be a natural number with the prime factorization $n = \prod_{i=1}^{r} p_i^{e_i}$, and let $v(n)$ be given by

$$v(n) = [p_1^{e_1-1}(p_1^2-1), \ldots, p_r^{e_r-1}(p_r^2-1)].$$

In [11] it is proved that the mapping $x \to g_k(x) \bmod n$ is a permutation of $Z/(n)$ if and only if $(k, v(n)) = 1$.

The set $D(n)$ of all Dickson-permutations $x \to g_k(x) \bmod n$ forms a semigroup under composition. Indeed, let the permutations π and ϱ be induced by $g_k(x)$ and $g_l(x)$. Then $\pi \circ \varrho$ is induced by $g_k(x) \circ g_l(x)$. In the case $n > 2$, the number $v(n)$ is even, hence k and l are odd, and therefore we have $g_k(x) \circ g_l(x) = g_{kl}(x)$. In the case $n = 2$ we have $1 = -1$, hence $g_k(x) = g_k(-1,x) = g_k(1,x)$, and therefore by (3) again we have $g_k(x) \circ g_l(x) = g_{kl}(x)$. Thus we have proved: The permutation $\pi \circ \varrho$ is induced by $g_{kl}(x)$.

As subsemigroup of the full permutation group of $Z/(n)$, the semigroup $D(n)$ is regular and finite, and therefore it is even a group. This implies that the inverse of a Dickson-permutation $\pi \in D(n)$ is itself a Dickson-permutation $\varrho \in D(n)$. In [4] the following result is proved: If $\pi \in D(n)$ is induced by $g_k(x)$ and if l is a natural number with $kl \equiv 1 \bmod v(n)$, then π^{-1} is induced by $g_l(x)$. Hence, if the factorization of n is known, it is easy to compute the inverse of a Dickson-permutation $x \to g_k(x) \bmod n$. On the other hand, no algorithms are known allowing to invert Dickson-permutations $x \to g_k(x) \bmod n$ if the factorization of n is unknown. Therefore, exactly like in the RSA-scheme, the trapdoor information of PKCs based on Dickson-polynomials is given by the factorization of the modulus n of the plaintext alphabet $Z/(n)$.

3. A fast evaluation algorithm

Since messages $m \in Z/(n)$ are encrypted by $m \to g_k(m) \bmod n$, we need a fast evaluation algorithm allowing to calculate function values of the Dickson polynomials $g_k(x) \bmod n$. In the following we describe an algorithm of complexity $O(\mathrm{ld}\,(k))$ (cf. also [9]), where $\mathrm{ld}\,(k)$ is the logarithm dualis of k.

Given $b \in Z/(n)$, we want to compute $g_k(b) \bmod n$. For doing this, we have to solve

$$u - \frac{1}{u} = b, \tag{4}$$

or equivalently

$$u^2 - bu - 1 = 0, \tag{5}$$

in some extension ring of $Z/(n)$. As can be seen easily, the factor ring $R_b = Z/(n)[u]/(u^2 - bu - 1)$ is an extension ring of $Z/(n)$, and every element $s \in R_b$ can be represented uniquely in the form

$$s = a_1 u + a_0, \qquad a_0, a_1 \in Z/(n).$$

Multiplication in R_b can be implemented by using the formula

$$(a_1 u + a_0)(b_1 u + b_0) = (a_1 b_0 + a_0 b_1 + a_1 b_1 b)\, u + a_0 b_0 + a_1 b_1. \tag{6}$$

By definition of R_b, the element $u \in R_b$ is a solution of (5). Since $u(u - b) = 1$, u is always invetible.

For the evaluation of $g_k(b)$ just calculate the power u^k in the ring R_b by using the "square- and multiply-technique": That is, first compute

$$u, u^2, (u^2)^2, \ldots,$$

and then multiply together the appropriate factors, thus finding elements a_0, $a_1 \in Z/(n)$ with

$$u^k = a_1 u + a_0.$$

Since $\dfrac{-1}{u}$ also satisfies (5), the equation

$$\left(\frac{-1}{u}\right)^k = \frac{-a_1}{u} + a_0$$

holds, and therefore by (1)

$$g_k(b) = g_k\left(u - \frac{1}{u}\right) = u^k + \left(\frac{-1}{u}\right)^k = a_1\left(u + \frac{-1}{u}\right) + 2a_0 = a_1 b + 2a_0.$$

We summarize our procedure in the following

Algorithm 1.

Input	n, k, b.
Compute	$a_0, a_1 \in Z/(n)$ *with* $u^k \equiv a_1 u + a_0 \bmod u^2 - bu - 1$.
	Comment [*use the square- and multiply-technique*].
Compute	$g_k(b) \equiv a_1 b + 2a_0 \bmod n$.
End.	

