Digital multisignature with distinguished signing authorities

L. Harn

The digital multisignature is signed by group members with knowledge of multiple private keys. Two ElGamal-type efficient multisignature schemes that can combine all individual signatures into a multisignature without any data expansion have previously been proposed. However, since in these two schemes all group members sign the same message, these schemes are called multisignature schemes with undistinguished signing authorities. The authors now modify these schemes and convert them to a multisignature scheme with distinguished signing authorities. Each group member is responsible for preparing and signing a partial group message.

Introduction: The digital multisignature (also called 'the group signature') is analogous to an ordinary digital signature. Instead of generating the digital signature by an individual signer with the knowledge of a single private key, the digital multisignatures are generated by multiple group members with the knowledge of multiple private keys. We list the following properties associated with the multisignature:

(i) digital multisignatures are generated by multiple group members with the knowledge of multiple private keys
(ii) digital multisignatures can be verified easily by using the group public key without knowing each signer's public key
(iii) it is computationally infeasible to generate the group signature without the co-operation of all group members.

Two ElGamal-type efficient multisignature schemes have been proposed [1, 2] which can combine all individual group signatures into a multisignature without any data expansion. In addition, in these schemes, the group public key is equivalent to the product of all group members' public keys. This feature enables all group members to establish security without the assistance of a mutually trusted party. However, since in these two schemes all group members sign the same messages, we call these schemes multisignature schemes with undistinguished signing authorities. In other words, all group members hold the same responsibility for signing the document.

Properties of multisignature with distinguished signing authorities: In fact, some applications need to use multisignatures with distinguished signing authorities. For example, a company releases a document that may involve the financial department, engineering department and program office. Each entity is responsible for preparing and signing a particular section of the document. The signing authority for the engineering department may have no interest in reading the contents prepared by the financial department. However, the combination of all sections represents the company's document. The company's document should be easily verified by any outsider using the company's public key. For the sake of confidentiality, some verifiers may be restricted to access and verify only some sections of the document. The multisignature schemes proposed in [1, 2] cannot provide these features. In this Letter, we modify these schemes to convert them to be a multisignature scheme with distinguished signing authorities. We list the following additional properties associated with the multisignature scheme with distinguished signing authorities:

(i) each group member has distinguished signing responsibility;
(ii) partial contents of the document can be verified without revealing the whole document.

We would like to point out that multisignatures with distinguished signing authorities can be found in many cryptographic applications. For example, a credit card company, telephone company, and medical insurance company can establish a joint venture to issue smart cards to customers. Use of the multisignature scheme proposed in this Letter can

(i) allow each company to register and sign its own customers
(ii) enhance the card security since multiple private keys are needed to forge a group signature
(iii) reduce memory storage on each card since only a multisignature is needed for each card
(iv) reduce the memory requirements for each verifier since only the group public key is needed
(v) speed up signature verification
(vi) provide confidentiality by just revealing partial customer information to some verifiers

Review of Harn digital multisignature: Here, we would like to review the design concept of the multisignature proposed in [1].

(i) *Determining the public keys*: A large prime p and a primitive element g of $GF(p)$ need to be made public. Each signer randomly selects an integer x_i from [1, p–1] and computes a corresponding public key as

$$Y_I = g^x I \bmod p$$

The public key for all signers is equivalent to the product of all individual public keys. We start with the multisignature generating phase.

(ii) *Generating the multisignature*:
(*a*) *Phase 1: Determining the commitment value of r*: We assume that there are two signers, U_1 and U_2, to sign the same message m. Each signer u_i randomly selects a number k_i from [1, p–1] and computes

$$r_I = g^k I \bmod p$$

(r_i) is broadcast to the other signer. Once r_1 and r_2 are avallable through the broadcast channel, each signer computes the commitment value r as $r = r_1 r_2 \bmod p$.

(*b*) *Phase 2*: Determining the multisignature value of s: Instead of signing the message m directly, all signers should sign the one-way hash result $m' = h(m)$, where h is the one-way hash function. Each signer uses his secret keys, x_i and k_i, to sign the message m'. U_i solves the equation

$$s_I = x_I m' - k_I r \bmod p - 1$$

for integer s_I where $0 < s_I < p$–1 and transmits (r_i, s_i) to the clerk.

