clearly the same, H.263 and MPEG-4 will transmit at least two bits for every block in the object.

Run length coding of motion vector data: It is found that much video material amenable to effective low bit rate coding contains substantial areas of regular linear motion or static background. Examination of the coded results of these sequences show residual redundancy in the VLC output, with repetitive runs of bits indicating blocks with identical motion. We propose that the most economical method of coding the motion in these cases is to provide the run-length of identical successive vectors together with a single representation of the vector data.

Assuming that a VOP is fully contained by N macro-blocks (B_i) with block co-ordinates (x_i, y_i) , where $0 \leq i < N$, then the standard FSBM scan approach orders them such that:

$$B_i < B_{i+1} \Leftrightarrow (y_i < y_{i+1}) \vee ((y_i = y_{i+1}) \wedge (x_i < x_{i+1})) \quad (5)$$

To improve the efficiency of the run-length coding, a bi-directional scan provides better continuity at the VOP boundaries. This would require the object macro-blocks to be ordered such that:

$$B_i < B_{i+1} \Leftrightarrow \begin{cases} (y_i < y_{i+1}) \vee ((y_i = y_{i+1}) \wedge (x_i < x_{i+1})) & y_i = 0, 2, 4, \dots \\ (y_i < y_{i+1}) \vee ((y_i = y_{i+1}) \wedge (x_i > x_{i+1})) & y_i = 1, 3, 5, \dots \end{cases} \quad (6)$$

For such an ordered macro-block sequence (in the sense of either eqns. 5 and 6), there exist subsequences: $B_i, B_{i+1}, \dots, B_{i+l-1}$ which can be run-length compressed to lB_i as long as $\mathbf{b}_i = \mathbf{b}_j, \forall j: i \leq j \leq i+l-1$ (where $\mathbf{b}_i$ is the 'best' motion vector for macro-block B_i and is obtained from the ordering provided by eqns. 3 and 4). Statistics indicate that the run-length (l) can be variable length coded using the simple scheme shown in Table 1.

Table 1: Run-length variable length codes

Run-length	VLC	Bits
1	1	1
2, 3	01x	3
4, 5, 6, 7	001xx	5
8, ...	000xxxxxxx	10

The conventional FSBM 2D predictor can still be used to differentially code the vector with a minor modification for the bi-directional scan. Because the scan order is reversed for odd rows of blocks, the vector x and y components will have to be calculated as the median of the vectors immediately to the right, above and to the above left of the block being considered.

Performance evaluation: The technique was evaluated using arbitrary shaped video objects for two MPEG-4 test sequences 'container ship' and 'weather', each comprising 300 frames. The primary objects in these sequences, the ship and the presenter, were coded and the results are shown in Table 2.

Table 2: Run-length coding improvement summary

		Container		Weather	
		Bits	Improvement	Bits	Improvement
Standard search	FSBM	203	%	444	%
	RL raster	79	61.0	438	1.3
	RL bi-dir.	60	70.4	381	14.1
Optimal search	FSBM	193		431	
	RL raster	64	67.3	422	2.0
	RL bi-dir.	49	74.6	368	14.6

Run-length coding the 'container ship' motion information reduces the average number of bits per frame from 193 to 49. For the more complex 'weather' presenter, object run-length coding manages 368 bits compared to 431, representing a saving of 15%.

Conclusions: A method of run-length coding motion vector data for low bit rate object-based video coding is presented. Significant increases in coding efficiency can be gained when the image source material contains regular motion which is consistent from frame to frame. The process was evaluated using two object-based MPEG-4 test sequences, each comprising 300 frames. Run-length coding of the motion vector data resulted in a 75% increase in coding efficiency for the 'container ship' object. Dynamically switching between the two coding schemes on a frame by frame basis would assure maximum motion vector coding efficiency, regardless of the source material characteristics.

