IEEE TRANSACTIONS ON INFORMATION THEORY, VOL. IT-22, NO. 6, NOVEMBER 1976

New Directions in Cryptography

Invited Paper

WHITFIELD DIFFIE AND MARTIN E. HELLMAN, MEMBER, IEEE

这篇论文实际上是一个预测性论文，以公钥密码学为核心，预测了密码学未来的发展方向，主要包括：

- 公钥密码学
- 单向认证，也就是后来的数字签名（One-Way Authentication）
- 陷门单向函数（Problem Interrelations and Trapdoors）
- 计算复杂性问题（Computational Complexity）

可以说，Diffie 和 Hellman 在这篇论文中指出了密码学的未来发展方向，并且论证了它们之间的关系：利用计算复杂性问题可以构造陷门单向函数，进一步可以构造公钥密码学，而公钥密码学可以实现加密和认证功能。

The new technique makes use of the apparent difficulty of computing logarithms over a finite field $GF(q)$ with a prime number q of elements. Let

$$Y = \alpha^X \bmod q, \qquad \text{for } 1 \le X \le q-1, \tag{4}$$

where α is a fixed primitive element of $GF(q)$, then X is referred to as the logarithm of Y to the base α, mod q:

$$X = \log_\alpha Y \bmod q, \qquad \text{for } 1 \le Y \le q-1. \tag{5}$$

fusion.

Merkle [1] has independently studied the problem of distributing keys over an insecure channel. His approach is different from that of the public key cryptosystems suggested above, and will be termed a *public key distribution system*. The goal is for two users, A and B, to securely exchange a key over an insecure channel. This key is then used by both users in a normal cryptosystem for both enciphering and deciphering. Merkle has a solution whose cryptanalytic cost grows as n^2 where n is the cost to the legitimate users. Unfortunately the cost to the legitimate users of the system is as much in transmission time as in computation, because Merkle's protocol requires n

References

[1] R. Merkle, "Secure communication over an insecure channel," submitted to *Communications of the ACM*.

[2] D. Kahn, *The Codebreakers, The Story of Secret Writing*. New York: Macmillan, 1967.

United States Patent [19]

Hellman et al.

[11] **4,200,770**

[45] **Apr. 29, 1980**

[54] **CRYPTOGRAPHIC APPARATUS AND METHOD**

[75] Inventors: **Martin E. Hellman,** Stanford; **Bailey W. Diffie,** Berkeley; **Ralph C. Merkle,** Palo Alto, all of Calif.

[73] Assignee: **Stanford University,** Palo Alto, Calif.

[21] Appl. No.: **830,754**

[22] Filed: **Sep. 6, 1977**

[51] **Int. Cl.**[2] **H04L 9/04**

[52] **U.S. Cl.** ..... **178/22;** 340/149 R; 375/2; 455/26

[58] **Field of Search** ..... 178/22; 340/149 R

[56] **References Cited**

PUBLICATIONS

"New Directions in Cryptography", Diffie et al., *IEEE Transactions on Information Theory,* vol. IT-22, No. 6, Nov. 1976.

Diffie & Hellman, Multi-User Cryptographic Techniques", *AFIPS Conference Proceedings,* vol. 45, pp. 109–112, Jun. 8, 1976.

Primary Examiner—Howard A. Birmiel

Attorney, Agent, or Firm—Flehr, Hohbach, Test

[57] **ABSTRACT**

A cryptographic system transmits a computationally secure cryptogram over an insecure communication channel without prearrangement of a cipher key. A secure cipher key is generated by the conversers from transformations of exchanged transformed signals. The conversers each possess a secret signal and exchange an initial transformation of the secret signal with the other converser. The received transformation of the other converser's secret signal is again transformed with the receiving converser's secret signal to generate a secure cipher key. The transformations use non-secret operations that are easily performed but extremely difficult to invert. It is infeasible for an eavesdropper to invert the initial transformation to obtain either conversers' secret signal, or duplicate the latter transformation to obtain the secure cipher key.