4. The public-key cryptosystem

Every participant C of the communication network chooses a positive integer $r = r_C$, r prime powers $p_i^{e_i}$, and an encryption key $k = k_C$ with $(k, p_i^{e_i - 1}(p_i^2 - 1)) = 1$ for $i = 1, 2, \ldots, r$. Then C calculates the numbers $n = n_C = \prod_{i=1}^{r} p_i^{e_i}$, $v(n) = [p_1^{e_1 - 1}(p_1^2 - 1), \ldots, p_r^{e_r - 1}(p_r^2 - 1)]$, and computes a decryption key $l = l_C$, that is a natural number l satisfying the linear congruence

$$kl \equiv 1 \bmod v(n). \tag{7}$$

The public key of C consists of the parameters n and k, and the secret key is given by the prime factorization of n and by l.

If A intends to send the secret message $m \in Z/(n_B)$ to B, he has to encrypt m

by calculating $c \equiv g_{k_B}(m) \bmod n_B$, and then he sends c to B. The receiver B decrypts c by calculating $g_{l_B}(c) \equiv g_{l_B}(g_{k_B}(m) \equiv m \bmod n_B$.

5. Cryptanalysis

Since unlike to B a spy does not know the factorization of n_B, he cannot compute a decryption key l_B in the same way as B does. However, he might try to use other methods of decryption, especially to do partial decryption, that is to decrypt certain ciphertexts without knowing the decryption key l_B.

In the following we discuss several procedures of partial decryption. We show that in some cases these attacks can be used also for factoring n. All discussed attacks are analogues to well-known attacks on the RSA-scheme (cf. Schnorr [16], Simmons and Norris [17], Berkowitz [1], Herlestam [2], Rivest [14]). We restrict ourselves to the cryptographically most important case, where n is the product of two distinct odd prime numbers, that is $n = p_1 p_2$. We show that the PKC is secure from the described attacks if $p_i - 1$ $(i = 1, 2)$ contains a large prime factor p_i', if $p_i + 1$ $(i = 1, 2)$ contains a large prime factor p_i^* and if the order of $k \bmod p_i'$ as well as the order of $k \bmod p_i^*$ $(i = 1, 2)$ is large. These requirements are fulfilled if, e.g., for $i = 1, 2$

$$\begin{cases} p_i - 1 = a_i p_i', & a_i < 10^5, \quad p_i' > 10^{80}, \\ p_i + 1 = b_i p_i^*, & b_i < 10^5, \quad p_i^* > 10^{80}, \end{cases} \tag{8}$$

$$\begin{cases} \operatorname{ord}_{p_i'}(k) > 10^{11}, \\ \operatorname{ord}_{p_i^*}(k) > 10^{11}. \end{cases} \tag{9}$$

5.1. Attacks by means of numbers s such that $g_s(c) \bmod n$ satisfies a given equation

5.1.1. Partial decryption

Let $c \in Z/(n)$ be a given ciphertext. Suppose, the cryptanalyst succeeds in finding a natural number s such that one of the following three conditions is satisfied:

$$g_s(c)^2 \equiv 0 \bmod n, \tag{10a}$$

$$g_s(c)^2 \equiv 4 \bmod n, \qquad s \text{ even} \tag{10b}$$

$$g_s(c)^2 \equiv -4 \bmod n, \quad s \text{ odd}. \tag{10c}$$

Let $s = s_1 s_2$, where s_1 contains all those prime factors of s which divide k, and s_2 contains the remaining prime factors. The numbers s_1 and s_2 can be computed without the knowledge of the prime factorization of s by using the following

Algorithm 2.

Input $\quad k, s.$

Initialize $\quad s_1 = 1;\ s_2 = s.$

While $\quad (s_2, k) > 1$ do $s_1 = s_1(s_2, k);\ s_2 = \dfrac{s_2}{(s_2, k)}.$

End.

Let $u_i \in \mathrm{GF}(p_i^2)$, $i = 1, 2$, be solutions of $u - \dfrac{1}{u} = c$. (Such solutions always exist.) If condition (10a) holds, then $g_s(c)^2 \equiv 0 \bmod p_i$ for $i = 1, 2$, hence $g_s(c) \equiv 0 \bmod p_i$, $i = 1, 2$, and using (1) it follows that in $\mathrm{GF}(p_i^2)$ the equation $g_s(c) = g_s\left(u_i - \dfrac{1}{u_i}\right) = u_i^s + \left(\dfrac{-1}{u_i}\right)^s = 0$ holds. This is equivalent to $u_i^{2s} = -(-1)^s$, which implies $u_i^{4s} = 1$. If condition (10b) holds, then $g_s(c)^2 \equiv 4 \bmod p_i$ for $i = 1, 2$, hence $g_s(c)^2 = \left(u_i^s + \left(\dfrac{-1}{u_i}\right)^s\right)^2 = 4$, $i = 1, 2$, and therefore $u_i^s + \dfrac{1}{u_i^s} = \pm 2$. This is equivalent to $(u_i^s \mp 1) = 0$, and we obtain $u_i^s = \pm 1$, which implies $u_i^{4s} = 1$. If condition (10c) holds, then $g_s(c)^2 \equiv -4 \bmod p_i$ for $i = 1, 2$, and since -4 is a square $\bmod p_i$ iff -1 is a square $\bmod p_i$, it follows that $p_i \equiv 1 \bmod 4$, $i = 1, 2$. If $f_i \in Z/(p_i)$ is such that $f_i^2 \equiv -1 \bmod p_i$, we have $g_s(c) = \pm 2 f_i$. From (1) we obtain $g_s(c) = u_i^s - \dfrac{1}{u_i^s} = \pm 2 f_i$ in $\mathrm{GF}(p_i^2)$, hence $u_i^{2s} \mp 2 f_i u_i^s - 1 = 0$, therefore $(u_i^s \mp f_i)^2 = 0$, and finally $u_i^s = \pm f_i$, which again implies $u_i^{4s} = 1$.

