The Solution of the General Equation for Public Key Distribution Systems

ERNST HENZE

Abstract—A generalization of the public key distribution is derived. It is shown that the public key of any two members must obey a functional equation, which can be solved in a closed mathematical form.

I. Introduction

It is assumed that the reader is familiar with the concept of public key distribution systems, as developed, i.e., by W. Diffie and M. E. Hellman [2]. The most common example of a one-way function is

$$z(x, a) \equiv x^a \pmod{p}. \tag{1}$$

where a is the private key of an arbitrary, but fixed, member of the key system; x is a primitive element of the finite field $GF(p)$; and p is a large prime number. The public keys of two members are then

$$x^a \quad \text{and} \quad x^b \pmod{p},$$

and $x^{ab} = x^{ba}$ is the common key used for encryption and decryption of messages.

II. Generalization of the Public Key Distribution System

Let (a) and (b) be again two arbitrary members of a general public key distribution system with a given fixed one-way function $f(x, \cdot)$. Let us suppose that (a) and (b) have the private keys a and b, respectively, and that x is a common variable of the system (fixed or fixed for some known period of time). The private keys a and b are elements of a key set C.

If the member (a) wishes to initiate an interchange of secret information with (b), it first extracts the public key $f(x, b)$ of (b) from the key library, $f(x, \cdot)$ being the above-mentioned one-way function. This cryptologically general one-way function could be a bijective mapping from C onto the set of public keys I.

After obtaining $f(x, b)$ from the key library, the member (a) inserts this value into his own public key in place of the variable x:

$$f(f(x, b), a). \tag{2}$$

The member (b) obtains the public key $f(x, a)$ of (a) and inserts it into his public key

$$f(f(x, y), b). \tag{3}$$

It is clear that—with the exception of cryptologically uninteresting generalizations—the transmission process can only start, if the above-mentioned functional equation

$$f(f(x, a), b) = f(f(x, b), a) \tag{4}$$

holds. Assuming I to be an interval $I \subset \mathbf{R}^1$, C a general set, f a function from $I \times C$ into I such that $f(x, c) = y$ has at least one solution $c_0 \in C$ for all $x, y \in I$, J. Aczél shows [1, corollary 1, p. 273] that with arbitrary continuous and strictly monotonic (invertible!) $g: I \to \mathbf{R}^1$ and arbitrary $h: C \to \mathbf{R}^1$,

$$f(x, c) = g^{-1}[g(x) + h(c)] \tag{5}$$

is the general solution of the (4).

An outline of the proof can be found in [1] or in a paper of Hosszu [4]. We only show that (5) is a solution of (4), by using simple arithmetic simplifications:

$$\begin{aligned} f(f(x,a),b) &= g^{-1}\{g[f(x,a)] + h(b)\} \\ &= g^{-1}\{g[g^{-1}(g(x) + h(a))] + h(b)\} \\ &= g^{-1}\{g(x) + h(a) + h(b)\} \\ &= g^{-1}\{g(x) + h(b) + h(a)\} \\ &= g^{-1}\{g[g^{-1}(g(x) + h(b))] + h(a)\} \\ &= g^{-1}\{g[f(x,b)] + h(a))\} \\ &= f(f(x,b),a). \end{aligned}$$

We have thereby the following result.

Corollary: Any one-way function of a general public key distribution system must have the form of (5), where the restrictions on the functions g and h are clear and mathematically very loose.

Finally, we can consider again (1). Elementary calculations show that in this case we have (mod p):

$$g(x) = \log \log \sqrt{\quad} \qquad h(a) = \log a.$$

The base of the logarithm can be chosen arbitrarily.

ACKNOWLEDGMENT

I would like to thank Prof. A. Shamir for his valuable ideas during a discussion at the Crypto 1981 meeting in Santa, Barbara, CA.

REFERENCES

[1] J. Aczél, *Lectures on Functional Equations and Their Applications*. New York: Academic, 1966.

[2] W. Diffie and M. E. Hellmann, "New directions in cryptography," *IEEE Trans. Inform. Theory*, vol. IT-22, pp. 644–654, 1976.

[3] E. Henze, "Kryptographie und Nachrichtenüber tragung," in *Informationsverarbeitung und Kommunikation*. München: R. Odenbourg Verlag, 1979.

[4] M. Hosszü, "Note on commutable mapping," *Public. Math.* Tom. 9, pp. 105–106, 1962.

Manuscript received September 22, 1981; revised January 7, 1982. This paper was presented in part at IEEE—Meeting Crypto '81, Santa Barbara, CA.

E. Henze is with the Institut für Angewandte Mathematik, Technische Universität Braunschweig, Pockelsstrabe 14, 3300 Braunschweig, Fed. Rep. Germany.