dimensional space. The profile of the object is then obtained using spline interpolation. Next, the method of moments (MoM) solution to the electric field integral equation is used as the forward electromagnetic solver to generate the computed scattered field E^{cal} from each assumed shape. A cost function is defined as the root-mean-squared (rms) difference between E^{cal} and the measured scattered-field E^{mea}. The HGA-tabu algorithm is then applied as the optimiser to minimise the cost function. Binary-encoded GA is used in our implementation.

Results: We have applied the HGA-tabu algorithm to reconstruct the shape of a metallic, partially open, circular cylindrical cavity with a diameter of 10.8 cm (Ips011 in the Ipswich data set) [9]. The measurement was taken at a single frequency of 10 GHz in a bistatic configuration. There were a total of 36 transmitter positions around the object and 18 receiver locations for each transmitter position. The electric field was parallel to the axis of the cylinder.

The number of the population for GA was set to 200, the geometry was described by $N=5$ points, and the crossover and mutation rates were set to 0.8 and 0.4, respectively. The search area was chosen to be 16.2×16.2 cm. We first tested the inversion algorithms using MoM-simulated field data as the input. The results showed that the HGA-tabu was able to converge to the correct shape after an average of 75 generations and the final shape was in excellent agreement with the actual shape. In comparison to the HGA, the HGA-tabu also showed an improvement of about 100 generations for convergence.

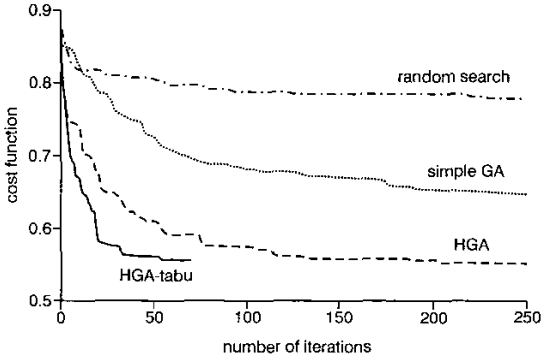

Fig. 2 *Convergence comparison for inversion of Ips011 for random search, simple GA, HGA and HGA-tabu*

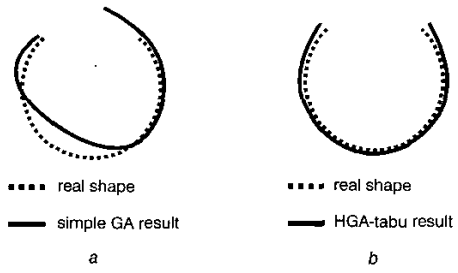

Fig. 3 *Ips011 inversion results from measured data*
a Typical inversion result by simple GA
b Typical inversion result by HGA-tabu

Next, we applied the inversion algorithms to the actual measured data for Ips011. Fig. 2 shows the convergence comparison between random search, simple GA, HGA and HGA-tabu. All the results were averaged over 10 independent runs with different initial populations. As expected, the simple GA showed improvement over the random search. The HGA further improved the convergence rate of the simple GA. The best results were consistently obtained by the HGA-tabu. To achieve an rms of 0.55, the HGA required an average of 220 generations while the HGA-tabu algorithm required only an average of 75 generations. (We note here that, due to the difference between the numerical modelling and the measurement, the rms error between the MoM-computed fields from the *exact* shape and the measured field data is 0.73.) Fig. 3*a* shows the typical shape from the simple GA after 250 generations plotted against the real profile of the cavity. The result indicates that more iterations are needed for convergence. Fig. 3*b* shows the typical reconstructed shape from the HGA-tabu after 75 generations. As we can see, the inverted shape is very close to the real profile. The overhead of implementing the gradient search in each generation is about 10% of the total computation cost. The time for the tabu list check is negligible, as there is no cost function evaluation.

Conclusion: An approach combining the hybrid genetic algorithm with the tabu list concept has been proposed in this Letter. The tabu list was set up to increase the search efficiency by forbidding revisits of local minima already explored by the local search. The algorithm has been applied to reconstruct the shape of a metallic cavity based on the measured Ipswich data. Inversion results from the HGA-tabu showed faster convergence and higher success rate than those of the simple GA and hybrid GA. The computation overhead per generation for the new algorithm was small. The algorithm could potentially be useful in other optimisation problems.

Acknowledgment: This work is supported by the Office of Naval Research under Contract No. N00014-03-1-0021.