Thus we have proved: If one of the conditions (10a), (10b) and (10c) is fulfilled, and if $u_i \in \mathrm{GF}(p_i^2)$ is a solution of $u - \dfrac{1}{u} = c$, then there holds $u_i^{4s} = 1$, and consequently $u_i^{4 s_1 s_2} = 1$. Let o_i be the order of u_i in $\mathrm{GF}(p_i^2)^*$, the multiplicative group of $\mathrm{GF}(p_i^2)$. Since $(k, p_i^2 - 1) = 1$, we have also $(s_1, p_i^2 - 1) = 1$, and since $o_i | p_i^2 - 1$, there holds

$$(s_1, o_i) = 1. \tag{11}$$

From $u_i^{4 s_1 s_2} = 1$ we get $o_i | 4 s_1 s_2$, hence $o_i | 4 s_2$ by (11), and therefore $u_i^{4 s_2} = 1$. Since by assumption p_i is odd, the number $p_i^2 - 1$ is even, and from $(k, p_i^2 - 1) = 1$ we obtain $(k, 2) = 1$. Further, by definition of s_2 we have $(k, s_2) = 1$. Together this yields $(k, 4s_2) = 1$, and consequently there exists an odd natural number $\bar{k}$ such that $k\bar{k} \equiv 1 \bmod 4s_2$. Suppose that $k\bar{k} = 4s_2 r + 1$.

If $m \equiv g_k^{-1}(c) \equiv g_l(c) \bmod n$ is the plaintext corresponding to c, then the equation $m = g_l(c) = g_l\left(u_i - \frac{1}{u_i}\right) = u_i^l + \left(\frac{-1}{u_i}\right)^l$ holds in $GF(p_i^2)$ for $i = 1, 2$. Therefore we have

$$g_{\bar{k}}(c) = g_{\bar{k}}(g_k(m)) = g_{\bar{k}k}(m) = g_{\bar{k}k}\left(u_i^l + \left(\frac{-1}{u_i}\right)^l\right) =$$

$$= u_i^{l\bar{k}k} + \left(\frac{-1}{u_i}\right)^{l\bar{k}k} = u_i^{l4s_2r + l} + \left(\frac{-1}{u_i}\right)^{l4s_2r + l} = u_i^l + \left(\frac{-1}{u_i}\right)^l = m$$

in $GF(p_i^2)$. By the Chinese remainder theorem we obtain $g_{\bar{k}}(c) \equiv m \bmod n$.

If we assume that the search of an s such that (10a) or (10b) or (10c) holds is done by trial and error, and more concretely by testing all s between 1 and 10^5, we can summarize our attack in the following

Algorithm 3 (*Deciphering the cryptogram* $c \in Z/(n)$).

Input $\quad n, k, c.$
Initialize $\quad s = 0.$
Repeat $\quad s = s + 1$ until
$\quad g_s(c)^2 \equiv 0 \bmod n$ or
$\quad (g_s(c)^2 \equiv 4 \bmod n$ and s *even*) or
$\quad (g_s(c)^2 \equiv -4 \bmod n$ and s *odd*) or
$\quad s > 10^5.$
If $s > 10^5$, then stop; comment [*algorithm unsuccessful*].
Else
  Compute $s = s_1 s_2$, *where* s_1 *contains all those prime factors of* s *which divide* k, *and* s_2 *contains the remaining prime factors of* s; comment [*use algorithm* 2].
  Compute *a natural number* $\bar{k}$ *such that* $k\bar{k} \equiv 1 \bmod 4s_2$.
  Decipher c *by calculating* $g_{\bar{k}}(c) \equiv m \bmod n$.
Endif.
End.

Now we will show that the PKC is secure from attack 5.1.1. if the key parameters satisfy (8). In the following let i, $1 \leqq i \leqq 2$, be fixed. We consider the p_i equations $z - \frac{1}{z} = \varrho$, $\varrho \in GF(p_i)$, or equivalently, the p_i quadratic equations