© IEE 1998

19 December 1997

Electronics Letters Online No: 19980383

M.K. Steliaros, G.R. Martin and R.A. Packwood (Department of Computer Science, University of Warwick, Coventry, CV4 7AL, United Kingdom)

Corresponding author: G.R. Martin

E-mail: grm@dcs.warwick.ac.uk

References

- 1 MPEG-4 Video Group, MPEG-4 video verification model version 9.0, ISO/IEC JTC/SC19/WG11 Document MPEG97/N1869, Fribourg, October 1997
- 2 JAIN, J.R., and JAIN, A.K.: 'Displacement measurement and its application in interframe image coding', *IEEE Trans. Commun.*, 1981, **COM-29**, pp. 1799-1808
- 3 RAO, K.R., and YIP, R.: 'Discrete cosine transform - algorithms, advantages and applications' (Academic Press, New York, 1990)
- 4 ITU-T Recommendation H.263 - Video coding for low bit rate communication, Geneva, March 1996

User efficient blind signatures

Chun-I Fan and Chin-Laung Lei

The authors present a fast blind signature scheme with fairly low computations for users. Only several modular additions and multiplications are required for a user to obtain and verify a signature in the proposed scheme. Comparing with the existing blind signature schemes proposed in the literatures, their method greatly reduces the amount of computations for users by almost 99%.

Introduction: Blind signatures are important techniques of modern cryptography since the techniques make it possible to prevent digital signatures from being forged and to protect the privacy of users. In a secure blind signature scheme, the signer cannot derive the link between a signature and the corresponding instance of signing protocol which produces that signature. This is usually referred to as the unlinkability (or blindness) property [1-5]. Because of the unlinkability property, blind signatures have been widely adopted to build the infrastructures of many advanced communication services proposed in the literatures to protect the users' privacy, such as anonymous electronic voting or cash systems [1-6].

In this Letter we propose a fast blind signature scheme with extremely low computations for users. No modular exponentiation and inverse computations are required for users, and, moreover, only several modular additions and multiplications are performed by a user to obtain and verify a signature in the proposed scheme. Comparing with the schemes of [1-5], the computations for users are greatly reduced by nearly 99% in our scheme. The proposed blind signature scheme is based on the theories of quadratic residues [7, 8]. Under a modulus n , x is a quadratic residue (QR) in Z_n^* if and only if there exists an integer y in Z_n^* such that $y^2 \equiv x \pmod{n}$ where Z_n^* is the set of all positive integers less than and relatively prime to n . Given x and n , it is infeasible to compute the square root y of x in Z_n^* if n contains large prime factors and the factorisation of n is unknown [7, 8].

Proposed scheme: There are two kinds of participant, a signer and a group of users, in the proposed blind signature scheme. A user requests signatures from the signer, and the signer computes and issues blind signatures to the users. Our blind signature scheme consists of four phases: (1) initialisation, (2) requesting, (3) signing, and (4) extraction. The signer publishes the necessary information in the initialisation phase. To obtain a signature of a message, a user submits an encrypted version of the message to the signer in the requesting phase. In the signing phase, the signer computes the blind signature of the message, and then sends the result back to the user. Finally, the user extracts the signature from the result he receives in the extraction phase. The details of our scheme are described as follows:

(1) **Initialisation:** The signer randomly selects two distinct large primes p_1 and p_2 where $p_1 \equiv p_2 \equiv 3 \pmod{4}$. The signer computes $n = p_1 p_2$ and publishes n . In addition, let H be a public one-way hash function.

(2) **Requesting:** To request a signature of a message m , a user randomly chooses two integers u and v such that $\alpha = (H(m)(u^2 + v_2) \pmod{n})$ is in Z_n^* , and then submits the integer α to the signer. After receiving α , the signer randomly selects x such that $(\alpha(x^2 + 1) \pmod{n})$ is a QR in Z_n^* , and then sends the integer x to the user. After receiving x , the user randomly selects an integer b in Z_n^* , and then computes $\delta = (b^2 \pmod{n})$ and $\beta = (\delta(ux + v) \pmod{n})$. The user submits β to the signer.

