A POLYNOMIAL TIME ALGORITHM FOR BREAKING THE BASIC MERKLE-HELLMAN CRYPTOSYSTEM

(Extended abstract)

Adi Shamir

Applied Mathematics
The Weizmann Institute
Rehovot, Israel

ABSTRACT

The cryptographic security of the Merkle-Hellman system (which is one of the two public-key cryptosystems proposed so far) has been a major open problem since 1976. In this paper we show that when the elements of the public key $a_1,\ldots,a_n$ are modular multiples of a superincreasing sequence (as proposed by Merkle and Hellman), almost all the equations of the form

$$\sum_{i=1}^{n} x_i a_i = b \qquad x_i \in \{0,1\}$$

can be solved in polynomia time, and thus the cleartexts $x_1 \ldots x_n$ that correspond to given ciphertexts b can be easily found.

OUTLINE OF THE ALGORITHM

The algorithm proposed in this paper analyses the given numbers $a_1,\ldots,a_n$ and attempts to find a trapdoor pair of natural numbers W and M such that $Wa_i \pmod M$ is a superincreasing sequence and its sum is smaller than M. Knowledge of any pair of numbers with these properties makes it possible to solve arbitrary equations of the form

$$\sum_{i=1}^{n} x_i a_i = b \qquad x_i \in \{0,1\}$$

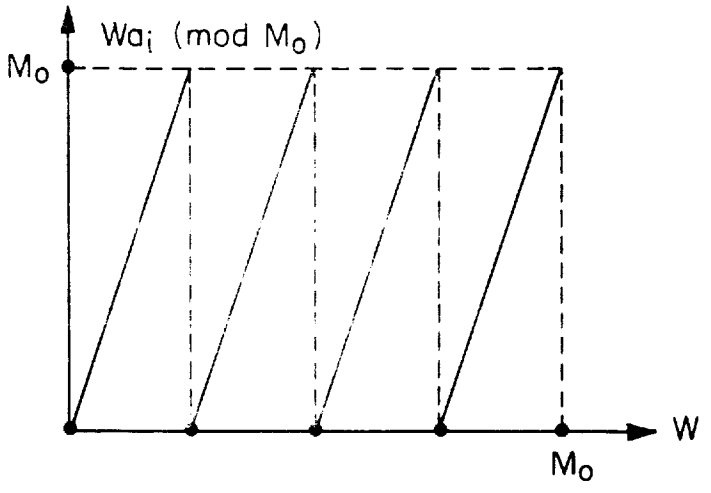
in polynomial time (see Merkle and Hellman [1978]). Since the a_i were obtained from a superincreasing sequence by modular multiplication, we know that at least one such pair exists. Our algorithm finds some trapdoor pair, but it is not guaranteed to find the original pair used in the construction of the a_i's.

In the Merkle-Hellman construction, the elements of the original superincreasing sequence have known sizes (but unknown values!). For the sake of simplicity, we assume that the i-th number has $n + i - 1$ bits, so that the smallest element is smaller than 2^n, the largest element is smaller than 2^{2n-1}, and the modulus is between 2^{2n-1} and 2^{2n} (in their original paper, Merkle and Hellman recommend this scheme with $n = 100$). After the modular multiplications, all the numbers become approximately 2n-bit long. They can be published in a permuted

order (so that a_1 does not necessarily correspond to the smallest element in the superincreasing sequence), but our algorithm remains polynomial in n even when such an unknown permutation is used.

The algorithm is divided into two parts. In the first part, Lenstra's integer programming algorithm is used to find a rational number $0 < \alpha < 1$ such that a necessary condition for W and M to be a trapdoor pair is that $\frac{W}{M} \in [\alpha, \alpha+\varepsilon]$ for a certain small ε. In the second part, we use the fact that the ratio $\frac{W}{M}$ is approximately known to find at most n^2 subintervals (ℓ_i, r_i) in $[\alpha, \alpha+\varepsilon]$ such that $\frac{W}{M} \in (\ell_i, r_i)$ for some i is also a sufficient condition for W, M to be a trapdoor pair. If we assume that some pair exists, at least one of the subintervals must be non-empty. By using a fast diophantine approximation algorithm, we can find the smallest W and M whose ratio is in such a subinterval.

Let W_0, M_0 be the (unknown) trapdoor pair of 2n-bit numbers used in the construction of the a_i sequence. The first step of the algorithm is to generalize the definition of a trapdoor pair to arbitrary real positive W and M. When $M = M_0$, the graph of the function $Wa_i \pmod{M_0}$ for real multipliers $0 \leq W < M_0$ has a sawtooth form:



The slope of the function (except at discontinuity points) is a_i, the number of minima is a_i, and the distance between successive minima is M_0/a_i (which is slightly more than 1).