$$z^2 - \varrho z - 1 = 0, \qquad \varrho \in GF(p_i). \tag{12}$$

Each of these equations has two eventually coincident solutions $u, v \in \mathrm{GF}(p_i^2)$. Let M_i be the set of all those elements of $\mathrm{GF}(p_i^2)$ which are solutions of any of the equations (12). If $u \in \mathrm{GF}(p_i)$ and $u \neq 0$, then $u - \frac{1}{u} = \varrho \in \mathrm{GF}(p_i)$ hence $u \in M_i$. Now let $u \in M_i$ and $u \notin \mathrm{GF}(p_i)$. Then u solves one of the equations (12). Since $\delta \to \delta^{p_i}$ is an automorphism of $\mathrm{GF}(p_i^2)$ that fixes the elements of $\mathrm{GF}(p_i)$, this equation is also fulfilled by $u^{p_i} \neq u$, and therefore we have $u^{p_i+1} = -1$. Conversely, if $u^{p_i+1} = -1$, then $u - \frac{1}{u} = u + u^{p_i} = \varrho \in \mathrm{GF}(p_i)$, hence $u \in M_i$. Thus we have proved (cf. also [12])

$$M_i = \{u \in \mathrm{GF}(p_i^2)\colon u^{p_i-1} = 1\} \cup \{u \in \mathrm{GF}(p_i^2)\colon u^{p_i+1} = -1\}.$$

Let ω_i be a generator of $\mathrm{GF}(p_i^2)^*$, and let $t_i = \omega_i^{(p_i-1)/2}$. We have $t_i^{p_i+1} = \omega_i^{(p_i^2-1)/2} = -1$. Moreover, we define two subgroups K_i, L_i of $\mathrm{GF}(p_i^2)^*$ by $K_i = \{\omega_i^{(p_i+1)r}\colon r = 0, 1, \ldots, p_i - 2\}$ and $L_i = \{\omega_i^{(p_i-1)s}\colon s = 0, 1, \ldots, p_i\}$. From $K_i = \{u \in \mathrm{GF}(p_i^2)\colon u^{p_i-1} = 1\}$ and $L_i = \{u \in \mathrm{GF}(p_i^2)\colon u^{p_i+1} = 1\}$ it follows that $K_i = \mathrm{GF}(p_i)^*$ and $M_i = K_i \cup t_iL_i$. If $u \in \mathrm{GF}(p_i^2)$ solves one of the equations (12), then $-\frac{1}{u}$ solves this equation, too. With $u \in K_i$ also $-\frac{1}{u} \in K_i$, and with $u \in t_iL_i$ also $-\frac{1}{u} \in t_iL_i$. We have $u = -\frac{1}{u}$ if and only if $u^2 = -1$, and all solutions of $z^2 = -1$ in $\mathrm{GF}(p_i^2)$ are given by $f_i = \omega_i^{(p_i^2-1)/4}$ and $-f_i = \omega_i^{3(p_i^2-1)/4}$. The element f_i is contained in $K_i \cup t_iL_i$, iff f_i solves one of the equations (12), that is iff $f_i - \frac{1}{f_i} \in \mathrm{GF}(p_i)$. Because of $-\frac{1}{f_i} = f_i$ this is equivalent to $2f_i \in \mathrm{GF}(p_i)$. Since by assumption p_i is odd, this holds if and only if $f_i \in \mathrm{GF}(p_i)$, hence if and only if the equation $z^2 = -1$ is solvable in $\mathrm{GF}(p_i)$, and consequently if and only if $p_i \equiv 1 \bmod 4$.

If $p_i \equiv 1 \bmod 4$, then $(\pm f_i)^{p_i-1} = 1$ and $(\pm f_i)^{p_i+1} = -1$, and therefore $\pm f_i \in K_i \cap t_iL_i$. On the other hand, if $u \in K_i \cap tL_i$, then $u^{p_i-1} = 1$ and $u^{p_i+1} = -1$, and therefore $u^2 = -1$. This implies that for $p_i \equiv 1 \bmod 4$ we have $K_i \cap tL_i = \{f_i, -f_i\}$, and for $p_i \equiv 3 \bmod 4$ we have $K_i \cap t_iL_i = \{\ \}$.

So far we have proved: For $p_i \equiv 1 \bmod 4$, $\varrho \neq \pm 2f_i$, and for $p_i \equiv 3 \bmod 4$, the equations (12) have exactly two solutions u, $-\frac{1}{u} \in \mathrm{Gf}(p_i^2)$, which are either both elements of K_i or of t_iL_i. For $p_i \equiv 1 \bmod 4$, $\varrho = \pm 2f_i$, these equations have exactly one solution in $\mathrm{GF}(p_i^2)$, namely $u = f_i$ or $u = -f_i$ respectively, and this solution is an element of $K_i \cap t_i L_i$.

We introduce another subgroup of $\mathrm{GF}(p_i^2)^*$ by $R_i = L_i \cup t_i L_i$. Obviously, $R_i = \{u \in \mathrm{GF}(p_i^2): u^{2(p_i+1)} = 1\} = \{\omega_i^{r(p_i-1)/2}: r = 0, 1, \ldots, 2p_i + 1\}$. The groups K_i, L_i and R_i are cyclic, and by (8), the orders of these groups are given by $|K_i| = p_i - 1 = a_i p_i'$, $|L_i| = p_i + 1 = b_i p_i^*$ and by $|R_i| = 2|L_i| = 2b_i p_i^*$. If $u \in K_i$, then $\mathrm{ord}(u) \leqq 4.10^5$ holds if and only if $\mathrm{ord}(u) | a_i$. If $d | a_i$, then the number of elements $u \in K_i$ with $\mathrm{ord}(u) = d$ is given by $\varphi(d)$, and therefore the number of elements $u \in K_i$ with $\mathrm{ord}(u) \leqq 4 \cdot 10^5$ is given by $\sum_{d|a_i} \varphi(d) = a_i$. Thus we have proved

