Signature verification: On receiving the signature $\{z_v, r_v, g_v, \beta_v\}$ any t of n verifiers can verify the signature of message m_v. Let t verifiers be denoted as u_i, $i = 1, 2, \ldots, t$, with public information x_i, $i = 1, 2, \ldots, t$. First, they need to work together to generate the public key y_v associated with the secret key s as $y_v = \beta_v^s \bmod p$.

Theorem: With the knowledge of g_v, and t secret shadows, S_i, $i = 1, 2, \ldots, t$, y_v can be generated.

Proof: With the knowledge of the secret shadow S_1, u_1 computes

$$SK1 = g_v^{\left(S_1^{\left(\prod_{j=1, j\neq 1}^{t} \frac{-x_j}{x_1 - x_j} \bmod q\right)} \bmod w\right)} \bmod p$$

$$= g_v^{\left(\alpha^{\left(f(x_1) \prod_{j=1, j\neq 1}^{t} \frac{-x_j}{x_1 - x_j} \bmod q\right)} \bmod w\right)} \bmod p$$

SK1 is sent to u_2. u_2 uses his secret shadow S_2 to compute

$$SK2 = SK1^{\left(S_2^{\left(\prod_{j=1, j\neq 2}^{t} \frac{-x_j}{x_2 - x_j} \bmod q\right)} \bmod w\right)} \bmod p$$

$$= g_v^{\left\{ \left(\alpha^{\left(f(x_1) \prod_{j=1, j\neq 1}^{t} \frac{-x_j}{x_1 - x_j} \bmod q\right)}\right) \times \left(\alpha^{\left(f(x_2) \prod_{j=1, j\neq 2}^{t} \frac{-x_j}{x_2 - x_j} \bmod q\right)}\right) \right\}} \bmod p$$

Just by repeating the same procedure until the tth verifier has used his secret shadow to work on the value obtained from its predecessor, the public key y_v can be finally obtained as

$$SKt = g_v^{\left(\alpha^{\left(\sum_{i=1}^{t} f(x_i) \prod_{j=1, j\neq i}^{t} \frac{-x_j}{x_i - x_j} \bmod q\right)} \bmod w\right)} \bmod p$$

$$= g_v^{\left(\prod_{i=1}^{t} S_i^{\left(\prod_{j=1, j\neq i}^{t} \frac{-x_j}{x_i - x_j} \bmod q\right)} \bmod w\right)} \bmod p$$

$$= g_v^{\alpha^s} \bmod p \quad \text{(from eqn. 1)}$$

$$= {\beta_v}^s \bmod p \quad \text{(from eqn. 2)}$$

$$= y_v \qquad QED$$

The signature of m_v can then be verified by checking the following relation as:

$$ {\beta_v}^{m_v'} = {r_v}^{z_v} {y_v}^{r_v} \bmod p$$

If the above relation does hold, the signature of m_v has been verified.

Security discussion: In this scheme, user A uses the secret key s to sign messages repeatedly; but the corresponding public key y_v is different for each message. This is because y_v is revealed after verifying each message and thus it cannot be used again, otherwise it will lose the property of the shared verification signature scheme. On the other hand, even multiple public keys associated with the same secret key s have been revealed; to derive the secret key we have to solve the discrete logarithm problem. The secret shadow for each verifier is also protected by the discrete logarithm problem during the public key derivation process.

© IEE 1993 23 September 1993
Electronics Letters Online No: 19931355

L. Harn (*Computer Science Telecommunications Program University of Missouri, Kansas City, Kansas City, MO 64110, USA*)

References

1 DE SOETE, M., QUISQUATER, J.-J., and VEDDER, K.: 'A signature with shared verification scheme'. Advances in Cryptology - CRYPTO '89, 20-24 August 1989, (Springer-Verlag, Santa Barbara), pp. 253–262

2 SIMMONS, G.J.: 'A natural taxonomy for digital information authentication schemes'. Advances in Cryptology - CRYPTO '87, 16-20 August 1987, (Springer-Verlag, Santa Barbara), pp. 269–288

3 SHAMIR, A.: 'How to share a secret', *Commun. ACM*, 1979, **22**, pp. 612–613

4 'The digital signature standard', *Commun. ACM*, 1992, **35**, (7), pp. 36–40

5 ELGAMAL, T.: 'A public key cryptosystem and a signature scheme based on discrete logarithms', *IEEE Trans.*, 1985, **IT-31**, pp. 469–472

Modified Chang-Hwang-Wu access control scheme

M.-S. Hwang, W.-P. Yang and C.-C. Chang

Indexing terms: Cryptography, Information theory

It is found that some security classes in the Chang-Hwang-Wu access control scheme can be combined to derive the secret key of their immediate ancestor in some cases. Some slight modifications to the proposed scheme to enhance the security levels are also given.