(3) **Signing:** After receiving β , the signer computes $\lambda = (\beta^{-1} \pmod{n})$ and derives an integer t in Z_n^* such that

$$t^4 \equiv \alpha(x^2 + 1)\lambda^2 \pmod{n}$$

since the signer knows the factors p_1 and p_2 of n [7, 8]. Hence t is one of the fourth roots of $(\alpha(x^2 + 1)\lambda^2 \pmod{n})$ in Z_n^* . The signer sends the tuple (t, λ) to the user.

(4) **Extraction:** After receiving (t, λ) , the user computes

$$\begin{cases} c = \delta\lambda(u - vx) \pmod{n} \\ s = bt \pmod{n} \end{cases}$$

The tuple (c, s) is a signature of m . To verify (c, s) of m , one can examine if

$$s^4 \equiv H(m)(c^2 + 1) \pmod{n}$$

Discussions: In the proposed scheme, the signer perturbs the message received from a user before he signs it by using a random integer x . This is usually referred to as the randomisation property [3]. A randomised blind signature scheme can withstand the chosen-text attacks [9]. Our scheme and the blind signature schemes of [1, 3 – 5] possess the randomisation property, while the blind signature scheme of [2] does not possess this property.

By the theories of quadratic residues, given a quadratic-residue integer in Z_n^* , it is infeasible to compute a square root of the integer in Z_n^* without the factorisation of n [7, 8]. In the proposed scheme, given integers c and m , it is intractable to compute s to forge the signature (c, s) of m such that $s^4 \equiv H(m)(c^2 + 1) \pmod{n}$ without the factorisation of n since s is a fourth root of the integer $(H(m)(c^2 + 1) \pmod{n})$ in Z_n^* .

In the requesting stage of the proposed scheme, the signer receives the integers α and β submitted by a user for requesting a signature of a message m . Then in the extraction stage, the user obtains the tuple (c, s) . The signer cannot link the tuple (α, β) (or the instance of the signing protocol) to the tuple (c, m, s) because the integers b, u, v are randomly selected and kept secret by the user in the proposed scheme. This is the unlinkability (or blindness) property.

In the proposed scheme, instead of applying a one-way hash function, we can let the message m contain proper redundancy, so that the message m can be recovered from its corresponding signature (c, s) by computing $(s^4(c^2 + 1)^{-1} \pmod{n})$ since $s^4 \equiv m(c^2 + 1) \pmod{n}$. Hence, it is not necessary to transmit the plaintext message m along with the corresponding signature (c, s) for verification. This is usually referred to as the message recovery property.

Finally, the comparisons of the properties between our scheme and the schemes of [1 – 5] are summarised in Table 1. The mathematical foundations of our scheme and the schemes of [5] are

QRs. The security of the schemes of [2, 3] depends on the RSA assumption, while the schemes of [1, 4] are based on discrete logarithms (DLs).

Table 1: Property comparisons

	Our scheme	[1] ¹	[2]	[3]	[4] ¹	[5] ¹
Mathematical foundation	QR	DL/DL	RSA	RSA	DL/RSA	QR/QR
Unlinkability	yes	yes/yes	yes	yes	yes/yes	yes/yes
Randomisation	yes	yes/yes	no	yes	yes/yes	yes/yes
Message recovery	yes	no/yes	yes	no	no/no	no/no

¹ Two blind signature schemes are proposed in [1, 4, 5]

Performance: A fast modular exponentiation algorithm is proposed in [10] which requires $0.3381|n|$ modular multiplications to perform a modular exponentiation computation where $|n|$ denotes the bit length of the modulus n . In general, an inverse computation in Z_n^* takes about the same time as that of a modular exponentiation computation in Z_n^* , and a hashing computation does not take longer time than that of a modular multiplication [8].

Table 2: Numbers of computations required for a user to obtain and verify a signature

	Our scheme	[1]*	[2]	[3]	[4]*	[5]*
No. of modular exponentiations	0	4	2	4	6	3
No. of inversive computations	0	2	1	1	0	0
No. of hashing computations	2	0	2	2	2	2
No. of modular computations	14	6	2	3	5	$2k^{**}$
Computations reduced by:	0%	99%	99%	99%	99%	99%

* The fastest scheme mentioned in the paper is selected for comparison in this Table

** k is a large enough integer

In the proposed scheme, only several modular additions and multiplications are required for a user to obtain and verify a signature. Comparing with the schemes of [1 – 5], our scheme reduces the amount of computations for users by almost 99% under a 1024-bit modulus n . The comparisons of the numbers of computations performed by a user between our scheme and the schemes of [1 – 5] are summarised in Table 2. In addition, compared to the blind signature scheme of [2] with a short public key $e = 3$, our method still largely reduces the amount of computations for users by 95% under a 1024 bit modulus since an inverse computation is needed for a user in that scheme.