$$|\{u \in K_i: \mathrm{ord}(u) \leqq 4 \cdot 10^5\}| = a_i. \tag{13}$$

Similarly, we obtain $|\{u \in t_i L_i: \mathrm{ord}(u) \leqq 4 \cdot 10^5\}| = |\{u \in R_i: \mathrm{ord}(u) \leqq 4 \cdot 10^5\}| - - |\{u \in L_i: \mathrm{ord}(u) \leqq 4 \cdot 10^5\}| = 2b_i - b_i$, and therefore

$$|\{u \in t_i L_i: \mathrm{ord}(u) \leqq 4 \cdot 10^5\}| = b_i. \tag{14}$$

For a given ciphertext $c \in Z/(n)$, algorithm 3 is successful if and only if there exists an s with $1 \leqq s \leqq 10^5$ such that one of the conditions (10a), (10b) and (10c) is satisfied. For $i = 1, 2$, let $u_i \in K_i \cup t_i L_i$ be a solution of $z - \frac{1}{z} = c$. We have proved above that each of the conditions (10a), (10b) and (10c) implies $u_i^{4s} = 1$, $i = 1, 2$. Hence, if there exists an s with $1 \leqq s \leqq 10^5$ such that (10a), (10b) or (10c) holds, then $\mathrm{ord}(u_i) \leqq 4 \cdot 10^5$. From what we have proved about the solutions of $z - \frac{1}{z} = c$ in $\mathrm{GF}(p_i^2)$, $i = 1, 2$, and from (13) and (14) it follows that

$$\begin{gathered}|\{c \in Z/(n): \exists s \textit{ with } 1 \leqq s \leqq 10^5 \textit{ such that one of the conditions}\\ (10\mathrm{a}), (10\mathrm{b}) \textit{ and } (10\mathrm{c}) \textit{ is satisfied}\}| \leqq\end{gathered}$$

$$\leqq \prod_{i=1}^{2} \left[\frac{1}{2}\left|\{u \in K_i: \mathrm{ord}(u) \leqq 4 \cdot 10^5\}\right| + \frac{1}{2}\left|\{u \in t_i L_i: \mathrm{ord}(u) \leqq 4 \cdot 10^5\}\right|\right] =$$

$$= \frac{1}{4} \prod_{i=1}^{2} (a_i + b_i) < 10^{10}.$$

Therefore, if condition (8) holds and if c is uniformly distributed on $Z/(n)$, then the probability that c can be decrypted by algorithm 3 is bounded by $10^{10}/10^{160} = 10^{-150}$.

5.1.2. Factoring of n

A special case of attack 5.1.1. is given if the cryptanalyst succeeds in finding an even natural number s with $g_s(c) \equiv 2 \bmod n$. Frequently, knowing such an s not only allows to decipher c, but also to factorize n.

For the following considerations we put $\nu_2(s) = \max\{e \in N : 2^e | s\}$. Suppose that the cryptanalyst knows an even s such that $g_s(c) \equiv 2 \bmod n$. For $i = 1, 2$ let $u_i \in \mathrm{CF}(p_i^2)$ be a solution of $u - \frac{1}{u} = c$. Then in $\mathrm{GF}(p_i^2)$ we have $u_i^s + \frac{1}{u_i^s} = 2$, and therefore $u_i^s = 1$, $i = 1, 2$. Let $j := \max\{r \in \{0, 1, \ldots, \nu_2(s) - 1\} : u_i^{s/2^r} = 1, i = 1, 2\} = \max\{r \in \{0, 1, \ldots, \nu_2(s) - 1\} : g_{s/2^r}(c) \equiv 2 \bmod n\}$. Since the equation $x^2 = 1$ has just the two solutions 1 and -1 in the cyclic group $\mathrm{GF}(p_i^2)^*$, $i = 1, 2$, one of the following four cases holds:

(i) $j = \nu_2(s) - 1$

(ii) $j < \nu_2(s) - 1$, $\quad u_1^{s/2^{j+1}} = 1$, $\quad u_2^{s/2^{j+1}} = -1$

(iii) $j < \nu_2(s) - 1$, $\quad u_1^{s/2^{j+1}} = -1$, $\quad u_2^{s/2^{j+1}} = 1$

(iv) $j < \nu_2(s) - 1$, $\quad u_1^{s/2^{j+1}} = -1$, $\quad u_2^{s/2^{j+1}} = -1$.

Case (i) is equivalent to $g_{s/2^{\nu_2(s)-1}}(c) \equiv 2 \bmod n$, case (iv) is equivalent to $g_{s/2^{j+1}}(c) \equiv -2 \bmod n$, and in these cases our procedure does not provide the factorization of n. If case (ii) holds, then $g_{s/2^{j+1}}(c) \equiv 2 \bmod p_1$ and $g_{s/2^{j+1}}(c) \not\equiv 2 \bmod p_2$, and therefore $(g_{s/2^{j+1}}(c) - 2, n) = p_1$. Similarly, in case (iii) there holds $(g_{s/2^{j+1}}(c) - 2, n) = p_2$.

