CRYPTOLOGIA VOLUME 6 NUMBER 4

APPLICATION OF VINCENT'S THEOREM IN CRYPTOGRAPHY

OR

ONE-TIME PADS MADE PRACTICAL

ALKIVIADIS G. AKRITAS

It is a well known fact that one-time pads are unconditionally crypto secure. As an example consider the scheme based on $c_i \equiv m_i + k_i \pmod{26}$ where the i-th symbol of the ciphertext, c_i, is obtained by adding modulo 26 the i-th message (plaintext) symbol m_i and the i-th key symbol k_i. Clearly, without knowledge of the key k_i, $i = 1,2,\ldots$ it is impossible to recover the plaintext, because all messages of the same length are equiprobable. The basic drawback, however, of known one-time pads is that an enormous amount of key must be generated and distributed before the commencement of communications. Because of the high cost involved in the key management, one-time pads are used only for highly sensitive communications, e.g. Moscow-Washington hot-line and high-level military communications.

In what follows, we propose a new one-time pad scheme where key management doesnot present a problem. As we will immediately see, with our scheme the key is "concealed" in a polynomial equation which can be easily exchanged using the public key-distribution methods described in [4]. Our approach is based on the following:

Vincent's Theorem Let $P(x) = 0$ be a polynomial equation of degree $n > 1$, with rational coefficients and without multiple roots, and let $\Delta > 0$ be the smallest distance between any two of its roots. Let m be the smallest index such that

$$F_{m-1}\frac{\Delta}{2} > 1 \quad \text{and} \quad F_{m-1}F_m\,\Delta > 1 + \frac{1}{\varepsilon_n}$$

where F_k is the k-th member of the Fibonacci sequence 1,1,2,3,5,8,13,... and

$$\varepsilon_n = \left(1 + \frac{1}{n}\right)^{\frac{1}{n-1}} - 1$$

Then the continued fraction transformation

$$x = a_1 + \frac{1}{a_2} + \cdots + \frac{1}{a_m} + \frac{1}{y}$$

(which is equivalent to the series of successive transformations of the form $x = a_i + \frac{1}{y}$, $i = 1,2,\ldots,m$) with arbitrary, positive, integral elements $a_1, a_2, \ldots, a_m$, transforms the equation $P(x) = 0$ into the equation $\tilde{P}(y) = 0$, which has not more than one sign variation in the sequence of its coefficients.

The theorem, as stated above, is an extension of Vincent's original theorem which was published in 1836 [8], and it has been used to isolate the real roots of a polynomial equation [7],[1].

To see how it is applied, observe the following:

(i) The continued fraction transformation (1) can be also written as

$$x = \frac{P_m y + P_{m-1}}{Q_m y + Q_{m-1}} \tag{2}$$

where P_k/Q_k is the k-th convergent to the continued fraction

$$x = a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cdots}}$$

and as we recall

$$P_{k+1} = a_{k+1} P_k + P_{k-1}$$

$$Q_{k+1} = a_{k+1} Q_k + Q_{k-1}$$

(ii) Provided there are positive roots, when the partial quotients a_i are properly chosen (explained below) (2) (or (1)) leads to an equation $\tilde{P}(y) = 0$ with exactly one sign variation in the sequence of its coefficients. Then from the Cardano-Descartes rule of signs we know that $\tilde{P}(y) = 0$ has one root in the interval $(0,\infty)$. If $\tilde{y}$ was this positive root, then the corresponding root $\tilde{x}$ of $P(x)$ could be easily obtained from (2). We only know though that $\tilde{y}$ lies in the interval $(0,\infty)$; therefore, substituting y in (2) once by 0 and once by ∞ we obtain for the positive root $\tilde{x}$ its isolating interval whose unordered

endpoints are P_{m-1}/Q_{m-1} and P_m/Q_m. Note that to each positive root there corresponds a different continued fraction; at most m partial quotients have to be computed for the isolation of any positive root. (Negative roots can be isolated if we replace x by $-x$ in the original equation.)

We now present a recursive description of the way in which we obtain an equation with one sign variation in the sequence of its coefficients (or equivalently, how we choose the partial quotients; see also [1]).

Recursive description of the isolation procedure:

Let

$$P(x) = 0 \qquad (3)$$

be a polynomial equation with μ sign variations in the sequence of it's integer coefficients and without multiple roots.

BASE: $\mu = 0$ or $\mu = 1$. From the Cardano-Descartes rule of signs we know that $\mu = 0$ implies that (3) has no positive roots, whereas $\mu = 1$ indicates that (3) has exactly one positive root, in which case $(0,\infty)$ is its isolating interval; in either case, no transformation of (3) is necessary, and the method stops.

