An Optimally Secure Relativized Cryptosystem (extended summary, May 1982)*

Gilles Brassard

Université de Montréal
Département d'informatique et de recherche opérationnelle
C.P. 6128, Succursale "A"
Montréal, Québec
H3C 3J7 CANADA

Introduction

Throughout the ages, cryptography has been a pathetic battle between smart guys trying to design unbreakable codes and smarter guys breaking them shortly afterwards. The most notable weakness of these codes has been that their claims of security were based on the amount of effort unsuccessfully spent by qualified experts trying to crack them, rather than being based on mathematics. Although substantial progress towards a more formal treatment of cryptographic security was achieved through Shannon's information theory in the late fourties, the most significant breakthrough came with Diffie and Hellman's public-key cryptography. A fairly new science, known as complexity theory, was perhaps going to give cryptographers the final word, leaving cryptanalysts speechless before a definitive proof that any attempts to break the new codes would be a waste of their time.

Unfortunately, it did not quite work this well. Too many open problems in complexity theory closed the door to any realistic hopes that proofs of security for public-key cryptosystems are shortly forthcoming. Even NP-completeness, the complexity theoretician's favourite tool when he is willing to accept compelling evidence rather than a proof, could not help because public-key cryptosystems with NP-hard cryptanalytical tasks cannot exist under reasonable assumptions [Br1], and even if they did, they would have no practical interest because of the worst-case aspects of NP-completeness.

As a result of the overwhelming difficulty of these open problems, public-key cryptographers fell into the old pattern: they proposed cryptosystems they could not prove secure, based their beliefs on some type of evidence and sometimes even offered cash prizes for anyone capable of breaking them! The two best known proposed public-

* Supported in part by Canada's NSERC Grant number A4107.

key cryptosystems are Merkle and Hellman's scheme based on the apparent difficulty of solving the knapsack problem [MH] and Rivest, Shamir and Adleman's scheme based on the apparent difficulty of factoring [RSA]. In neither case was the evidence of security compelling because one could perhaps crack the codes without solving the underlying presumably difficult problems. And sure enough, what had to happen happened... Very recently, Shamir cashed Merkle and Hellman's prize [Sh]! This breakthrough showed dramatically that "evidence" of security may be no better with public-key cryptography than it has been in the past with classical cryptography.

Until complexity theory comes of age with a proof that P differs from NP, more convincing evidence for the security of some public-key cryptosystems can be obtained by proving the *equivalence* of their cryptanalytical tasks with outstanding problems having baffled the best mathematicians for centuries, such as factorization. This idea was first used by Rabin [Ra]. More recently, a truly superb scheme was put forward by Goldwasser and Micali who proved that getting to know *any* information on a cleartext message encoded with their scheme is as difficult as deciding quadratic residuosity in a very strong probabilistic sense. Nevertheless, assumptions are still needed about the difficulty of this problem [GM].

The above considerations are rather unpleasant for the theoretician: current evidence is unsatisfactory whereas hoping for proofs would be unrealistic. For this reason, the question of cryptographic security in relativized models of computation* was addressed in [Br2, Br3]. The following level-oriented definition of security was given: "A cryptosystem is *immune* to an algorithm if the latter's likelihood of decoding a (randomly chosen) cryptogram goes to zero *exponentially fast* in the length of the cleartext message transmitted. Given a function t the cryptosystem *achieves level* t *of security* if it is immune to any t(n)-time bounded Las Vegas algorithm."
A more formal definition of this notion can be found in [Br3].

---

* The reader unfamiliar with relativization is encouraged to read [BGS] both for definitions and for motivations.

It was proved in [Br2] that there exists a relativized model of computation in which no cryptosystems can achieve every polynomial level of security while there is another one in which there is a cryptosystem that does achieve simultaneously every (deterministic) polynomial levels of security. It was later proved in [Br3] that there also exists a relativized model of computation in which there is a cryptosystem that nearly achieves level $2^{n/\log n}$ of security. This is fairly tight since exhaustive search techniques show that no cryptosystem can achieve level 2^{cn} of security for any positive constant c. The following question was then raised: Does there exist a relativized model of computation in which there is a cryptosystem capable of achieving level $2^{n\,\delta(n)}$ of security for *every* real-valued function δ such that $\lim_{n\to\infty} \delta(n) = 0$?

The purpose of this paper is to provide a positive answer to the above question. A provocative way of interpreting this result is to say that such an *optimally secure cryptosystem* is so safe that no cryptanalytical algorithm can hope for any significant success short of using nearly as much time as exhaustive search would have required. Said otherwise, complete knowledge of how the enciphering algorithm works cannot help the cryptanalyst significantly more than a mere enciphering black box.

It is important to understand that this result says rather little about the possibility of optimally secure *un*relativized cryptography. It does indicate, however, that the definition of optimal security makes sense. Moreover, should optimally secure cryptosystems not exist, this sad fact would have a somewhat unusual proof because most proofs in complexity theory relativize [BGS]. In view of the Random Oracle Hypothesis [BG], it would be very interesting to see whether optimally secure cryptosystems exist with probability one relatively to a random oracle. The reader is warned that this open question is likely to be difficult because Bennett and Gill "can think of no way to use a random oracle to construct a rapidly-evaluable 1-1 function" [BG].