If we assume that searching for an s such that $g_s(c) \equiv 2 \bmod n$ is done by testing all even s between 1 and 10^5, we can summarize the attack in the following

Algorithm 4.
Input $\quad n, c.$
Initialize $\quad s = 0.$
100 Repeat $\quad s = s + 2$ until $g_s(c) \equiv 2 \bmod n$ or $s > 10^5$.
If $\quad s > 10^5$ stop; comment [*algorithm unsuccessful*]
Compute $\quad \nu_2(s)$.
Compute $\quad j = \max\{r \in \{0, 1, \ldots, \nu_2(s) - 1\} : g_{s/2^r} \equiv 2 \bmod n\}$.
If $\quad j = \nu_2(s) - 1$, then goto 100; comment [*case* (i); *test next s*].
Else if $g_{s/2^{j+1}}(c) \equiv -2 \bmod n$ goto 100; comment [*case* (iv); *test next s*].
Else compute $d = (g_{s/2^{j+1}}(c) - 2, n)$; comment [*d is a nontrivial factor of n*].

Endif;
End.

Since algorithm 4 is successful only with ciphertexts c which can be decrypted by algorithm 3, this algorithm does not represent a real threat to our PKC: If condition (8) holds and if c is uniformly distributed on $Z/(n)$, then the probability that algorithm 4 provides a nontrivial factor of n is bounded by 10^{-150}.

5.2. Factoring by means of fixed points

Let s be an d natural number, and let c be a fixed point of $g_s(x) \bmod n$ with $(c^2+4, n) = 1$. Clearly c is also a fixed point of $g_s(x) \bmod p_i$ for $i = 1, 2$. Let $u_i \in \mathrm{GF}(p_i^2)$ be a solution of $u - \frac{1}{u} = c$, $i = 1$, 2. Then we have $g_s\left(u_i - \frac{1}{u_i}\right) = u_i^s - \frac{1}{u_i^s} = u_i - \frac{1}{u_i}$, hence $(u_i^{s+1}+1)(u_i^{s-1}-1) = 0$, and therefore for $i = 1$, 2 one of the equations $u_i^{s+1} = -1$ and $u_i^{s-1} = 1$ holds. If for an i, $1 \leqq i \leqq 2$, both equations hold, then $u_i^2 = -1$, hence $u_i = -\frac{1}{u_i}$, therefore $c = u_i - \frac{1}{u_i} = u_i + u_i = 2u_i$, and consequently $c^2 = 4u_i^2 = -4 \bmod p_i$, which yields a contradiction to $(c^2+4, n) = 1$. Since $s+1$ and $s-1$ are even, $u_i^{s+1} = -1$ is equivalent to $u_i^{s+1} + \left(\frac{-1}{u_i}\right)^{s+1} = -2$ hence to $g_{s+1}(c) \equiv$ $\equiv -2 \bmod p_i$, and $u_i^{s-1} = 1$ is equivalent to $g_{s-1}(c) \equiv 2 \bmod p_i$. If $u_1^{s+1} = -1$ and $u_2^{s-1} = 1$ or $u_1^{s-1} = 1$ and $u_2^{s+1} = -1$, then $(g_{s-1}(c) - 2, n) \in \{p_1, p_2\}$, and a factor of n is found. However, if $u_1^{s+1} = -1$ and $u_2^{s+1} = -1$ or $u_1^{s-1} = 1$ and $u_2^{s-1} = 1$, then we have found an even number $\bar{s}$ with $g_{\bar{s}}(c)^2 \equiv 4 \bmod n$, and therefore attack 5.1.2. can be applied.

A special case of this attack is given when $s = k$. Then c is a fixed point of the enciphering polynomial $g_k(x) \bmod n$.

As there is not known any systematic algorithm for the search of fixed points of $g_s(x) \bmod n$, only trial and error methods can be used. Therefore, the Dickson-scheme is secure from attack 5.2. if the number $\mathrm{fix}(n, s)$ of fixed points of $g_s(x) \bmod n$ is small. By the Chinese remainder theorem we have $\mathrm{fix}(n, s) =$ $= \prod_{i=1}^{2} \mathrm{fix}(p_i, s)$, and from the results proved in [7] it follows that

$$\mathrm{fix}(p_i, s) = \frac{1}{2}[(s-1, p_i - 1) + \alpha_1(s+1, p_i - 1) +$$

$$+ \alpha_2(s-1, p_i+1) + \alpha_3(s+1, p_i+1)] - 2\alpha_4,$$

where

$$\alpha_1 = \begin{cases} 1 & \text{if } v_2(s+1) < v_2(p_i - 1) \\ 0 & \text{if } v_2(s+1) \geqq v_2(p_i - 1), \end{cases}$$

$$\alpha_2 = \begin{cases} 1 & \text{if } v_2(s-1) > v_2(p_i + 1) \\ 0 & \text{if } v_2(s-1) \leqq v_2(p_i + 1), \end{cases}$$

$$\alpha_3 = \begin{cases} 1 & \text{if } v_2(s+1) = v_2(p_i + 1) \\ 0 & \text{if } v_2(s+1) \neq v_2(p_i + 1), \end{cases}$$

$$\alpha_4 = \begin{cases} 1 & \text{if } v_2(s-1) \geqq 2 \text{ and } v_2(p_i - 1) \geqq 2 \\ 0 & \text{if } v_2(s-1) < 2 \text{ or } v_2(p_i - 1) < 2. \end{cases}$$