8 Claims, 6 Drawing Figures

Ralph Merkle

Merkle at the Singularity Summit 2007

Born	February 2, 1952 (age 71) Berkeley, California, US
Education	UC Berkeley (B.A., 1974; M.S., 1977) Stanford University (Ph.D., 1979)
Known for	Co-inventor of public key cryptography Merkle tree[1] Merkle's puzzles Merkle–Hellman knapsack cryptosystem Merkle–Damgård construction

Contributions [edit]

While an undergraduate, Merkle devised Merkle's Puzzles, a scheme for communication over an insecure channel, as part of a class project.[3] The scheme is now recognized to be an early example of public key cryptography. He co-invented the Merkle–Hellman knapsack cryptosystem, invented cryptographic hashing (now called the Merkle–Damgård construction based on a pair of articles published 10 years later that established the security of the scheme), and invented Merkle trees. The Merkle–Damgård construction is at the heart of many hashing algorithms.[4][5] While at Xerox PARC, Merkle designed the Khufu and Khafre block ciphers, and the Snefru hash function.

Continuing with his studies, in 1979 he obtained his **PhD in Electrical Engineering** in the **University of Stanford**. To do this, he presented one of the most advanced cryptography works of its time, "**Secrecy, authentication, and public key systems (Secret, authentication and public key systems) "**. In this paper, Merkle discussed public key systems and their advantages in offering more robust security structures.

Beginnings in cryptography

Merkle's work as a cryptographer began before the end of his stay at Berkeley. It was during this period, under the guidance of **Lance Hoffmann**, when Merkle presented his first work for the creation of a public encryption system. Merkle presented his development to Hoffman, who rejected it without further explanation. However, Merkle continued working on it to continue improving it. What Merkle did not know at the time was that his research was going to be completely revolutionary. No one had worked on the concept of public key crypto and there were no experts in that area. All this effort was even before **Whitfield diffie** y **Martin hellman** They will create the Diffie-Hellman protocol in 1977.

A Method for Obtaining Digital Signatures and Public-Key Cryptosystems

在 1977 年，Ron Rivest，Adi Shamir 和 Leonard Adleman 这三个人真正提出了一个公钥加密/数字签名算法，也就是我们都知道的 RSA 算法[3]。RSA 算法的提出，标志着公钥密码学在实际中确实是可以实现的。计算机领域是一个理论与应用结合的领域，只有真正实现了的算法才能被广泛认可。早在 2002 年，Rivest、Shamir 和 Adleman 就因共同提出了 RSA 算法而得到图灵奖。Diffie 和 Hellman 得到图灵奖的时间反而晚了 14 年。

我们要明确的是，RSA 算法实际上涵盖了 Diffle 和 Hellman 所提出的所有概念：

- RSA 算法可以用来对数据进行加密，是公钥密码学的一个典型实例
- RSA 算法可以用来实现数字签名，是单向认证的一个典型实例
- RSA 算法的本质是 RSA 陷门单向函数。而且，RSA 安全性所基于的大整数分解问题，至今为止都被认为是唯一可以用来构造陷门单向置换（Trapdoor One-Way Permutation）的方法。
- RSA 算法的安全性可以规约为一个计算复杂性问题。

According to the (very short) introduction, this paper purports to present a practical implementation of Diffie and Hellman's public-key cryptosystem for applications in the electronic mail realm. **If this is indeed the premise, the paper should be rejected both for a failure to live up to it and for its irrelevance**.
I doubt that a system such as this one will ever be practical. The paper does a poor job of convincing the reader that practicality is attainable. For one thing, there is the issue of the number n used to factor the message.
……..

The introduction is only two paragraphs long, the relevant literature is not presented or cited, and there is virtually no comparison with the relevant work in the area. In summary, it looks as if this paper is a mathematical exercise **with little originality** (the authors claim that most of their ideas come from other papers), **too far from practical applicability, running against the established standards, and with a declared application area of dubious feasibility**. Not the kind of material our readers like to see in the journal. **Reject**.

I Introduction

The era of "electronic mail" [10] may soon be upon us; we must ensure that two important properties of the current "paper mail" system are preserved: (a) messages are *private*, and (b) messages can be *signed*. We demonstrate in this paper how to build these capabilities into an electronic mail system.

At the heart of our proposal is a new encryption method. This method provides an implementation of a "public-key cryptosystem," an elegant concept invented by Diffie and Hellman [1]. Their article motivated our research, since they presented the concept but not any practical implementation of such a system. Readers familiar with [1] may wish to skip directly to Section V for a description of our method.

II Public-Key Cryptosystems

In a "public key cryptosystem" each user places in a public file an encryption procedure E. That is, the public file is a directory giving the encryption procedure of each