A Public Key Analog Cryptosystem

George I. Davida & Gilbert G. Walter

University of Wisconsin-Milwaukee
Milwaukee,WI 53201
USA

In this paper we present a public key cryptosystem based on error correcting codes [1, 7, 15]. The new public key system is obtained by extending the public key cryptosystem of McEliece [6, 12].

In this scheme a message M, consisting of a column vector of k elements from a finite field is first scrambled by multiplying it by a non singular matrix Q to get

$$M' = Q\ M$$

This scrambled message has parity check variables added to it, by multiplying it by a generator matrix G and then has all the variables reordered by multiplication by a permutation matrix P. Noise is then added to obtain the encrypted message

$$C = P\ G\ Q\ M\ + Z \tag{1}$$

The product of the three matrices $G' = P\ G\ Q$ is made public, but the factors are not.

The analogs of these matrix operations are integral transforms, while the column vectors are functions which we take to be square integrable on (0,1) or (0,2) [2-5, 11, 13, 14, 18]. The message M will now be denoted by $x =. x(t)$, and $x' = Q\ x$ will mean

$$x'(t) = \int_0^1 q(t,s)\, x(s)\, ds \tag{2}$$

where $q(t,s)$ is the kernel of the transformation. P will be a similar operator except that it must be an orthogonal operator to avoid changing the magnitude of the noise. This noise will consist of a realization of a random process $z(t)$ on (0,2). The operator G will have a special form to be discussed below.

In the McEliece digital scheme, the matrix $G = \left| \begin{matrix} I \\ -A \end{matrix} \right|$ where the submatrix A introduces the new variables [12]. Decryption is accomplished by multiplying both sides of

The research reported in this paper was supported in part by NSF grant DCR-8504620.

D. Chaum and W.L. Price (Eds.): Advances in Cryptology - EUROCRYPT '87, LNCS 304, pp. 143-147, 1988.

$$P^T\, C = G\ Q\ M\ +\ P^T Z \tag{3}$$

by a matrix $H\ =\ [A\ \ I\,]$. This annihilates the term $G\ Q\ M$ and leaves the syndrome $S\ =\ H\ P^T\ C$ on the left. Coding Theory is used to estimate P^{TZ} which in turn is used with (3) to estimate $G\ Q\ M$. An estimate for M then is obtained by a projection operator followed by Q^{-1}.

In the analog scheme G is based on a kernel $k\,(t\,,s\,)$, $t\,,s\,\epsilon(0,1)$ and is given by

$$(Gx\,)(t\,) = \int_0^1 \{\ \delta(t-s\,) - k\,(t-1,s\,)\ \}\ x\,(s\,)\ ds\,,\quad 0< t\ < 2$$

and H is given by

$$(Hy\,)(t\,) = \int_0^1 k\,(t\,,s\,)\ y\,(s\,)\ ds\ +\ \int_1^2 \delta(t+1-s\,)\ y\,(s\,)\ ds\,,\quad 0< t < 1.$$

Clearly both are continuous operators and $H\ G\ =\ 0$. The analog encryption consists of first operating with Q , then G, then P on x and then adding noise, i.e. the ciphertext is

$$y = \ P\ G\ Q\ x + Z \tag{4}$$

where $y\ =\ y\,(t\,)$ is in L^2 (0,2). The kernel $q\,(t\,,s\,)$ of the operator Q may be taken to be a Green's function of appropriate differential operator. The kernel $p\,(t\,,s\,)$ of P may be taken to be

$$p\,(t\,,s\,) = \sum_n\ \phi_{i\,(n\,)}\,(t\,)\ \phi_n\,(s\,)$$

where $\{\phi_n\}$ is a complete orthonormal system in L^2 (0,2), and $i\,(n\,)$ is a permutation of the integers. In general this will be a singular kernel, (i.e. not an L^2 function) but in practical cases will be approximated by a finite sum.

The kernel $k\,(t\,,s\,)$ is chosen to be of the form

$$k\,(t\,,s\,) =\ \sum_n \psi_n\,(s\,)\delta(t-t_n)$$

where $\{\psi_n\}$ is again an orthonormal system, the Rademacher system, which takes the values $+-1$ and $\{t_n\}$ is a dense sequence of numbers in (0,1). The number of terms in the series will again be a finite number in practical situations and the impulse δ will be approximated by a function. Furthermore the integral transform

$$\int_0^1 k(s,t)\,y(s)\,ds = \sum_n \psi_n(t)\,Y(n)$$

(in which is $y(s)$ happens to be white noise) gives us a finite sum of independent normal random variables.

