A "PARADOXICAL" SOLUTION TO THE SIGNATURE PROBLEM*

Shafi Goldwasser**

Silvio Micali**

Ronald L. Rivest**

Brief Abstract[1]

We present a general signature scheme which uses any pair of trap-door permutations (f_0, f_1) for which it is infeasible to find any x,y with $f_0(x) = f_1(y)$. The scheme possesses the novel property of being robust against an adaptive chosen message attack: no adversary who first asks for and then receives sgnatures for messages of his choice (which may depend on previous signatures seen) can later forge the signature of even a single additional message.

For a specific instance of our general scheme, we prove that

(1) forging signatures is provably equivalent to factoring (i.e., factoring is polynomial-time reducible to forging signatures, and vice versa)

while

(2) forging an additional signature, after an adaptive chosen message attack is still equivalent to factoring.

Such a scheme is "paradoxical" since the above two properties were believed (and even "proven" in the folklore) to be contradictory.

The new scheme is potentially practical: signing and verifying signatures are reasonably fast, and signatures are not too long.

* This research was supported by NSF grant MCS-80-06938, and IBM/MIT Faculty Development Award, and DARPA contract N00014-85-K-0125.

** MIT Laboratory for Computer Science, Cambridge, MA 02139

[1] A fuller version of this paper can be found in the Proceedings of the 25th Annual Syposium on Foundations of Computer Science, Singer Island, Florida, October, 1984, pages 441-448.

G.R. Blakley and D. Chaum (Eds.): Advances in Cryptology - CRYPTO '84, LNCS 196, p. 467, 1985.