If the key parameters satisfy (8), then

$$\operatorname{fix}(p_i, s) \leqq \frac{1}{2}[(s-1, a_i)(s-1, p_i') + (s+1, a_i)(s+1, p_i') +$$

$$+ (s-1, b_i)(s-1, p_i^*) + (s+1, b_i)(s+1, p_i^*)].$$

Let us write $a \nmid b$ for "a does not divide b". If for $i = 1, 2$

$$p_i' \nmid s-1,\ p_i' \nmid s+1,\ p_i^* \nmid s-1,\ p_i^* \nmid s+1, \tag{15}$$

then $\operatorname{fix}(p_i, s) \leqq 10^6$, and consequently $\operatorname{fix}(n, s) \leqq 10^{12}$. In this case, the probability that a uniformly distributed $c \in Z/(n)$ is a fixed point of $g_s(x) \bmod n$ is bounded by $10^{12}/10^{160} = 10^{-148}$, and the task of finding fixed points is computationally unfeasible.

Let us assume that the number s itself is chosen according to a uniform distribution on $M = \{1, 2, \ldots, r\}$, where r is a large positive integer, e.g. $r = 10^{100}$. In the following we write $[x]$ for the greatest integer which is less or equal than the real number x. There are exactly $\left[\frac{r-1}{p_i'}\right] + 1$ numbers $s \in M$ such that $p_i' \mid s-1$, namely the numbers $1, 1 + p_i', 1 + 2p_i', \ldots, 1 + \left[\frac{r-1}{p_i'}\right]p_i'$. Similarly, there are exactly $\left[\frac{r-1}{p_i^*}\right] + 1$ numbers $s \in M$ such that $p_i^* \mid s-1$, there are exactly $\left[\frac{r+1}{p_i'}\right]$ numbers $s \in M$ such that $p_i' \mid s+1$, and there are exactly $\left[\frac{r+1}{p_i^*}\right]$

numbers $s \in M$ such that $p_i^* | s + 1$. Since $p_i' > 10^{80}$, we obtain

$$\left[\frac{r-1}{p_i'}\right] + 1 \leqq \left[\frac{r}{p_i'}\right] + 1 \leqq \left[\frac{r}{10^{80}}\right] + 1,$$

$$\left[\frac{r+1}{p_i'}\right] \leqq \left[\frac{r}{p_i'}\right] + 1 \leqq \left[\frac{r}{10^{80}}\right] + 1,$$

and the same inequalities hold also with p_i^* instead of p_i'. Therefore, an upper bound for the number of elements $s \in M$ with

$$p_i' | s - 1 \text{ or } p_i' | s + 1 \text{ or } p_i^* | s - 1 \text{ or } p_i^* | s + 1$$

is given by $4\left(\left[\frac{r}{10^{80}}\right] + 1\right)$. Consequently, a lower bound for the probability that a uniformly distributed $s \in M$ satisfies (15) is given by

$$\left(r - \frac{4r}{10^{80}} - 4\right) \Big/ r = 1 - \frac{4}{10^{80}} - \frac{4}{r}.$$

Therefore, a uniformly distributed $s \in \{1, 2, \ldots, r\}$ satisfies (15) almost certainly.

Altogether we obtain: If the key parameters satisfy (8), then the task of finding an $s \in N$ and a $c \in Z/(n)$ such that c is a fixed point of $g_s(x) \bmod n$ is computationally unfeasible.

5.3. Superenciphering

Let $c \in Z/(n)$ be a given ciphertext, and let $m \equiv g_k^{-1}(c) \bmod n$ be the plaintext corresponding to c. We consider $g_k(c)$, $g_k^2(c)$, $g_k^3(c), \ldots$, where $g_k^r(x)$ denotes the function $g_k(x)$ iterated r times. Since $Z/(n)$ is finite, there are two exponents r and s such that $g_k^r(c) \equiv g_k^s(c) \bmod n$, and this implies the existence of a positive integer t such that $g_k^t(c) \equiv c \bmod n$. Applying $g_k^{-1}(x) \bmod n$ on both sides yields $g_k^{t-1}(c) \equiv g_k^{-1}(c) \equiv m \bmod n$, and the plaintext is obtained.