Once the clerk receives the individual signature (r_i, s_i) from U_i he needs to verify the validity of this individual signature. The verification procedure checks that

$$Y_i^{m'} = r_i^r g^s i \bmod p$$

Once all individual signatures are received and verified by the clerk, the multisignature of message m can be generated as (r, s), where $s = s_1 + s_2 \bmod p$–1.

(iii) *Verifying the multisignature*: Since individual signatures, (r_1, s_1) and (r_2, s_2), satisfy

$$Y_1^{m'} = r_1^r g^s 1 \bmod p \quad \text{and} \quad Y_2^{m'} = r_2^r g^s 2 \bmod p$$

by multiplying these two equations, we obtain the multisignature verification equation as

$$Y^{m'} = r^r g^s \bmod p \quad \text{where} \quad y = y_1 y_2 \bmod p$$

Proposed multisignature scheme with distinguished signing authority: The group public key and the commitment value r can be determined in the same way as described previously. However, since the commitment value r does not depend on the message, this value can be pre-determined by all signers.

Instead of signing the same message m directly, each signer should prepare a section of message m_i that he is responsible for and broadcast $h(m_i)$ to all other signers, where h is the one-way hash function. Under our previous assumption that U_1 and U_2 are two signers in a group, each signer, U_i for i = 1, 2, uses his secret keys x_i and k_i to sign the message $m' = h(h(m_1), h(m_2))$, where $h(h(m_1), h(m_2))$ is the hash value of the concatenation of $h(m_1)$ and $h(m_2)$. The individual signature (r_i, s_i) from U_i and the multisignature of message $m = (m_1, m_2)$ are generated in the same way as described previously.

Discussion:
(*a*) Since each singer is responsible for preparing a section of message, each signer has distinguished signing authority.
(*b*) Instead of signing $m' = h(m_1, m_2)$, each signer needs to sign $m' = h(h(m_1), h(m_2))$. The computation of $h(h(m_1), h(m_2))$ is faster than that of $h(m_1, m_2)$ since each signer needs only to compute his own $h(m_i)$ and the other $h(m_i)$ has been computed by the other signer.

(*c*) To successfully forge a group signature, the attacker needs to know all the signing keys.
(*d*) In case some verifiers are only allowed to access partial contents of the message, the partial contents can still be verified using the group public key without revealing the whole message. This feature can be achieved by just providing the one-way hash values of the inaccessible contents to the verifier. For example, by revealing m_1 and $h(m_2)$ to the verifier, the verifier can still verify the authenticity of m_1.
(*e*) Signature schemes 1, 3, 7, 8, 13 and 14, as listed in the Table of [3], can provide similar multisignature schemes.

18 November 1998
Electronics Letters Online No: 19990166
DOI: 10.1049/el:19990166

L. Harn (*Department of Computer Networking, University of Missouri-Kansas City, MO 64110, USA*)

References

1 HARN, L.: 'Group-oriented (t, n) threshold signature and multisignature', *IEE Proc. Comput. Digital Techniques*, 1994, **141**, (5), pp. 307–313
2 HARN, L.: 'New digital signature scheme based on discrete logarithm', *Electron. Lett.*, 1994, **30**, (5), pp. 396–398
3 HARN, L., and XU, Y.: 'On the design of generalized ElGamal type digital signature schemes based on the discrete logarithm', *Electron. Lett.*, 1994, **30**, (24), pp. 2025–2026

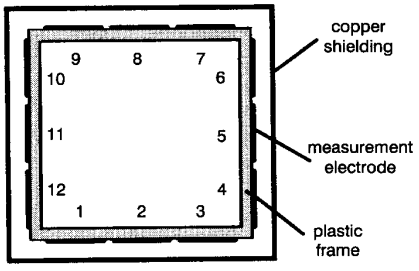
Electrical capacitance tomography with square sensor

W.Q. Yang and S. Liu

Electrical capacitance tomography (ECT) with circular sensors has previously been investigated. For some industrial applications such as circulating fluidised beds, square sensors are required. Research into this specific area has been carried out for the first time. To generate sensitivity maps, the Laplace equation is solved using a finite difference method. Both the linear back-projection algorithm and an iterative algorithm have been implemented for image reconstruction. Experimental results are promising.

