Character Recognition Systems Conference [5]. Typical recognition rates were around 95% on the digits, with only one system (based on a set of multilayer perceptrons) approaching the human performance of 98.5%. For a system using less than 0.05% of the training data, the n-tuple method seems quite respectable. Extension of these preliminary tests to the full dataset would be an interesting project.

Similar tests were run using various tuple sizes from 2 to 10, with qualitatively similar results. Recognition accuracy is poor for 2-tuples, best for 4-tuples, and degrades slightly as the size increases beyond 4.

Conclusions: These results demonstrate in character recognition applications that the test-before-train heuristic provides a convenient way to control saturation in an n-tuple recogniser, thereby making efficient use of the available training data.

© IEE 1993 *20 September 1993*
Electronics Letters Online No: 19931390

R. Tarling (*92 Elmcroft Ave., Wanstead, London E11 2DB, United Kingdom*)

R. Rohwer (*Dept. of Computer Science and Applied Mathematics, Aston University, Aston Triangle, Birmingham B4 7ET, United Kingdom*)

References

1 BLEDSOE, W.W., and BROWNING, I.: 'Pattern recognition and reading by machine'. Proc. Eastern Joint Computer Conf., 1959, (Boston), pp. 232–255

2 ROHWER, R., and CRESSY, D.: 'Phoneme classification by Boolean networks'. Proc. European Conf. on Speech Communication and Technology, 1989, (Paris), pp. 557–560

3 ROHWER, R., and LAMB, A.: 'An exploration of the effect of super large n-tuples on single layer ramnets', in ALLINSON, N., Ed. 'Proceedings of the weightless neural network workshop '93, Computing with logical neurons' (University of York, 1993), pp. 33–37

4 TARLING, R.: 'Computer recognition of hand-printed characters using weightless neural networks'. Final year project report, Dept. of Computer Science and Applied Mathematics, Aston University, Birmingham, UK, 1993

5 WILKINSON, R., GEIST, J., JANET, S., GROTHER, P., BURGES, C., CREECY, R. HAMMOND, R., HULL, J., LARSEN, N., VOGL, T., and WILSON, C.: 'The first census optical character recognition systems conference'. Technical Report NISTIR 4912, National Institute of Standards and Technology, Gaithersburg, MD, USA, 1992

Digital signature with (*t*, *n*) shared verification based on discrete logarithms

L. Harn

Indexing terms: Information theory, Public-key cryptography

The Letter presents a digital signature scheme based on the discrete logarithm problem which enables any t of the n verifiers to verify the validity of the signature.

Introduction: The digital signature with (t, n) shared verification is the same as regular digital signatures which consists of a string of binary numbers generated by a single user with the knowledge of a secret key, except that the signature verification has the following properties:

(i) any t of the n verifiers can verify the validity of the signature

(ii) any t–1 or fewer verifiers cannot verify the validity of the signature.

This definition is very similar to the definition of a (t, n) secret sharing scheme. However, the major differences are:

(i) in the secret sharing scheme, because the secret shadows are exchanged among users and the master key is derived after each secret reconstruction process, the master key can only be used once if no other encryption scheme has been used; but, in a shared verification signature scheme, because the secret shadows and the master key are used to verify the signature, it may never be revealed in the cleartext form and thus the master key and secret shadows can be used repeatedly

(ii) in the shared verification signature scheme, the master key corresponds to the public key used in the digital signature schemes and by knowing only the public key, it is still infeasible to obtain the secret key used to sign the message.

Soete *et al.* [1] proposed a (t, n) shared verification signature scheme in 1989 based on generalised quadrangles. It requires the use of secure boxes for the verifiers to verify the signature. The possible applications of this signature scheme can be found in [1,2]. In this Letter, we propose a signature scheme with (t, n) shared verification based on the computational difficulty of discrete logarithms.

Proposed signature scheme with (t, n) shared verification: p = a prime modulus where $2^{511} < p < 2^{512}$; $w = (p - 1)/2$, a large prime, where $2^{510} < w < 2^{511}$ q = a prime divisor of $w - 1$, where $2^{159} < q < 2^{160}$; s = a secret integer for the user with $0 < s < q$; $y_v = \beta_v^s$ mod p, for $v = 1, 2, \ldots$, where y_v is the public key for the signer used for message m_v, and β_v is a generator with order w in $GF(p)$; $\{a_i$, for $i = 1, \ldots, t - 1\}$, and $f(x) = s + a_1x + \ldots + a_{t-1}x^{t-1} \bmod q$, each a_i is a random integer with $0 < a_i < q$; $\{g_v$, for $v = 1, 2, \ldots\}$, where $g_v = h_v^{(p-1)/w} \bmod p > 1$; each h_v is a random integer with $0 < h_v < p$; each g_v is a generator with order w in $GF(p)$, thus we have $g_v^t \bmod p = g_v^{t \bmod w} \bmod p$ for any non-negative integer t; $\alpha = e^{(w-1)/q} \bmod w > 1$, e is a random integer with $0 < e < w$; α is a generator with order q in $GF(w)$, thus we have $\alpha^t \bmod w = \alpha^{t \bmod q} \bmod w$, for any non-negative integer t; m_v, for $v = 1, 2, \ldots$, are messages to be signed and transmitted; k_v, for $v = 1, 2, \ldots$, are random integers with $0 < k_v < w$; H = a one-way hash function.

