

COMPUTATIONAL COMPLEXITY, EFFICIENCY & ACCOUNTABILITY IN
LARGE SCALE TELEPROCESSING SYSTEMS

FINAL REPORT

AFOSR CONTRACT F-49620-78-C-0086

May 1, 1978 to April 30, 1979

John T. Gill

Martin E. Hellman

Accession For	
NTIS GRA&I	☒
DTIC TAB	☐
Unannounced	☐
Justification	
By	
Distribution/	
Availability Codes	
Dist	Avail and/or Special
A-1	



We have developed a digital signature system whose security rests primarily on the existence of a one-way function. Since many one-way functions are known, and since their existence is essential to even conventional authentication systems, the security of the new system is at least as good as in conventional authentication. The security of previously known digital signature systems depends on the difficulty of factoring and related problems and is open to more question. There is a penalty paid for this security in the increased time required to compute a signature, but recent modifications reduce this penalty to an acceptable level.

The signature system uses a form of tree authentication, coupled with a one-way hash function to compress a large authentication file into a single number of approximately 100 bits. A patent disclosure has been filed and a paper will be submitted for publication.

We have also developed a direct demonstration of the equivalence between two NP-complete problems: satisfiability and the knapsack problems. Applying this equivalence to the circuitry of the data encryption standard (DES) results in a 10,000 dimensional knapsack. If the DES is secure then it follows that no fast general algorithm exists for solving 10,000 dimensional knapsacks.

In other work we have established new achievable regions for multiuser communication channels with feedback and privacy constraints.

Satellization arguments involving artificial pre- and post- channels proved valuable in establishing these results. A paper has been submitted to the Transactions on Information Theory.

One-way functions are a key requirement for computationally secure systems. We have investigated the relationship between one-way functions and random functions, in an attempt to obtain a method by which good pseudorandom functions can be transformed into good one-way functions.

One-way functions belong to the class NP of problems whose solutions can be checked quickly (in polynomial time). Therefore, if $P = NP$, that is, if every problem that can be checked quickly can also be solved quickly, there can be no one-way functions. We have studied computers augmented with subroutines for random functions, and shown that for these computers, for almost all choices of random functions, the classes NP and P are different. Thus, with the aid of an ideal pseudorandom number source, we can generate (not uniquely invertible) one-way functions.

PUBLICATIONS SUPPORTED UNDER CONTRACT #F-49620-78-C-0086

1. Charles Bennett and John Gill, "Relative to a Random Oracle, P NP with Probability 1," IBM Technical Report.
2. Norbert Cot and John Gill, "Optimal t-ary Trees with Weighted Branches," preprint.
3. Raynold Kahn and Martin Hellman, "On the Wiretap Channel with Feedback", submitted to IEEE Trans. on Info. Theory.
4. Ralph Merkle, "A Certified Digital Signature" submitted to CACM.
5. Ralph Merkle, "Secrecy, Authentctication, and Public Key Systems" Ph.D Thesis, June 1979.