7 SUN, H.M., and SHIEH, S.P.: 'On dynamic threshold schemes', to appear in *Inf. Process. Lett.*, 1994

8 ELGAMAL, T.: 'A public key cryptosystem and a signature scheme based on discrete logarithms', *IEEE Trans.*, 1985, **IT-31**, pp. 469–472

Design of generalised ElGamal type digital signature schemes based on discrete logarithm

L. Harn and Y. Xu

Indexing term: Cryptography

The ElGamal type digital signature schemes have received wide attention recently. ElGamal type signature schemes can provide 'subliminal' channel, message recovery, multisignature, etc. The authors investigate the design criteria of ElGamal type signature scheme and develop a complete list of all variations.

Introduction: A digital signature is analogous to an ordinary written signature used for signing messages. It must be unique and private to the user. At this time, there are two most popular public-key algorithms which can provide a digital signature: the RSA scheme [1]; and the ElGamal scheme [2].

A modification of the ElGamal signature was proposed by Agnew, Mullin and Vanstone (AMV) [3] in 1990. Instead of solving $m = xr + ks \bmod p{-}1$, the signer solves the congruence $m = xs + kr \bmod p{-}1$. The advantage of this modified scheme over the ElGamal scheme is that, in order to compute the signature by solving the congruence for s, the signer only needs to compute x^{-1} in Z_{p-1}^* once, instead of computing k^{-1} in Z_{p-1}^* for every signature, where x is the secret key for the signer and k is an integer randomly selected by the signer for signing every message. Yen and Laih [4] also proposed a variation of the ElGamal type signature scheme. In 1994, Harn [5, 6] proposed two other variations of ElGamal type schemes.

In 1989, Schnorr [7] proposed an ElGamal type signature scheme to shorten the signature. Later, the digital signature algorithm (DSA) was proposed [8] by NIST, also based on a very similar approach. These two schemes have also been developed based on the original ElGamal signature scheme.

A recent paper, Nyberg and Rueppel [9], pointed out that all ElGamal type signature schemes have variants giving message recovery and also analysed six of the simplest ElGamal type variations in $GF(p)$. Being motivated by their paper, we have developed a complete list of 18 ElGamal type signature schemes in this Letter.

Generalised ElGamal type signature schemes: Let p be a large prime and α be a primitive number in $GF(p)$. Each user selects a secret key $x \in [1, p{-}1]$ and computes a public key $y = \alpha^x \bmod p$. For each message $m \in [1, p{-}1]$ to be signed a new random integer $k \in [1, p{-}1]$ is privately selected. Instead of signing the message m directly, all ElGamal type signature schemes should sign the one-way hash result of m. For simplicity, we will ignore the one-way hash function in the following discussion.

In all ElGamal type signature schemes [3–9] the commitment part r of the signature is computed as

$$r = \alpha^k \bmod p$$

The other part s of the signature is computed differently. In the original ElGamal scheme, s is solved with the knowledge of the signer's secrets, x and k, as

$$m = ks + rx \bmod \phi(p)$$

where k should be selected such that $\mathrm{GCD}(k, \varnothing(p)) = 1$. The triplet $(m; (r,s))$ constitutes the signed message and is sent to the verifier.

The signature (r, s) is accepted by evaluating whether the equality

$$\alpha^m = r^s y^r \bmod p$$

holds true.

Without loss of generality, we can represent the generalised equation for all ElGamal type signature schemes as

$$ax = bk + c \bmod \phi(p)$$

where (a, b, c) are three parameters from the set of values (m, r, s). More specifically, each parameter can be a mathematical combination of (m, r, s). For example, the parameter a can be rm, or r, etc. The verification equation is determined accordingly as

$$y^a = r^b \alpha^c \bmod p$$

In the following we will discuss the form of the above generalised signature equation and some restrictions applied on parameters (a, b, c) based on the security considerations.

(a) Because x and k are two secret numbers and the verifier does not know these two values, x and k should be treated as two different terms in the above equation. Otherwise, if we combine these two secret parameters together (i.e. for example, if $xk = rm + s \bmod \varnothing(p)$, then $y^k = \alpha^{rm+s} \bmod p$ or $r^x = \alpha^{rm+s} \bmod p$), the verifier cannot verify the signature.

(b) To claim that (r, s) is a signature for the message, the message m itself should be included in the signature equation and can be in any of parameters (a, b, c).

(c) To provide proper security of algorithms, r and s should also be included in parameters (a, b, c). Thus, there are five parameters in the equation. If r is contained in parameter b, the verification equation is very similar to the scheme proposed by Agnew, Mullin and Vanstone [3], in which r will appear in both the base and the exponent of the same base (i.e. $\alpha^m = y^s r^r \bmod p$). Otherwise, r will appear in both the base and the exponent of a different base (i.e. $\alpha^m = r^s y^r \bmod p$) as in the original ElGamal scheme [2].

(d) For security reasons, s and m cannot be combined together in any of parameter (a, b, c). For example, if $x = rk + sm \bmod \varnothing(p)$. Then only by modifying the partial signature s of a legitimate signature (r, s) corresponding to the message m, can it forge a signature (r, s') of another message m', where $m' = \beta m \bmod \varnothing(p)$ and $s' = \beta^{-1}s \bmod \varnothing(p)$.