Integers $\{a_i, i = 1, \ldots, t - 1\}$ are secret values, and p, w, q, and g_v, for $v = 1,2, \ldots$, are public values. The signer's private and public keys are s and y, for $v = 1, 2, \ldots$, respectively. s, α, and k_v must be kept secret. k_v must be changed for each signature.

Shadow generation: Our scheme uses the cryptographic techniques of the perfect secret sharing scheme of Shamir [3] based on the Lagrange interpolating polynomial and the digital signature algorithm [4] proposed by NIST.

Let A be the signer and s be the secret key used by A to sign messages. A is responsible for generating secret shadows for all verifiers. A selects the $(t - 1)$ th degree polynomial $f(x) = s + a_1 x + \ldots + a_{t-1}x^{t-1} \bmod q$. The shadows for each verifier are computed as $S_i = \alpha^{f(x_i)} \bmod w$, where x_i is the public information associated with the verifier u_i. We would like to point out here that with any t pairs of (x_i, S_i), α^s can be determined as $\alpha^s = \alpha^{f(0)} \bmod w$

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

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

Signature generation: The signature scheme is based on the ElGamal signature scheme [5] with some modifications. Assume A wants to sign a message m_v, where $0 \le m_v \le p - 1$. With the knowledge of the secret key s, A can find β_v to satisfy the relation

$$g_v \alpha^s = \beta_v{}^s \bmod p \qquad (2)$$

We have defined $y_v = \beta_v^s \bmod p$. A then randomly selects an integer k_v, where $0 \le k_v \le w - 1$, and computes

$$r_v = \beta_v{}^{k_v} \bmod p$$

A now solves the congruence

$$m_v{}' = k_v z_v + s r_v \bmod w$$

or

$$z_v = (m_v{}' - s r_v) k_v{}^{-1} \bmod w$$

for integer z_v, where $0 \le z_v \le w - 1$ and $m_v' = H(m_v)$. $\{z_v, r_v, g_v, \beta_v\}$ is the signature for message m_v.

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, ..., t, with public information x_i, i = 1, 2, ..., 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, ..., t, y_v can be generated.

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

$$\begin{aligned} SK1 &= g_v^{\left(S_1^{\left(\prod_{j=1,j\neq1}^{t}\frac{-x_j}{x_1-x_j} \bmod q\right)} \bmod w\right)} \bmod p \\ &= g_v^{\left(\alpha^{\left(f(x_1)\prod_{j=1,j\neq1}^{t}\frac{-x_j}{x_1-x_j} \bmod q\right)} \bmod w\right)} \bmod p \end{aligned}$$

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

$$\begin{aligned} SK2 &= SK1^{\left(S_2^{\left(\prod_{j=1,j\neq2}^{t}\frac{-x_j}{x_2-x_j} \bmod q\right)} \bmod w\right)} \bmod p \\ &= g_v^{\left\{\left(\alpha^{\left(f(x_1)\prod_{j=1,j\neq1}^{t}\frac{-x_j}{x_1-x_j} \bmod q\right)}\right) \times \left(\alpha^{\left(f(x_2)\prod_{j=1,j\neq2}^{t}\frac{-x_j}{x_2-x_j} \bmod q\right)}\right)\right\}} \bmod p \end{aligned}$$

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

$$\begin{aligned} SKt &= g_v^{\left(\alpha^{\left(\sum_{i=1}^{t} f(x_i)\prod_{j=1,j\neq i}^{t}\frac{-x_j}{x_i-x_j} \bmod q\right)} \bmod w\right)} \bmod p \\ &= g_v^{\left(\prod_{i=1}^{t} S_i^{\left(\prod_{j=1,j\neq i}^{t}\frac{-x_j}{x_i-x_j} \bmod q\right)} \bmod w\right)} \bmod p \\ &= g_v^{\alpha^s} \bmod p \quad \text{(from eqn. 1)} \\ &= {\beta_v}^s \bmod p \quad \text{(from eqn. 2)} \\ &= y_v \qquad\qquad QED \end{aligned}$$

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,..., 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},...,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:

$$\begin{aligned} H_i(x) =& (K_i + g_1(K_i)X + g_2(K_i)X^2 + \cdots \\ &+ g_d(K_i)X^d) \bmod P \end{aligned} \tag{1}$$

where $g_j(K_i)$ can be represented as a linear polynomial with one