Introduction: Electrical capacitance tomography (ECT) has an ability to present concentration distributions in two-phase dielectric processes and has been deployed in the visualisation of flow patterns, e.g. in circulating fluidised beds [1] and pneumatic conveyors [2]. In recent years, the image quality and measurement accuracy of ECT have been improved significantly. For example, in a recent experimental investigation of fluidisation processes, the difference between the results obtained from an ECT system and pressure measurements is < 3% under certain conditions [3].

In the past, all ECT systems have been designed for use with circular sensors, normally having 6, 8 or 12 electrodes. A large number of industrial applications, however, involve a square or rectangular geometry, such as most industrial boilers and circulating fluidised beds in thermal engineering. This Letter reports the feasibility of ECT with a square sensor.



135/1

Fig. 1 *Square sensor*

Sensor structure: The sensor is depicted in Fig. 1. It consists of 12 measurement electrodes, a plastic frame and copper shielding. The electrodes 10cm in length, are mounted onto the outer surface of the plastic frame with 2mm spacing between neighbouring electrodes. The cross-section of the copper shielding is 80 × 80mm². The inside dimensions of the plastic frame are 60 × 60mm². The thickness of the plastic frame is 2mm.

Generation of sensitivity maps: Sensitivity distributions of a sensor, which are called sensitivity maps, are essential for image reconstruction. In the linear back-projection (LBP) algoritlim, for example, an image is obtained by superimposing all sensitivity maps together using capacitance measurements as weighting factors. In most cases the sensitivity maps are generated from numerical solutions of the Laplace equation.

$$\frac{\partial^2 \phi}{\partial x^2} + \frac{\partial^2 \phi}{\partial y^2} = 0 \qquad (1)$$

where ϕ is the potential distribution.

Because of the difficulty in finding analytical solutions of the equation, finite element methods (FEMs) are often used to solve this problem. For square sensors, finite difference methods (FDM) are suitable for solving the equation [4]. For the sensor shown in Fig. 1, the sensing domain is divided into 160 by 160 square mesh grids and a central differencing scheme is used. The procedures are summarised as follows. One electrode is set of a voltage as a source electrode and the remaining electrodes are kept at the earth potential. An iterative approach is used to solve the potentials over the whole domain. For the 12 electrode sensor, 12 potential distributions are obtained. Fig. 2 shows two typical potential distributions when electrode 1 and electrode 2 are energised, respectively.

The sensitivity of electrode pair *i-j* at a spatial location (x, y) is calculated by dot-multiplying the two electric fields:

$$S_{ij}(x,y) = -\int_{p(x,y)} \frac{\vec{E}_i(x,y)}{V_i} \cdot \frac{\vec{E}_j(x,y)}{V_j} dxdy \qquad (2)$$

where $E_i(x, y)$ is the electric field distribution when electrode i is the source electrode with an excitation voltage V_i applied, while other electrodes remain at the earth potential, and $P(x, y)$ is the area of the pixel at (x, y). Fig. 3 illustrates some of the sensitivity maps, showing the higher sensitivity between neighbouring electrods (e.g. 1 and 2) and the symetric feature between two opposite electrodes (e.g. 2 and 8).

Fig. 2 *Typical potential distributions*
a Electrode 1 energised
b Electrode 2 energised

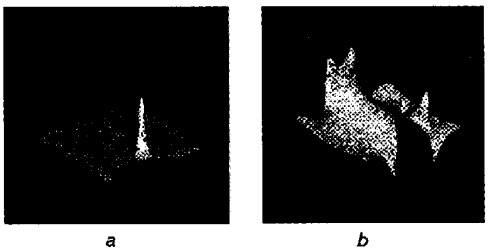


Fig. 3 *Sensitivity maps calculated using finite difference method*
a Between electrodes 1 and 2
b Between electrodes 2 and 8

Image reconstruction: LBP is a simple image reconstruction algorithm and has commonly been used in ECT with circular sensors.