A PROTOCOL FOR SIGNING CONTRACTS

Shimon Even*

1. Introduction

Assume two participants, A and B, in a communication network, have negotiated a contract C, which they wish to sign.

It was shown by Even and Yacobi [1] that no deterministic protocol exists, in which there is no participation of a third party. Essentially, the reason is that in the sequence of messages being sent between A and B, a point must be reached where one of the participants has a signature of the other without committing himself; if he terminates the conversation at this point, the principle that one should not be committed unless the other is committed too is violated.

The use of a third party can easily correct this fault. In fact, it is sufficient to have a Center of Cancellations. Each contract starts with a number, the date the contract becomes effective (say 24 hours after the informal negotiations terminate) and a statement that the contract is binding only if neither A nor B cancel it before the date.

Now, A signs C and sends to B and B signs C and sends to A. Normally, each will receive the commitment of the other, and on date, C will become binding. If either does not get the other's signature, say up to 1 hour before date, he calls the center, refers to the numbered contract between A and B and announces that it is canceled. The center informs the other party of the cancellation. Notice that normally the center does not even know of the signing of a contract between A and B, and even if a cancellation occurs, it only knows the contract's number and the names of the participants.

It remains desirable to have a protocol for signing contracts in which no third party involvement is ever necessary.

*Computer Science Department, Technion, Haifa, Israel.

During the summer of 1980, in a conversation, M. Blum suggested the use of randomization for such protocols. The present paper is an implementation of such a protocol. Other protocols have been suggested by Blum and Rabin [2], and by Blum [3]. Their methods rely on the infeasibility of some number theoretic operations, such as the difficulty of factoring large integers, while the method presented here uses any Public Key Cryptosystem (PKCS) which is considered safe.

2. Assumptions

It is assumed that the contract C is concerned with some business transaction, and the items being traded are approximately of equal value, V, to both parties.

Also, it is assumed that the cost of computing is approximately the same for both parties.

The existence of a PKCS [4] is assumed. Let E_p and D_p be, respectively, the encryption algorithm and decryption algorithm of participant P. Clearly, E_p is publically known, while D_p is known to P alone. For every word w, $D_p(w)$ is defined (this is P's signature of w) and

$$E_p\,(D_p(w)) = w.$$

A secure conventional cryptosystem is used also, but its existence is guaranteed if a secure PKCS exists. One can use, instead, a conventional cryptosystem which is designed as such, for example, the DES [5], if it is trusted to be secure. If M is a message and K is the key, then $F_K(M)$ is the cryptogram produced by the conventional cryptosystem being used. The decryption algorithm is denoted by F^{-1}. Thus,

$$F_K^{-1}(F_K(M)) = M.$$

3. Preliminaries

The ideas used in the construction of this protocol are Rabin's signature method [6] and Merkle's concept of a puzzle [7].

A puzzle is a pair of message and cryptogram, $(M,F_K(M))$, where the solver's task is to find K. [This assumption is justified on the basis that by using a relatively short key, in comparison to the message length, the probability of the key being unique becomes very high; see Shannon's discussion [8] of the unicity distance.]

One may control the cost of solving the puzzle by exhaustion, by announcing some of the key bits. For example, if one uses DES for F, then instead of using a 56 bit key, one may decide to use only 30, while the remaining 26 bits are known to everyone and are fixed. By changing the number of bits, one may control the cost of solving the puzzle through exhaustion.

We shall use a standard message S, known to all, and form puzzles by randomly choosing K and announcing $F_K(S)$.

In the process of signing C, it will be numbered 2N times:

$$(C,1),\ (C,2),\ldots,(C,2N),$$

where (C,i) is simply formed by appending the string of bits representing i to C; the resulting string is called the i-th copy of C. N is an integer that is used in the network, or agreed on by the participants, In the demonstration to follow, N = 50.

A convention is made that A has a formal commitment of B to contract C if he possesses any N + 1 of the 2N signatures:

$$D_B(C,1),\ D_B(C,2),\ldots,\ D_B(C,2N).$$

4. The Protocol

(1) A prepares 2N puzzles

$$F_{K_1}(S),\ F_{K_2}(S),\ldots,\ F_{K_{2N}}(S)$$

and 2N encoded signed copies of C

$$F_{K_1}(D_A(C,1)),\ F_{K_2}(D_A(C,2)),\ldots,\ F_{K_{2N}}(D_A(C,2N))$$

and sends it all to B.