Decryption begins by operating with H on

$$P^{-1}\,y = G\ Q\ x + P^{-1}\,Z$$

to obtain the syndrome $S = HP^{-1}y$. The value of $P^{-1}Z$ of minimum error which satisfies

$$H\ Z' = H\ P^{-1}Z = S$$

is then found. This can be done by using the generalized inverse

$$\hat{Z}' = H^*\ (H\ H^*)^{-1}S$$

where H^* is the adjoint operator. This then is used to estimate $P^{-1}Z$ and $P^{-1}y - \hat{Z}'$ restricted to (0,1) is used to estimate Qx which is then inverted to obtain the estimate of the message.

The final estimate cannot be made completely noise free as in the digital case but the noise can be reduced by this method. The reason noise could be eliminated completely in the digital case is that there is a minimum distance between a correct and an incorrect message. This is nor longer true in the analog case in which an incorrect message can be arbitrarily close to the correct message. Thus the best that can be done is to reduce the variance of the noise by means of a decoding algorithm.

The error between the true noise and the estimated noise may be shown, after a few manipulations, to be given by

$$e = G(G^*G)^{-1}G^*Z$$

This in turn can be shown to be the average of a finite number of independent normal random variables with variance σ^2 which has a variance approaching zero as the number of terms increases.

Fortunately in analog signals it is unnecessary to obtain the exact correct message since in most cases it suffices to obtain a message close to the correct one. In voice transmissions, for example, messages slightly corrupted by noise can be understood.

The three operators P, G and Q can be combined in a single integral transform which can then serve as a public key. The security of this arrangement will be at least as good as the original scheme of McEliece. This is particularly true if Q is taken to be a Green's function operator as in [5]. However in this case the inverse would involve noise amplification and must be balanced against the noise reduction of G.

References

[1] Berlekamp, E., *Algebraic Coding Theory*, McGraw Hill, New York (1968).

[2] Blum, J., Susarla, V., and Walter, G., "Estimation of the Prior Distribution Using Differential Operators," *Colloquia Mathematica Societatis*, (1980).

[3] Coddington, E.A. and Levinson, N., *Theory of Ordinary Differential Equations*, McGraw Hill, New York (1955).

[4] Davida, G., Gilbertson, C., and Walter, G., "Analog Cryptosystems," *Eurocrypt85*, (1985).

[5] Davida, G. and Walter, G., "A Class of Analog Cryptosystems," *SECURICOM 87*, (1987).

[6] Denning, D., *Cryptography and Computer Security*, Addison Wesley, Reading, MA (1982).

[7] Diffie, W. and Hellman, M., "New Directions in Cryptography," *IEEE Transactions on Information Theory* IT-22(6)(1976).

[8] E., Hellman, M., "An Extension of the Shannon Theory Approach to Cryptography," *IEEE Trans. on Info. Theory* **IT-23** pp. 289-294 (May 1977).

[9] Hellman, M., "A Cryptanalytic Time-Memory Tradeoff," *IEEE Transactions on Information Theory* IT-26(4)(1980).

[10] Kak, S. and Jayant, N., "On Speech Encryption Using Waveform Scrambling," *Bell System Technical Journal*, (1977).

[11] Kak, S., "Overview of Analog Signal Encryption," *IEEE Proceedings*, (1983).

[12] McEliece, R., "A Public Key Cryptosystem Based on Algebraic Coding Theory," DSN Progress Rep. 42-44, Jet Propulsion Lab.,Cal Inst. of Tech, Pasadena, CA (Jan., Feb. 1978).

[13] Nashed, M., "Operator-Theoretic and Computational Approaches to Ill-Posed Problems with Apaplications to Antenna Theory," *IEEE Transactions on Antennas and Propogation*, (March 1981).

[14] O'Bryan, T. and Walter, G., "Mean Square Estimation of the Prior Distribution," *Sankya, The Indian Journal of Statistics*, (1979).

[15] Rivest, R., Shamir, A., and Adleman, L., "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," *Comm. ACM* Vol 21(2). pp. 120–126 (Feb. 1978).

[16] Shannon, C., "Communcation Theory of Secrecy Systems," *Bell Systems Technical Journal* 28(1949).

[17] Stakgold, I., *Green's Functions and Boundary Value Problems*, Wiley, New York (1975).

[18] Tikhonov, A. and Arsenin, V., *Solutions of Ill-Posed Problems*, Winston-Wiley, New York (1977).

[19] Wyner, A., "An Analog Scrambling Scheme Which Does Not Expand Bandwidth: Part II -Continuos Time," *IEEE Transactions on Information Theory* IT-25(6)(1979).

[20] Wyner, A., "An Analog Scrambling Scheme Which Does NOt Expand Bandwidth: Part I -Discrete Time," *IEEE Transactions on Information Theory* IT-25(3)(1979).