If a_i corresponds to the smallest element in the superincreasing sequence, then the multiplier W has the property that $Wa_i \pmod{M_0}$ is at most 2^n, and thus the distance between W and the closest minimum to its left cannot exceed $2^n/a_i \simeq 2^{-n}$. The unknown W must thus be very close to some minimum of the sawtooth curve. Unfortunately, even if we impose the integrality constraint on W (which we do not), there are too many possible values for W and we cannot check them one by one.

If a_j corresponds to the second smallest element in the superincreasing sequence, then a similar analysis shows that W must also be within a distance of $2^{n+1}/a_j$

from a minimum of the a_j-sawtooth, and thus the two minima of a_i and a_j must be very close to each other. This greatly reduces the number of places in which W may be, but it still does not characterize it uniquely.

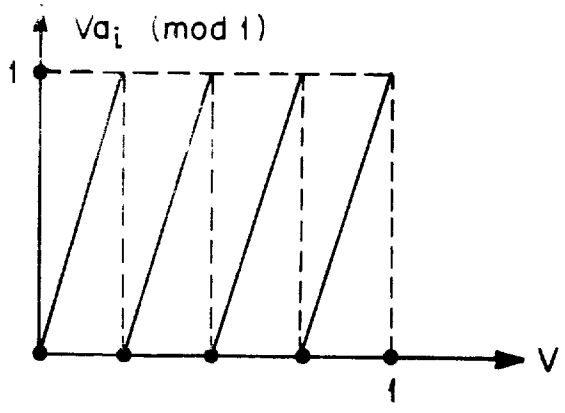
We can proceed in a similar way and superimpose more sawtooth curves on the same diagram. The fact that W is close to a minimum on each curve implies that all these minima are close to each other, and thus we can replace the problem of finding W by the equivalent problem of finding the accumulation points of minima of the various curves.

In the full paper we show that when four sawtooth curves are superimposed, the probability that four minima will be so close to each other is so small that it is extremely unlikely to happen in more than a few places in the region $0 \leq W < M_0$ (it must happen somewhere since by the construction of the a_i's such a W_0 exists). The number 4 is independent of n, and depends only on the ratio between the sizes of M_0 and the smallest element of the superincreasing sequence (which was assumed to be 2).

Two problems remain: How to get rid of M_0 (whose value is actually unknown) and how to find the accumulation point of the minima of the four sawtooth curves.

The key observation is that the location of the accumulation point in the diagram depends on the slopes of

the curves, but not on their sizes. If we divide both coordinates by M_0, we get the sawtooth curve of the function $Va_i \pmod 1$, $0 \leq V < 1$, which is independent of M_0:



In the new coordinate system the slope of the curve remains a_i, the number of minima remains a_i, but the distance between successive minima is reduced to $1/a_i$. The original W parameter is replaced by a new $V = W/M_0$ parameter, and the allowable distance between this parameter and the closest curve minimum is reduced by a factor of approximately 2^{2n} (from 2^{-n} to 2^{-3n}).

The problem of locating the accumulation point of minima in the new coordinate system can be described by linear inequalities with four integral unknowns. Without loss of generality, we assume that a_1 a_2 a_3 a_4 correspond to the four smallest elements in the superincreasing sequence (there are $0(n^4)$ ways to guess them). We further assume that among the four minima at the accumula-

tion point, the a_1-minimum is the rightmost (i.e., closest to W_0/M_0). Then the conditions that the i-th minimum of a_1, j-th minimum of a_2, k-th minimum of a_3, and ℓ-th minimum of a_4 are sufficiently close to each other are:

$$i,j,k,\ell \text{ integers} \qquad 1 \le i \le a_1 - 1$$

$$0 \le \frac{i}{a_1} - \frac{j}{a_2} \le 2^{-3n+1} \qquad 1 \le j \le a_2 - 1$$

$$0 \le \frac{i}{a_1} - \frac{k}{a_3} \le 2^{-3n+2} \qquad 1 \le k \le a_3 - 1$$

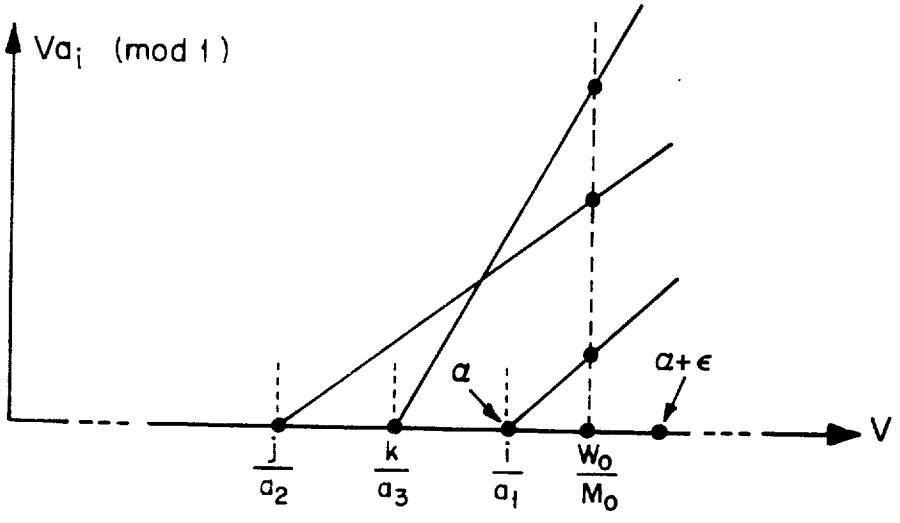
$$0 \le \frac{i}{a_1} - \frac{\ell}{a_4} \le 2^{-3n+3} \qquad 1 \le \ell \le a_4 - 1$$

By multiplying the inequalities by their denominators, we get an equivalent system in which all the coefficients of i,j,k and ℓ are integers with no more than 5n bits. Since Lenstra's integer programming algorithm is polynomial in the size of the coefficients for a fixed number of unknowns, we can find the (almost certainly unique) accumulation point of the four minima in polynomial time.

Once the value of i is known, it is easy to find the interval $[\alpha,\alpha+\varepsilon]$ of V values for which the values of all the n sawtooth curves are properly bounded. An important property of this interval is that it cannot contain discontinuity points since all the sawtooth values in it must be smaller than 1.

A typical enlarged section of the superimposed

diagram in the vicinity of W_0/M_0 is:



Any pair of numbers W,M such that $\frac{W}{M} \in [\alpha,\alpha+\varepsilon]$ gives properly bounded values under modular multiplication, but these values need not be a superincreasing sequence and thus they do not necessarily lead to an easily solvable knapsack. The second part of the algorithm extracts from the $[\alpha,\alpha+\varepsilon]$ interval those subintervals (ℓ_i,r_i) for which the transformed sequence is guaranteed to be superincreasing.

Since the $[\alpha,\alpha+\varepsilon]$ interval does not contain discontinuity points, the n sawtooth curves look like n linear segments in it. These n segments can intersect each other in at most $0(n^2)$ points. By finding and sorting these points, we can subdivide $[\alpha,\alpha+\varepsilon]$ into $0(n^2)$ subintervals with a well defined vertical order

between the curves in each subinterval. When this order is known, we can express the conditions for a superincreasing sequence by the linear inequalities

$$\left(Va_{\pi(i)} - c_{\pi(i)} \right) > \sum_{\pi(j)<\pi(i)} \left(Va_{\pi(j)} - c_{\pi(j)} \right)$$

$$\sum_{i=1}^{n} (Va_i - c_i) < 1$$

in which the π is the permutation of the indices specified by the vertical ordering in the subinterval and the c_i is the number of a_i-minima between 0 and the accumulation point. The solution of each set of inequalities is a (possibly empty) subinterval (ℓ_i, r_i) in which all the superincreasing and size conditions are satisfied. At least one of these subintervals must be non-empty, and the smallest natural numbers W and M such that W/M belongs to such an interval can be found in polynomial time (note that W and M cannot exceed W_0 and M_0, which are 2n-bit long). Once these numbers are found, the cryptanalysis of arbitrary ciphertexts in the $a_1,\ldots,a_n$ system becomes trivial.

CONCLUSIONS AND OPEN PROBLEMS

We have demonstrated that Merkle-Hellman cryptosystems in which the public keys are obtained from superincreasing sequences by a single modular multiplication are totally insecure. It remains an open problem whether

keys obtained by two or more modular multiplications are cryptographically secure. In addition, the exact complexity of our algorithm needs further analysis since it can be optimized in a number of ways (e.g., 3 superimposed sawtooth curves are sometimes enough, and then the Lenstra algorithm can be replaced by a much simpler algorithm based on continued fractions).

BIBLIOGRAPHY

Merkle, R., and Hellman M.,[1978],"Hiding information and signature in trapdoor knapsacks," IEEE Trans. Information Theory, IT-24-5, September 1978.