In the proposed scheme, the signer performs a fourth root computation and an inverse computation in Z_n^* . Comparing with the scheme of [2], our protocol does not decrease the computation load for the signer. However, in most of the applications based on blind signatures, the signer usually possesses much more computation capacities than a user such as the bank of an electronic cash system or the tally centre of an electronic voting system, while the computation capacities of the users are limited in some situations such as mobile clients and smart-card users. Hence, to guarantee the quality of these ever-growing popular communication services, it is more urgent to reduce the computation load for the users than that for the signer.

Conclusions: We have proposed an efficient blind signature scheme with fairly low computations for users. Since no modular exponentiation and inverse computations are performed by users, our scheme is suitable for the situations where the computation capacities of users are limited. Comparing with the existing blind signature schemes, the computation loads are greatly reduced for the users to obtain and verify signatures in the proposed blind signature scheme.

© IEE 1998

Electronics Letters Online No: 19980378

24 December 1997

Chun-I Fan and Chin-Laung Lei (Department of Electrical Engineering, Rm. 303, New E.E. Buildings, National Taiwan University, Taipei, Taiwan 10764, Republic of China)

E-mail: lei@cc.ee.ntu.edu.tw

References

- 1 CAMENISCH, J.L., PIVETEAU, J.M., and STADLER, M.A.: 'Blind signatures based on the discrete logarithm problem'. Advances in Cryptology-EUROCRYPT'94, LNCS 950, (Springer-Verlag, 1995), pp. 428-432
- 2 CHAUM, D.: 'Blind signatures systems'. Advances in Cryptology-CRYPTO'83, (Plenum, 1983), p. 153
- 3 FERGUSON, N.: 'Single term off-line coins'. Advances in Cryptology-EUROCRYPT'93, LNCS 765, (Springer-Verlag, 1994), pp. 318-328
- 4 POINTCHEVAL, D., and STERN, J.: 'Provably secure blind signature schemes'. Advances in Cryptology-ASIACRYPT'96, LNCS 1163, (Springer-Verlag, 1996), pp. 252-265
- 5 POINTCHEVAL, D., and STERN, J.: 'New blind signatures equivalent to factorization'. Proc. 4th ACM Conf. on Computer and Communication Security, 1997, pp. 92-99
- 6 CHAUM, D., FIAT, A., and NAOR, M.: 'Untraceable electronic cash'. Advances in Cryptology-CRYPTO '88, LNCS 403, (Springer-Verlag, 1990), pp. 319-327
- 7 RABIN, M.O.: 'Digitalized signatures and public-key functions as intractable as factorization'. Technical Report, MIT/LCS/TR212, MIT Lab., Computer Science, Cambridge, MA, USA, January 1979
- 8 SIMMONS, G.J.: 'Contemporary Cryptology: The Science of Information Integrity' (IEEE Press, N.Y., 1992)
- 9 SHAMIR, A., and SCHNORR, C.P.: 'Cryptanalysis of certain variants of Rabin's signature scheme', *Inf. Process. Lett.*, 1984, **19**, pp. 113-115
- 10 DIMITROV, V., and COOKLEV, T.: 'Two algorithms for modular exponentiation using nonstandard arithmetics', *IEICE Trans. Fundam. Electron. Commun. Comput. Sci.*, 1995, **E78-A**, (1), pp. 82-87

Initial results for a quadrupole mass spectrometer with a silicon micromachined mass filter

S. Taylor, J.J. Tunstall, R.R.A. Syms, T. Tate and M.M. Ahmad

Initial results are presented from tests of a low voltage, low power, miniature quadrupole mass spectrometer with a novel silicon micromachined mass filter. The construction of the device is discussed, along with its mounting on a conventional ion source and testing in a vacuum system. Results are presented for the operation of the lens including a mass spectrum for an argon/air mixture and the effect of cage voltage, emission current and pressure on the performance.