RECURSION: $\mu > 1$. In this case (3) has to be further investigated. We first compute the lower bound b on the values of the positive roots and then we obtain the translated equation $P_b(x) = P(b+x) = 0$, which also has μ sign variations provided $P(b) \neq 0$ (if $P(b) = 0$ we have found an integer root of the original equation and μ is decreased). $P_b(x) = 0$ is now transformed by the substitutions $x \longleftarrow 1+x$ and $x \longleftarrow 1/(1+x)$ and the procedure is applied again twice, once with $P_b(1/(1+x)) = 0$ in place of (3) and once with $P_b(1+x) = 0$.

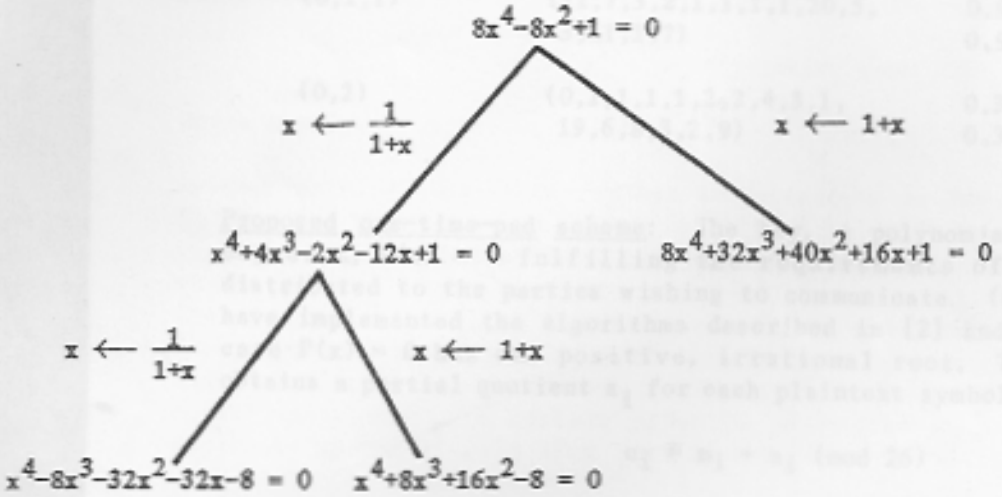
The lower bound on the positive roots is computed with the help of Cauchy's rule [1]. Detailed algorithms can be found in [2]. As an illustration let us isolate the positive roots of the Chebyshev polynomial equation

$$8x^4 - 8x^2 + 1 = 0 \qquad (4)$$

(Recall that Chebyshev polynomials have symmetric roots.) Using our recursive procedure we first observe that $\mu = 2$, which implies that we need to compute the lower bound, b, on the positive roots. $b = 0$ and so $P_b(x) = P(x) = 0$, which is now transformed by the substitutions $x \longleftarrow 1+x$ and $x \longleftarrow 1/(1+x)$. The resulting equations $8x^4+32x^3+40x^2+16x = 0$ and $x^4+4x^3-2x^2-12x+1 = 0$ respectively, are easily obtained using the Ruffini-Horner method ([7] pp.129-130).

The first of the transformed equations has no sign variations, indicating that there are no positive roots.

Continuing our process with the second transformed equation we obtain two new equations, $x^4+8x^3+16x^2-8 = 0$ and $x^4-8x^3-32x^2-32x-8 = 0$, each with only one sign variation in the sequence of its coefficients. In a tree form we have:



The transformations of the form (2) which lead to the last two equations are $(1+x)/(2+x)$ and $1/(2+x)$ from which we see that the isolating intervals for the positive roots of the original equation are $(1/2,1)$ and $(0,1/2)$ (the corresponding lists of the partial quotients are $(0,1,1)$ and $(0,2)$).

Besides real root isolation, Vincent's theorem has been used to approximate the real roots of a polynomial equation to any degree of accuracy [5], [6]. (Note that the approach followed in [6] has an exponential computing time bound; that is, in certain cases it will not terminate within any reasonable amount of time.) One sees that the approximation of the real roots can be easily achieved by extending (in various ways) the continued fraction (1) as long as desired. The point used in our scheme is that it some of the real roots are irrational, then there will be an infinite expansion of the corresponding continued fractions. In Table 1, we approximate to within $\varepsilon = 10^{-15}$ the two roots we isolated above [5].