Introduction: In [1], the authors proposed an efficient cryptographic key assignment scheme for solving the access control problem in a partially ordered hierarchy. Basically, the scheme is based on the Newton interpolation method and a predefined one-way function. The scheme not only reduces the amount of storage required for storing public parameters, but also is simple and efficient in generating and derivating keys. However, some security classes can be combined to derive the secret key of their immediate ancestor in some cases. We also give some modifications to slightly modify that subject scheme so that the security will be greatly improved.

Weakness of proposed scheme: In [1], the authors assumed that there is a trusted third party in the system that is responsible for generating and distributing keys. They assigned each security class C_{ij} an associated distinct pair (a_{ij}, b_{ij}) as the public parameter. Assume that the security class C_i has d immediate successors C_{i1}, C_{i2}, ..., C_{id}. The security class C_i, using the Newton interpolation method, constructs an interpolating polynomial $H_i(X)$ of degree d by interpolating on the points $(0, K_i)$, (a_{i1}, b_{i1}), (a_{i2}, b_{i2}),..., (a_{id}, b_{id}) over $GF(P)$. Let $H_i(X) = (K_i + \Sigma_j c_{ij} X^j) \bmod P$, where c_{ij} is an integer between 0 and $P - 1$. The secret key K_{ij} of C_{ij} is calculated by $K_{ij} = f(c_{ij}) \bmod P$, for $j = 1,2,\ldots, d$, where c_{ij} is the coefficient of the term X^j in $H_i(X)$.

The key derivation is quite similar to the key generation. Using the Newton interpolation method, they reconstruct the interpolating polynomial $H_i(X) = (K_i + \Sigma c_{ij} X^j) \bmod P$ by interpolating on points $(0, K_i)$, (a_{i1}, b_{i1}), (a_{i2}, b_{i2}),..., (a_{id}, b_{id}). The secret key of C_{ij} is thus obtained from $K_{ij} = f(c_{ij}) \bmod P$, where c_{ij} is the coefficient of the term X^j in $H_i(X)$.

In the proposed scheme, the pairs of public parameters (a_{ij}, b_{ij})s, the prime number P and the predefined one-way function f are known to all security classes in the hierarchy. The security class C_i only keeps its own secret key K_i secretly.

We now show the weakness in the security of the above scheme. Let C_{i1}, C_{i2},...,C_{id} be d immediate successors of the security class C_i. Because the points (a_{i1}, b_{i1}), (a_{i2}, b_{i2}),..., (a_{id}, b_{id}) for $C_{i1}, C_{i2}, \ldots, C_{id}$, respectively, are known to each security class, we can construct an interpolating polynomial $H_i(X) = (K_i + \Sigma_j c_{ij} X^j) \bmod P$ with one unknown point $(0, K_i)$ and d known points (a_{i1}, b_{i1}), (a_{i2}, b_{i2}),..., (a_{id}, b_{id}), based on the Newton interpolation method [2]. The formula is as follows:

$$H_i(x) = (K_i + g_1(K_i)X + g_2(K_i)X^2 + \cdots + g_d(K_i)X^d) \bmod P \qquad (1)$$

where $g_j(K_i)$ can be represented as a linear polynomial with one unknown variable K_i. (i.e. $g_1(K_i) = g_1K_i + g_0$, g_1, g_0 are two integers.) Now suppose f is a one-way function of degree d. Then the coefficient $g_j(K_i)$ in eqn. 1 is substituted for the function f. Consequently, we have

$$\begin{aligned} f(g_j(K_i)) &= K_j \\ &= (e_{jd}K_i^d + e_{j(d-1)}K_i^{d-1} + \cdots \\ &\quad + e_{j1}K_i + e_{j0}) \bmod P \quad \text{for } j = 1, 2, \cdots, d \end{aligned}$$

We have d equations and d variables, by the Gauss elimination method [3], thus when d immediate successors of the security class C_i collude, the secret key K_i of C_i is revealed. In fact, only one security class is needed to break the scheme when the one-way function is in quadratic residue modulo (i.e. $f(X) = g_2X^2 + g_1X + g_0$ mod P.) [4]. Therefore, when the one-way function is a polynomial of degree d, they need $d - 1$ immediate successors for conspiracy attack.

Modifications and discussions: From the above statements and example, we see that $d - 1$ security classes can attack the one-way function of degree d. We now give two modifications for withstanding this attack.

(i) *Modification 1:* Each security class has its own private one-way function. This means that the one-way function f_i has to be kept secretly by the security class C_i and the third party.

(ii) *Modification 2:* Choose a one-way function of degree $d + 2$ where d is a maximal number of immediate successors of each security class in the whole system.