Quadrupole mass spectrometers (QMS) have been widely researched and developed as sensors and diagnostic tools for over 40 years [1]. They have found a wide range of applications in the medical field, chemical process industries and more recently in process monitoring in semiconductor fabrication plants where ultra clean processes for ULSI are a priority. QMS based on cylindrical rods for the mass filter are now highly developed and successful [2]. Only in recent years have economic methods of precision lens assembly been devised [3], however the mass filters are still bulky and require large drive voltages at RF frequencies. If the cost, the size and voltages can be reduced then the range of applications for these types of QMS would increase: this is the motivation for our work. The conventional arrangement uses circular cross-section metallic rods as the mass filter (typical dimensions: rod-length: 50-225mm; diameter: 5-15mm) excited electrically at voltages up to 1kV depending on the application. We have produced a micromachined quadrupole lens made from silicon with metallised borosilicate glass drawn to diameter as the electrodes [4]. The correct electrode spacing and alignment are achieved through the use of V-shaped grooves etched into the silicon. A description of the fabrication of such a device using 0.5mm diameter electrode rods is given in [5].

A quadrupole mass filter thus realised was mounted onto a conventional VG ANAVAC ion source which was in turn attached to a vacuum flange. External connections from the mass lens and the ion source were made to pins on the outside of the flange. The ion

source was connected to an emission regulator. The filament which produces the electrons for ionisation of the gas was held at -78.5V, (filament return was set at -76.0V), the focusing element was set at -7.7V and the source cage held at 11.0V. With argon gas in the vacuum, system ions were produced in the source, which in turn passed through the mass filter. A split phase RF alternating voltage (amplitude $V = 20V$), and a direct voltage ramp ($U(t): 0 < U < 10V$), was applied to the quadrupole rods. The U/V voltage ratio was kept fixed and the voltages scanned from high to low values with the ratio adjusted so that the effective scan-line would pass close to the tip of the Mathieu stability diagram for singly charged argon ions [1].

Fig. 1 End-on optical microscope view of micromachined quadrupole mass filter

Fig. 2 Typical spectrum obtained from output of electrometer for an argon/air gas mixture

Gas pressure was 5.0×10^{-5} Torr and frequency of RF voltage was 6MHz. Argon peak at mass 40 is clearly seen, along with a broad peak for air. Also apparent is the doubly charged argon peak at mass 20

Fig. 1 shows an end-on optical microscope view of the micromachined quadrupole mass filter. A typical mass spectrum is plotted in Fig. 2 showing the output from the electrometer (ion current) for an argon/air gas mixture. From peaks at mass 40 ($M = 40$) and mass 20 the mass scale can be calibrated and the resolution of the QMS ($M/\Delta M$) at half height can be calculated.

There are several parameters that can be varied which affect the performance of a mass spectrometer. Our first investigation was to see how resolution varied with cage voltage. The spectrum was scanned for a range of cage voltages ensuring that both the singly-charged argon peak and the doubly-charged argon peak were recorded. Along with the positions of the peaks the ion current was measured so that the sensitivity for the peaks at $M = 40$ and $M = 20$ could be determined. A general trend of decreasing resolution for increased cage voltage (ion energy) was seen. It can be shown the mass peak width ΔM (in a.m.u.) of an ideal quadrupole lens is given by [1]:

$$\Delta M \approx 4 \times 10^9 V_z / f^2 L^2 \quad (1)$$

where V_z is the ion axial energy in eV and L the electrode length (metres). For the QMS tested here at $V_z = 6eV$ (corresponding to a cage voltage of 6V), $f = 6MHz$ and $L = 20mm$, eqn. 1 predicts a maximum resolution of 24 which is close to the value obtained in practice (Fig. 3). The fall off in resolution for low cage voltages is