Sometimes superenciphering also yields the factorization of n. Indeed, from $g_k^t(x) = g_{k^t}(x)$ we obtain that every c with $g_k^t(c) \equiv c \bmod n$ is a fixed point of $g_{k^t}(x) \bmod n$, and since k^t is odd, attack 5.2. can be applied. Superenciphering is successful iff there exists a small t — say $t \leqq 10^{10}$ — such that c is a fixed point of $g_{k^t}(x) \bmod n$. Thus the Dickson-scheme is secure from superenciphering if for all $t \leqq 10^{10}$ the mapping $x \to g_{k^t}(x) \bmod n$ has only a small number of fixed points. Let us assume that the conditions (8) and (9) are satisfied. Then all t between 1 and 10^{10} fulfill $k^t \not\equiv \pm 1 \bmod p_i'$ and $k^t \not\equiv \pm 1 \bmod p_i^*$. Hence fix$(p_i,$

$k') \leqq \frac{1}{2}[(k'-1, a_i p_i') + (k'+1, a_i p_i') + (k'-1, b_i p_i^*) + (k'+1, b_i p_i^*)] \leqq a_i +$

$+ b_i < 10^6$, and therefore $\mathrm{fix}(n,k') < 10^{12}$. This yields

$$|\{c \in Z/(n) \colon \exists t \text{ with } 1 \leqq t \leqq 10^{10} \text{ such that } g_{k'}(c) \equiv c \bmod n\}| \leqq$$

$$\leqq \sum_{t=1}^{10^{10}} \mathrm{fix}(n,k') < 10^{10} \cdot 10^{12} = 10^{22}.$$

Therefore, if the conditions (8) and (9) are fulfilled, then the fraction of ciphertexts $c \in Z/(n)$ which can be decrypted by superenciphering is bounded by $10^{22}/10^{160} = 10^{-138}$.

REFERENCES

[1] BERKOWITZ, S.: Factoring via superencryption. Cryptologia. 6, 1982, 229—237.

[2] HERLESTAM, T.: Critical remarks on some public-key cryptosystems. BIT. 18, 1978, 493—496.

[3] LIDL, R.—MÜLLER, W. B.: Permutation polynomials in RSA-cryptosystems. Proc. Crypto 83. Univ. Calif. St. Barbara, 1984, 293—301.

[4] MÜLLER, W. B.: Über eine Klasse von durch Dickson-Polynome dargestellten Gruppen. Proc. of the Colloq. on rings, modules and radicals. Keszthely 1971, 1973, 361—376.

[5] MÜLLER, W. B.—NÖBAUER, R.: Cryptanalysis of the Dickson-scheme. Proc. Eurocrypt 85, Lecture Notes in Computer Science, Vol. 219, 1986, 50—61.

[6] MÜLLER, W. B.—NÖBAUER, W.: Some remarks on public-key cryptosystems. Studia Sci. Math. Hungar. 16, 1981, 71—76.

[7] NÖBAUER, R.: Über die Fixpunkte von durch Dicksonpolynome dargestellten Permutationen. Acta Arith. 45, 1985, 91—99.

[8] NÖBAUER, R.: Cryptanalysis of the Rédei-scheme. Proc. Vienna Conf. 84. Contributions to General Algebra. 3, 1985, 255—164.

[9] NÖBAUER, R.: Key distribution systems based on polynomial functions and on Rédei-functions. Problems of Control and Information Theory. 15, 1986, 91—100.

[10] NÖBAUER, R.: Rédei-Funktionen und ihre Anwendung in der Kryptographie. To appear in Acta Sci. Math. Szeged.

[11] NÖBAUER, W.: Über Permutationspolynome und Permutationsfunktionen für Primzahlpotenzen. Nonatsh. Math. 69, 1965, 230—238.

[12] NÖBAUER, W.: Über eine Klasse von Permutationspolynomen und die dadurch dargestellten Gruppen. J. reine angew. Math. 231, 1968, 215—219.

[13] RÉDEI, L.: Über eindeutig umkehrbare polynome in endlichen Körpern. Acta Sci. Math. Szeged. 11, 1946, 85—92.

[14] RIVEST, R. L.: Remarks on a proposed cryptanalytic attack on the M.I.T. public-key cryptosystem. Cryptologia. 2, 1978, 62—65.

[15] RIVEST, R. L.—SHAMIR, A.—ADLEMAN, L.: A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM. 21, 1978, 120—126.

[16] SCHNORR, C. P.: Is the RSA-scheme safe? Lecture Notes in Computer Science. Vol. 149, 1983, 325—329.

[17] SIMMONS, G. J.—NORRIS, N. J.: Preliminary comments on the M.I.T. public-key cryptosystem. Cryptologia. 1, 1977, 406—414.

Received December 30, 1986

Universität für Bildungswissenschaften
Institut für Mathematik
Universitätsstraße 65—67
A-9010 Klagenfurt
Austria

АНАЛИЗ КРИПТОСИСТЕМЫ С НЕТАЙНЫМ КЛЮЧОМ ПОСТРОЕННОЙ С ПОМОЩЪЮ ПОЛИНОМОВ ДИКСОНА

Rupert Nöbauer

Резюме

В статье с помощью полиномов Диксона строится криптосистема. Обсуждаются различные атаки против етой системы. Указываются условия на параметры ключа, которые гарантируют устойчивость системы при всех известных атаках.