Although Modification 1 can prevent conspiracy attack, it wastes a large amount of storage space to store these one-way functions. Modification 2 not only keeps the advantage of the proposed scheme but also enhances the security.

Acknowledgment: This research was partially supported by the National Science Council, Taiwan, ROC, under contract no.: NSC82-0408-E-009-161, and by the Telecommunication Laboratories, Taiwan, ROC, under contracts no.: TL-NSC-82-5206.

© IEE 1993 *20 September 1993*
Electronics Letters Online No: 19931391

M.-S. Hwang and W.-P. Yang (*Department of Computer and Information Science, National Chiao Tung University, Hsinchu, Taiwan 300, Republic of China*)

C.-C. Chang (*Institute of Computer Science and Information Engineering, National Chung Cheng University, Chiayi, Taiwan 621, Republic of China*)

M.-S. Hwang is also with the Directorate General of Telecommunication Laboratories, Ministry of Transportation and Communications, Chung Li, Taiwan 320, Republic of China

References

1 CHANG, C.C., HWANG, R.J., and WU, T.C.: 'Cyptographic key assignment scheme for access control in a hierarchy', *Information Systems*, 1993, **17**, (3), pp. 243–247

2 KNUTH, D.E.: 'The art of computer programming, Vol 2: seminumerical algorithm' (MA: Addison-Wesley, 1980)

3 NOBLE, B., and DANIAL, J. W.: 'Applied linear algebra, 2nd Edn.' (Prentice-Hall, 1977)

4 SCHROEDER, M.R.: 'Number theory in science and communication, 2nd Edn.' (Springer-Verlag, 1985)

Measuring technique for characterising the electrical properties of piezoelectric tubular devices

A.M. Sabatini and P. Dario

Indexing terms: Piezoelectric devices, Polymers

The Letter describes a simple measuring technique which is useful for characterising in a nondestructive manner the electrical properties of tubular devices made from piezoelectric polymers. The proposed measuring technique allows us to estimate the so-called d_{33}^* constant, a parameter often used for evaluating piezoelectric activity.

Introduction: Recent substantial advances in the production of synthetic polymers have made possible the conception, fabrication and testing of a variety of medical devices to be used in basic research as well as in clinical investigations. Among them, piezoelectric materials, such as polyvinylidene fluoride (PVDF) [1], or electret materials, such as polytetrafluoroethylene (PTFE) [2], have been proposed and used as guidance channels, that is small tubular devices, in a number of applications that require some physical agents for promoting regenerative processes. The ability of piezoelectric materials to enhance tissue regeneration is believed to be an effect of their electrical properties. Hence, simple means for characterising these properties in a nondestructive manner are required. A thorough investigation of the properties of piezoelectric materials requires considerable effort [3]; in some cases, however, a simple characterisation is sufficient for the purpose of comparing different devices under identical operating conditions [4], so as to select samples with roughly equivalent properties for the intended application.

Theory of measurement: The aim of this Letter is to describe the simple apparatus we propose for measuring the so-called d_{33}^* constant of piezoelectric tubular devices. Refer to Fig. 1 for an explanation of the terms and notation usually adopted in dealing with piezoelectric planar films [3]. The transverse and machine directions refer to the directions along which the mechanical stretching of the film must be exerted; the poling direction relates to the direction of the electric field to be applied to the stretched material during the fabrication of the device. Both processing steps are necessary for inducing proper conformation changes in the crystalline structure of the polymer so as to make it piezoelectrically active.

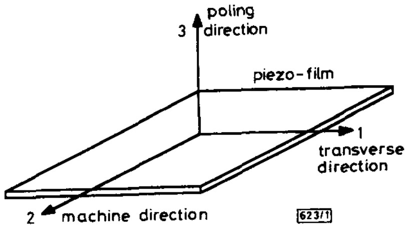

Fig. 1 *Axis nomenclature for piezoelectric films*

Piezoelectric measurements on polymer films are usually made by properly applying a mechanical tension to the sample and measuring the short-circuit charge or the open circuit voltage on opposing electrodes. Owing to the anisotropy of piezoelectric materials, it is important to specify the directions along which the mechanical tension is applied or the electrodes are placed. The d_{33}^* constant is defined as

$$d_{33}^* = \frac{\Delta Q}{\Delta F} \qquad (1)$$

where ΔQ is the charge developed in a double-sided metallised film of piezoelectric material with surface area A, as a consequence of a force ΔF applied in the normal direction, that is direction 3 in Fig. 1. Let E denote the transverse electric field existing between the two electrodes. The underlying boundary condition $E=0$ is assumed for eqn. 1, therefore the electrodes must be short-circuited: when the charge ΔQ is measured by a charge amplifier, the short-circuit conditions are virtually met. The d_{33}^* constant is