6 November 2002
Electronics Letters Online No: 20030207
DOI: 10.1049/el:20030207

Yong Zhou and Hao Ling (*Department of Electrical and Computer Engineering, The University of Texas at Austin, Austin, TX 78712-1084, USA*)

Junfei Li (*Department of Electrical Engineering, The University of Texas-Pan American, Edinburg, TX 78539, USA*)

References

1 CHIU, C.C., and LIU, P.T.: 'Image reconstruction of a perfectly conducting cylinder by the genetic algorithm', *IEE Proc., Microw. Antennas Propag.*, 1996, **143**, (3), pp. 249–253
2 PASTORINO, M., MASSA, A., and CAORSI, S.: 'A microwave inverse scattering technique for image reconstruction based on a genetic algorithm', *IEEE Trans. Instrum. Meas.*, 2000, **49**, pp. 573–578
3 ZHOU, Y., and LING, H.: 'Electromagnetic inversion of Ipswich objects with the use of the genetic algorithm', *Microw. Opt. Tech. Lett.*, 2002, **33**, pp. 457–459
4 YEN, J., LIAO, J.C., LEE, B., and RANDOLPH, D.: 'A hybrid approach to modeling metabolic systems using genetic algorithm and simplex method', *IEEE Trans. Syst. Man Cyber.*, 1998, **28**, pp. 173–283
5 PARK, C., and JEONG, B.: 'Reconstruction of a high contrast and large object by using the hybrid algorithm combining a Levenberg-Marquardt algorithm and a genetic algorithm', *IEEE Trans. Magn.*, 1999, **35**, pp. 1582–1585
6 GLOVER, F.: 'Tabu search—part I', *ORSA J. Comput.*, 1989, **1**, pp. 190–206
7 GLOVER, F., and LAGUNA, M.: 'Tabu search: modern heuristic techniques for combinatorial problems' (Blackwell Scientific Publication, Oxford, UK, 1993)
8 OTTO, G.P., and CHEW, W.C.: 'Microwave inverse scattering-local shape function imaging for improved resolution of strong scatters', *IEEE Trans. Microw. Theory Tech.*, 1994, **42**, pp. 137–141
9 MCGAHAN, R.V., and KLEINMAN, R.E.: 'Second annual special session on image reconstruction using real data', *IEEE Antennas Propag. Mag.*, 1997, **39**, pp. 7–9

Publicly verifiable authenticated encryption

Changshe Ma and Kefei Chen

A new authenticated encryption scheme with public verifiability is presented. The new scheme requires less computational costs and communication overhead than the conventional signature-then-encryption approaches. Furthermore the message is not divulged during the public verification.

Introduction: Secure and authenticated message deliver/storage is one of the major aims of computer and communication security research. Horster, Michels and Petersen (HMP for short) [1] proposed an efficient authenticated encryption scheme with lower expansion

rate, computation costs, and communication costs. Lee and Chang [2] modified the HMP scheme with the same merits but without the use of a one way function. However, neither of them has the public verifiability.

Public verifiability: It is computationally feasible for a judge (who may be the arbiter of the system) to verify the sender's signature without divulging the receiver's private key and the message.

It is necessary for an authenticated encryption scheme to have public verifiability to implement the non-repudiation. Zheng [3] introduced a new type of authenticated encryption termed 'signcryption' which simultaneously satisfies unforgeability, confidentiality, and non-repudiation: but its non-repudiation protocol is inefficient as it is based on the zero-knowledge proof protocol, especially when the non-repudiation procedure is always executed.

In this Letter, we propose an authenticated encryption scheme with public verifiability. Our scheme is as efficient as the signcryption in [3] with respect to both computational costs and the communication overhead. In addition, our scheme has an efficient non-repudiation procedure without using the zero-knowledge proof protocol.

Proposed scheme: Initially, two large primes p and q with $q|(p-1)$ and an element $g \in Z_p^*$ of order q are computed by a trusted third party (TTP for short) and are authenticated to each user. Each user $i \in \{A, B\}$ chooses a secret key $x_i \in Z_q^*$ and computes his public key $y_i \equiv g^{x_i} \bmod p$. He publishes y_i which is certified by the TTP and keeps x_i secret. In addition, the TTP chooses a public one way hash function H with $|H| < |p|$, where $|x|$ denotes the number of bits in x and $|H|$ denotes the number of bits in the output value of hash function H. To send message $m \in Z_p^*$, Alice does the following:

(A-1) picks a random number $k \in Z_q^*$
(A-2) computes $v \equiv (g \cdot y_B)^k \bmod p$ and $e \equiv v \bmod q$
(A-3) computes $c \equiv m \cdot (H(v))^{-1} \bmod p$
(A-4) computes $r = H(e, H(m))$
(A-5) computes $s = k - x_A \cdot r \bmod q$

Alice then sends (c, r, s) to Bob. After receiving (c, r, s), Bob does the following:

(B-1) computes $v \equiv (g \cdot y_B)^s \cdot y_A^{r(x_B+1)} \bmod p$ and $e \equiv v \bmod q$
(B-2) recovers the message $m \equiv c \cdot H(v) \bmod p$
(B-3) verifies $r = H(e, H(m))$

For public verification, Bob computes

$$K_1 \equiv (y_B^k \bmod p) \bmod q \equiv (y_B^s \cdot y_A^{r x_B} \bmod p) \bmod q$$

and forwards $(H(m), K_1, r, s)$ to an arbitrary TTP. To verify that Alice is the originator of the encryption and signature, the TTP does the following:

(TTP-1) computes $e \equiv (g^s \cdot y_A^r \cdot K_1 \bmod p) \bmod q$
(TTP-2) verifies $r = H(e, H(m))$

Our scheme is best used for small message transmission, but it can be adapted for the case of a long message as follows. Alice partitions message m into $(|p|-1)$-bit blocks $m_1, \ldots, m_t$ (use padding if necessary), and she computes the ciphertext blocks $c_1, \ldots, c_t$ by $c_i = (m_i \oplus c_{i-1}^l) \cdot (H(v))^{-1} \bmod p$ (where c_i^l denotes the most left $(|p|-1)$ bits of c_i and $c_0 = v$) and r, s by (A-4) and (A-5), respectively. Alice than sends $(c_1, \ldots, c_t, r, s)$ to Bob. The rest of the scheme can be modified correspondingly.

Security considerations: Basically, a secure authenticated encryption scheme should satisfy the following properties: unforgeability, confidentiality, and non-repudiation. We now analyse the security properties of our scheme.

Unforgeability: Regarding forging Alice's signature, a dishonest Bob is in the best position to do so, as he is the only person who knows x_B which is required to directly decrypt and verify Alice's encryption and signature, i.e. the dishonest Bob is the most powerful attacker we should look at. Given (c, r, s) generated by Alice, Bob can use his private key to decrypt c and obtain m. Thus the original problem is reduced to one in which Bob is in possession of (m, r, s). The latter is equivalent to the Schnorr's digital signature which is unforgeable [4]. Therefore we conclude that our scheme is unforgeable against adaptive attacks.

Non-repudiation: Once Bob computes $K_1 \equiv (y_B^k \bmod p) \bmod q$, everyone can verify the signature (r, s) of the message m. Therefore it is computationally feasible for any TTP to settle a dispute between Alice and Bob without divulging Bob's private key and the message m.

Confidentiality: If any intruder tries to decrypt the message m, he must first compute at least one of the secrets P_{AB} (the Deffie-Hellman secret key between Alice and Bob), x_B or k. One can know K_1 and compute e, but it is infeasible to compute P_{AB} or v, as discussed in [2]. By known-plaintext attack, one can compute $H(v)$, but it is still infeasible to compute P_{AB}. Therefore our scheme can withstand the known plaintext-ciphertext attack.

Efficiency: To compute an authenticated encryption requires only one exponentiation modulo p, one inversion modulo p, and three hash-function evaluations. Signature generation does not require the computation of inversion modulo q. The cost of decryption and verification includes two exponentiations modulo p, and three hash-function evaluations. For public verifiability, two exponentiations modulo p is needed for Bob and the TTP, respectively. Moreover the TTP needs one hash-function evaluation.

The communication overhead between the sender and receiver is very small, only $|H| + |q|$ bits, the communication cost for public verification being $2(|H| + |q|)$ bits.

Conclusion: We have proposed an efficient authenticated encryption scheme with public verifiability. It has only one exponentiation modulo p for encryption and signature, and two exponentiations modulo p for decryption and verification. In addition, the communication overhead is very small, only $|H| + |q|$ bits, and the non-repudiation procedure is very efficient.

Acknowledgment: This work was partially supported by NSFC under grants 60273049 and 90104005.

9 December 2002
Electronics Letters Online No: 20030190
DOI: 10.1049/el:20030190

Changshe Ma and Kefei Chen (*Department of Computer Science and Engineering, Shanghai Jiaotong University, 1954 Hua Shan Road, Shanghai 200080, People's Republic of China*)

E-mail: mcs@sjtu.edu.cn

References

1 HORSTER, P., MICHELS, M., and PETERSEN, H.: 'Authenticated encryption scheme with low communication costs', *Electron. Lett.*, 1994, **30**, (15), pp. 1212–1213
2 LEE, W.-B., and CHANG, C.-C.: 'Authenticated encryption scheme without using a one way function', *Electron. Lett.*, 1995, **31**, (19), pp. 1656–1657
3 ZHENG, Y.: 'Signcryption and its application in efficient public key solution' ISW'97, *in Lect. Notes Comput. Sci.*, 1998, **1397**, pp. 291–312
4 Pointcheval, D., and Stern, J.: 'Security proofs for signature scheme'. Eurocrypt'96, in *Lect. Notes Comput. Sci.*, 1996, **1070**, pp.387–398.

Precision current and charge amplifiers for driving highly capacitive piezoelectric loads

A.J. Fleming and S.O.R. Moheimani

Piezoelectric transducers are known to be highly capacitive loads that exhibit less hysterisis when driven with current or charge rather than voltage. Compliance feedback current and charge amplifiers are introduced. A secondary output voltage feedback loop is employed to prevent DC charging of capacitive loads and to compensate for any voltage or current offsets in the driver circuit. Low frequency bandwidths in the milliHertz range can be achieved.

Introduction: Piezoelectric transducers have found countless applications in such fields as vibration control, nano-positioning, acoustics and sonar. The piezoelectric effect [1] is a phenomena exhibited by