Having explained the ideas involved we can now proceed to our cryptographic scheme.

Table 1

List of Partial Quotients for:		Approximating Intervals
Isolation	Approximation	
(0,1,1)	(11,7,3,2,1,1,1,1,20,5, 3,11,1,7)	0.92387953251128634045 0.92387953251128676332
(0,2)	(0,1,1,1,1,2,2,4,3,1, 19,6,8,3,2,9)	0.38268343236508971655 0.38268343236509064218

Proposed one-time-pad scheme: The key, a polynomial equation of arbitrary degree n, $P(x) = 0$ fulfilling the requirements of Vincent's theorem, is distributed to the parties wishing to communicate. (It is assumed, that they have implemented the algorithms described in [2] and [5]). In the simplest case $P(x) = 0$ has one positive, irrational root. The party transmitting obtains a partial quotient a_i for each plaintext symbol m_i and transmits

$$c_i \equiv m_i + a_i \pmod{26} \qquad (5)$$

At the other end of the line, for each c_i received there is an a_i computed and m_i is easily recovered from (5). Anyone who intercepts the c_i's must find (guess) the polynomial equation in order to decipher the message, an impossible task.

Advantages of the new scheme: The proposed scheme provides, once and for all, an infinite amount of key. No other polynomial equation ever need be exchanged because at the end of each enciphering-deciphering process both parties will have obtained a new polynomial equation $\bar{P}(x) = 0$, which can be used as above for subsequent communications. (Actually $\bar{P}(x) = 0$ constitutes the new key which both parties already possess.)

Things to watch for and topics for further research: Caution should be exercised in selecting the polynomial equation so that its real root is not a quadratic irrational which is represented by a periodic continued fraction. Moreover, from [3] we know that for almost all numbers α, the probability that the n-th partial quotient a_n, in the continued fraction expansion of α, equal to a positive integer j is given by

$$\log_2 \frac{(j+1)^2}{j(j+2)} \qquad (6)$$

For $j = 1$ and almost all numbers, this means that the probability for $a_n = 1$ is approximately .41 (see also Table 1). Therefore in order to better conceal messages, our scheme has to be modified. Two possible modifications (which need more study) are the following: (m_1) After the computation of each partial quotient a_i, calculate the decimal expansion of the root and use the next decimal digit d_i as the next key k_i (I am indebted to a referee for this suggestion.) (m_2) Use a counter initialized to some constant so that

$$c_i \equiv m_i + a_i + \text{counter}_i \pmod{26}$$

where $\text{counter}_i = \text{counter}_{i-1} + 1$.

Another problem that needs further investigation is how to speed up computations. The algorithms described in [2] and [5] have been implemented in the computer algebra system SAC-1 (Symbolic and Algebraic Computations-Version 1) which provides exact (infinite precision) integer arithmetic. This implies that, in our scheme, as the continued fraction expands, the coefficients of the polynomial equation will continuously grow, and the speed of the computations will slow down. The most obvious solution seems to be to reduce the coefficients modulo a certain prime p, after the computation of λ partial quotients (p and λ could form part of the key exchanged).

We are currently investigating these, and other alternatives and we hope to come up with interesting results. It is our hope that this paper will stimulate the reader for further research on the subject.

REFERENCES

1. Akritas, A.G. 1980. An implementation of Vincent's Theorem. Numerishche Mathemetik. 36: 53-62.

2. Akritas, A.G. 1980. The fastest exact algorithms for the isolation of the real roots of a polynomial equation. Computing. 24: 299-313.

3. Lang, S. and H. Trotter. 1972. Continued fractions for some algebraic numbers. Journal Fur Die Reine und Angewandte Mathematik. 255: 122-134.

4. Merkle, R.C. 1978. Secure communications over insecure channels. Communications of the ACM. 21: 294-299.

5. Ng, K.H. 1980. Polynomial real root approximation using continued fractions. M. S. Research Report. University of Kansas, Department of Computer Science. Lawrence, Kansas.

6. Rosen, D. and J. Schallit. 1978. A continued fraction algorithm for approximating all real polynomial roots. Mathematics Magazine. 51: 112-116.

7. Uspensky, J.V. 1948. Theory of Equations. New York: McGraw-Hill.

8. Vincent, A.J.H. 1836. Sur la resolution des equations numeriques. Journal de Mathematiques Pures et Appliquees. 1: 341-372.

Cartoon reproduced with permission from Creative Computing. Artist is Professor M. E. Sabbatini, Faculty of Medicine, University of Sao Paulo.