Numerical results: Eqns. 3 are solved by the over-relaxation method [3]. Then the time-stepping for the FDTD method is accomplished in the $\xi\eta$-plane, and centred-difference expressions are used for both the space and time derivatives in eqns. 7 to attain second-order accuracy in the space and time increments.

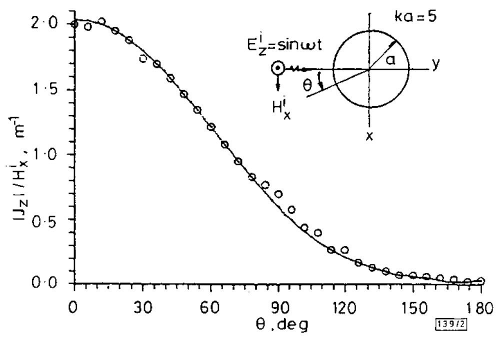

Fig. 2 *Comparison of our results with modal expansion results [5]*

Inset: magnitude of surface current for TM case
O this Letter
—— [5]

As an example, we treated the case of an infinitely long circular conducting cylinder subject to a TM-polarised sinusoidal wave illumination at normal incidence (illustrated in Fig. 2). The radiation boundary is a coaxial cylinder, and Bayliss-Turkel first-order RBC [4] was used. The results (shown in Fig. 2) are in good agreement with model expansion results. Our largest space increment (δ_{max}) is $\lambda/10$, and the RBC is lowest-order accurate, bringing some errors. If we use higher mesh density and higher-order RBC, the results improve.

Conclusion: Our method has been proved effectively. Although only the two-dimensional case is presented in this Letter, there are no fundamental problems in extending it to the three-dimensional case.

Acknowledgments: This work was supported by the Natural Science Foundation of China.

28 October 1994
Electronics Letters Online No: 19950182

Cheng Liao, Yu-shen Zhao and Wei-gan Lin (*Institute of Applied Physics, University of Electronic Science and Technology of China, Chengdu, Sichuan 610054, People's Republic of China*)

References

1 HOLAND, R.: 'Finite difference solutions of Maxwell's equations in generalized nonorthogonal coordinates', *IEEE Trans Nucl. Sci.*, 1983, **30**, (6), pp. 4689–4691

2 FUSCO, M.: 'FDTD algorithm in curvilinear coordinates', *IEEE Trans. Antennas Propag.*, 1990, **38**, (1), pp. 76–89

3 THAMES, F.C., THOMPSON, J.F., MASTIN, C.W., and WALKER, R.A.: 'Numerical solutions for viscous and potential flow about arbitrary two-dimensional bodies using body-fitted coordinates systems', *J. Comput. Phys.*, 1977, **24**, pp. 245–273

4 BAYLISS, A., and TURKEL, E.: 'Radiation boundary conditions for wavelike equations', *Commun. Pure Appl. Math.*, 1980, **33**, pp. 707–725

5 BLADEL, J.V.: 'Electromagnetic fields' (McGraw-Hill, New York, 1964)

Comment

Multistage secret sharing based on one-way function

L. Harn

Indexing term: Cryptography

Introduction: He and Dawson recently proposed a multistage (t, n) secret sharing (MSS) scheme [1] to share multiple secrets based on any one-way function. The public shift technique is used to implement MSS. For k secrets shared among n participants, each participant has to keep only one secret; but there are a total of kn public values. In this Letter, the author shows an alternative implementation which requires the same number of secrets for each participant to keep; but there are only a total of $k(n - t)$ public values. This implementation becomes very attractive, especially when the threshold value t is very close to the number of participants n.

New scheme: Let $f: Z_p \to Z_p$ be any one-way function. $f^j(x)$ denotes j successive applications of f to x, i.e. $f^0(x) = x$ and $f^j(x) = f(f^{j-1}(x))$. A trust dealer randomly selects n distinct integers, $x_i \in [n - t+1, p-1]$, for $i = 1, 2, ..., n$, as participants' public information and n random integers, $y_i \in [1, p-1]$, for $i = 1, 2, ..., n$, (i.e. y_i not necessarily distinct) as participants' secret values. The dealer will do the following:

(i) For $j = 0, 1, ..., k-1$, repeat the following steps:

(a) Compute $f^j(y_i)$, for $i = 1, 2, ..., n$.

(b) Reconstruct an $(n-1)$th degree Lagrange interpolation polynomial [2] $h_j(x)$ which passes through the co-ordinates $(x_i, f^j(y_i))$, for $i = 1, 2, ..., n$ and $h_j(0) = s_j$ is the jth stage secret to be shared among participants.

(c) Compute $(n-t)$ public values as $h_j(m)$, for $m = 1, 2, ..., n-t$.

(ii) Deliver y_i to each participant and publish all public values.

The secrets should be reconstructed in the following order: $s_{k-1}, s_{k-2}, ..., s_1, s_0$. When trying to reconstruct the secret s_j, each involved participant should submit his secret share $f^j(y_i)$. With the knowledge of t secret shares and $(n-t)$ additional public shares, $h_j(m)$, for $m = 1, 2, ..., n-t$, a unique Lagrange interpolation polynomial $h_j(x)$ can be determined and the secret $h_j(0) = s_j$ can be obtained.

Complexity: For k secrets shared among n participants, each participant has to keep only one secret; but there are only a total of $k(n-t)$ public values. Our implementation becomes very attractive, especially when the threshold value t is very close to the number of participants n. For example, for multistage (n, n) secret sharing there is no public value.

5 December 1994
Electronics Letters Online No: 19950201

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

References

1 HE, J., and DAWSON, E.: 'Multistage secret sharing based on one-way function', *Electron. Lett.*, 1994, **30**, (19), pp. 1591–1592

2 SHAMIR, A.: 'How to share a secret' *Commun. ACM*, 1979, **22**, (11), pp. 612–613