B acts symmetrically.

Comment: Each of them has now the information necessary to find 2N signed copies of the other; he can get them by solving the 2N puzzles and using the same keys to decode the signatures. The cost of solving each puzzle is tuned to be approximately 2V/N. Thus, the cost of solving N+1 puzzles is more than twice the contract's value, V.

(2) A chooses an $1 \leq i \leq 2N$, not chosen by him before. He requests B to reveal his K_i. B complies. Upon receiving K_i, A can verify that the received key is indeed the solution of the i-th puzzle of B. He then uses K_i to decode B's signature of the i-th copy, and verifies that it is indeed a signature by B of (C,i), by applying E_B to $D_B(C,i)$.

B acts symmetrically.

Step (2) is repeated N+1 times.

□

Let each pair $F_{K_i}(S),\ F_{K_i}(D_A(C,i))$ be called the i-th unit of the message sent by A to B in step (1).

Upon receiving K_i from A, in response to B's request, B should consider the unit to be bad if any of the following holds:

(i) The fixed bits of the puzzle-key K_i are not as agreed on before the signature protocol has started. I.e., A tried to cheat by making the puzzle harder.

(ii) The received K_i is not the solution of A's i-th puzzle, P_i. I.e., $F_{K_i}^{-1}(P_i) \neq S$.

(iii) Upon decoding the i-th part, M_i, of the (alleged) encoded signature sequence which A sent in step (1) to B, the signature of (C,1) is not verified. I.e.,

$$E_A(F_{K_i}^{-1}(M)) \neq (C,1).$$

Once B detects a bad unit, for his own protection, he should discontinue the protocol immediately, since A has been caught cheating.

5. Properties of the Protocol

If both participants follow the protocol honestly to its intended end, then each has a 'signature' of the other on C, and each knows that he has got it.

If one of the participants stops the protocol before its intended end, but none has cheated, then the uncooperative participant has an edge on the other (if he is A) only in the sense that he needs to invest less money in computing in order to produce a 'signature' of the other. His edge, $2V/N$, can be kept down to a small fraction of V by choosing N large enough. (For $N = 50$, it is 4% of V.)

Assume A 'plants' m bad units. The probability of him not being caught in the first k exchanges is

$$P = \frac{\binom{2N-m}{k}}{\binom{2N}{k}}.$$

For $N = 50$, if $m = k = 10$ then $p \approx 0.33$. If $m = k = 15$ then $p \approx .07$, and if $m = k = 25$ then $p \approx .0002$.

If the cost of solving a puzzle is approximately 4% of V, then $N = 50$ is sufficient to prevent cheating; if $m = 25$, A is almost certain to be caught during the 25 first exchanges, and in order to produce a complete 'signature' he will have to solve 26 puzzles. The cost of doing it is more than V.

If m is small and A is not caught at all, than B can still produce a complete 'signature' by solving a few puzzles, once A stops communicating upon receiving the 51-st signature.

References

[1] Even, S., and Yacobi, Y., "Relations among Public Key Signature Systems", Technical Report # 175, Comp. Sci. Dept., Technion, Haifa, Israel, March, 1980.

[2] Blum, M., and Rabin, M.O., "How to Send Certified Electronic Mail", in preparation.

[3] Blum, M., "How to Exchange Secrets", in preparation.

[4] Diffie, W., and Hellman, M.E., "New Directions in Cryptography", IEEE Trans. on Info. Th., Vol. IT-22, No. 6, Nov. 1976, pp. 644-654.

[5] Data Encryption Standard, National Bureau of Standards, Federal Information Processing Standards, Publ. 46, 1977.

[6] Rabin, M.O., "Digitalized Signatures", in Foundations of Secure Computation, R.A. DeMillo et.al., eds., Academic Press, 1978, pp. 155-168.

[7] Merkle, R.C., "Secure Communication Over Insecure Channel", Comm. of the ACM, Vol. 21, April 1978, pp. 294-299.

[8] Shannon, C.E., "Communication Theory of Secrecy Systems", Bell Syst. J., Vol. 28, Oct. 1949, pp. 656-715.

Part of the work was done while the author spent the summer of 1981 at the Computer Science Division, EECS, University of California, Berkeley. Supported by NSF Contract No. MCS79-15763 and by the Fund for the Promotion of Research at the Technion.