An Overview of the New Technical Results

The proof of existence of an optimally secure relativized cryptosystem is similar to that of the relativized cryptosystem nearly achieving level $2^{n/\log n}$ of security given in [3r3], although one has to be more careful with counting arguments and a new technique known as *flexible padding* is used. This section is but a short sketch of the additional ideas involved and technical results obtained. More details will appear later. As an extension of a definition from [3r3], let $Suc^{Q}_{A_t}(n)$ denote the probability that Las Vegas algorithm A successfully decodes *within t(n) steps* a randomly chosen length n cryptogram enciphered with cryptosystem Q. Assuming one can verify within polynomial time whether a candidate cleartext message does indeed correspond to a given cryptogram, and assuming there are 2^n length n cleartext messages, it is obvious that there exists an exhaustive search algorithm B and a polynomial p such that $Suc^{Q}_{B_t}(n) \geq \min(1, \lfloor t(n)/2^n \rfloor / p(n))$ for every time bound t. The main result in this paper is that we can come fairly close to this bound in an appropriate relativized setting: there is a relativized cryptosystem S such that given any Las Vegas cryptanalytical algorithm A and any time bound function t, $Suc^{S}_{A_t}(n) \leq \lfloor t(n)/2^n \rfloor \times n^{3 \log\log n}$ for all n but perhaps a finite number. This result immediately implies optimal security.

Even if it were not for the fact that it is relativized, the new cryptosystem suffers from a serious drawback that would make it unfit for practical use: a length n cleartext message can be expanded into an n^2-long ciphertext. This inconvenience is a direct consequence of flexible padding. For technical reasons, the previous relativized cryptosystems could be used directly only for enciphering messages of length an exact power of two. Padding to the next power of two was otherwise necessary. In order to get optimal security, it turns out to be convenient to be more flexible with the padding and encipher directly only messages of length in the image of some strictly increasing, easily computable function σ to be specified later. Messages of length between $\sigma(n)$ and $\sigma(n+1)$ are enciphered after padding to the length $\sigma(n+1)$. The main technical result is that to any such function σ corresponds a relativized cryptosystem S_σ such

that for any cryptanalytical Las Vegas algorithm A, any time bound function t and any integer n (*not* necessarily in the image of ρ), $Suc_{A_t}^{So}(n) \le \lceil t(n)/2^n \rceil \times Z_A^\rho(n)$ where the factor multiplying $t(n)/2^n$ depends only on the amount of padding used, on the cryptanalytical algorithm, and on the length of the cleartext *but not on the time bound function*. Elaborate calculations give an upper bound for $Z_A^\rho(n)$:

$$Z_A^\rho(n) \le \lceil 4 \lceil n \rceil a^{(\alpha(2^{\lceil n \rceil}) - \alpha(n))} (\alpha(2^{\lceil n \rceil})+1)! \rceil / (\alpha(n)+1)!$$

where a is a constant that depends only on A,

$\alpha(n) = \max(m \mid \rho(m) \le n)$ is the inverse function of ρ,

and $\lceil n \rceil = \rho(\alpha(n)+1)$ is the integer following n in the image of ρ.

This leads to an unexpected and bizarre *padding-security tradeoff*: as long as the padding function ρ remains resonably small, the function Z_A^ρ decreases (more security) with increases of ρ (less efficient padding). The author does not believe that this tradeoff is genuine, but rather that it is a freak consequence of the particular type of construction involved.

Let us conclude by giving two typical padding functions together with their corresponding security. If we choose $\rho(n) = 2^{2^n}$, then padding can be as bad as quadratic since $\rho(n+1) = (\rho(n))^2$, but $Z_A^\rho(n) \le n^{3 \log\log n}$ for all A and almost every n. Smaller amounts of padding can be used while preserving optimal security: if $\rho(n) = 2^{n^\omega}$ for any given $\omega > 1$, then $Z_A^\rho(n) \le 2^{n^{1/\sqrt{\omega}}}$ for all A and almost every n.

References (Due to space limitations, some titles are shortened)

[BGS] Baker, Gill and Solovay, "Relativizations of P=?NP", SIAM J. Comput. 4, 1975, 431-442.

[BG] Bennett and Gill, "Relative to a Random Oracle...", SIAM J. Comput. 10, 1981, 96-113.

[Br1] Brassard, "A Note on the Complexity of Cryptography", IEEE IT-25, 1979, 232-233.

[Br2] Brassard, "Relativized Cryptography", 20th IEEE FOCS, Puerto Rico, 1979, 383-391.

[Br3] Brassard, "A Time-Luck Tradeoff in Relativized Cryptography", JCSS 22, 1981, 280-311.

[GM] Goldwasser and Micali, "Probabilistic Encryption & How to Play Mental Poker Keeping Secret all Partial Information", 14th ACM STOC (SIGACT) San Francisco, 1982, 365-377.

[MH] Merkle and Hellman, "Hiding Information and Receipts...", IEEE IT-24, 1978.

[Ra] Rabin, "Digitalized Signat. ... as Intractable as Factorization", MIT/LCS/TR-212, 1979.

[RSA] Rivest, Shamir and Adleman, "On Digital Signatures...", CACM 21, 1978, 120-126.

[Sh] Shamir, "A Polynomial-Time Algorithm for Breaking Merkle-Hellman Cryptosystems", Applied Mathematics, The Weizmann Institute, Renovot, Israel, 1982.