(e) For security reasons, s and r cannot be combined together. For example, if $mx = k + rs \bmod \varnothing(p)$ and the corresponding verification equation is $y^m = r\alpha^{rs} \bmod p$. The attacker can first randomly select an integer R and computes r' to satisfy $y^m = r'\alpha^R \bmod p$. The forged signature is (r', s'), where $r's' = R \bmod \varnothing(p)$.

(f) r can be combined with m. For example, if $x = rmk + s \bmod \varnothing(p)$. This is due to the fact that the partial signature r is locked by the secret number k and it is impossible to forge a signature by changing r only.

(g) There must be three separate terms as specified in the equation. For example, if $(m{+}r)x = sk \bmod \varnothing(p)$, then it can forge signature (r, s') for another message m', where $m{-}m' = \beta \bmod \varnothing(p)$ and $s' = (1 - \beta(m{+}r)^{-1})s \bmod \varnothing(p)$.

(h) The generalised signature equation contains five parameters: three parameters, (m, r, s), are public information, x is the fixed secret key of the signer and k is a random secret value for each message. Because the number of secret parameters is always one larger than the number of linear equations available to the attacker, the signature scheme is secure based on the discussion in the original ElGamal paper [2].

If we neglect the difference between $+d$ and $-d$, and the difference between d and d^{-1}, where $d \in (x, k, m, r, s)$, we can list all possible ElGamal type signature variations in Table 1.

Table 1: Generalised ElGamal type signature schemes

	Signature equation	Signature verification	Comment
(1)	$mx = rk + s \bmod \varnothing(p)$	$y^{m} = r^{r}\alpha^{s} \bmod p$	Harn scheme [5]
(2)	$mx = sk + r \bmod \varnothing(p)$	$y^{m} = r^{s}\alpha^{r} \bmod p$	
(3)	$rx = mk + s \bmod \varnothing(p)$	$y^{r} = r^{m}\alpha^{s} \bmod p$	
(4)	$rx = sk + m \bmod \varnothing(p)$	$y^{r} = r^{s}\alpha^{m} \bmod p$	ElGamal scheme [2]
(5)	$sx = rk + m \bmod \varnothing(p)$	$y^{s} = r^{r}\alpha^{m} \bmod p$	AMV scheme [3]
(6)	$sx = mk + r \bmod \varnothing(p)$	$y^{s} = r^{m}\alpha^{r} \bmod p$	
(7)	$rmx = k + s \bmod \varnothing(p)$	$y^{rm} = r\alpha^{s} \bmod p$	Optimal scheme [9]
(8)	$x = mrk + s \bmod \varnothing(p)$	$y = r^{mr}\alpha^{s} \bmod p$	Yen and Laih scheme [4]
(9)	$sx = k + mr \bmod \varnothing(p)$	$y^{s} = r\alpha^{mr} \bmod p$	
(10)	$x = sk + rm \bmod \varnothing(p)$	$y = r^{s}\alpha^{rm} \bmod p$	
(11)	$rmx = sk + 1 \bmod \varnothing(p)$	$y^{rm} = r^{s}\alpha \bmod p$	
(12)	$sx = rmk + 1 \bmod \varnothing(p)$	$y^{s} = r^{rm}\alpha \bmod p$	
(13)	$(r + m)x = k + s \bmod \varnothing(p)$	$y^{r+m} = r\alpha^{s} \bmod p$	Harn scheme [6]
(14)	$x = (m + r)k + s \bmod \varnothing(p)$	$y = r^{m+r}\alpha^{s} \bmod p$	
(15)	$sx = k + (m + r) \bmod \varnothing(p)$	$y^{s} = r\alpha^{m+r} \bmod p$	
(16)	$x = sk + (r + m) \bmod \varnothing(p)$	$y = r^{s}\alpha^{r+m} \bmod p$	
(17)	$(r + m)x = sk + 1 \bmod \varnothing(p)$	$y^{r+m} = r^{s}\alpha \bmod p$	
(18)	$sx = (r + m)k + 1 \bmod \varnothing(p)$	$y^{s} = r^{r+m}\alpha \bmod p$	

Eqns. 13–18 can be drived from eqns. 7–12 by replacing the multiplication with the addition between two parameters of values (m, r)

Discussion:

(*a*) The most time-consuming computation in signature generating is $r = \alpha^{k} \bmod p$, which can be precomputed. The signature verification requires two modular exponentiations. There are some schemes, such as 7, 8, 13 and 14, in which the partial signature s can be solved and the signature can be verified without computation of the inverse. In [9], scheme 7 in the Table is selected as the optimal scheme for use in the design.

(*b*) The subliminal channel can be used to conceal secret information and the secret information can only be recovered by the insider with the secret key shared with the signer. The ElGamal type signature scheme is a good candidate for establishing such a subliminal channel. The interested reader on this subject and on possible applications of subliminal channels should refer to [10]. In 1993, Simmons [10] showed that the 'broadband' subliminal channel exists in the digital signature algorithm (DSA) [8] proposed by the NIST. However, the DSA uses modulus p for which p–1 has one large prime factor q. In [6], Harn proposed the signature scheme 13 in Table 1 as a broadband subliminal signature scheme, in which the modulus can be any prime number. Because the key factor of a broadband subliminal signature scheme is that s and k can be solved without computation of the inverse, schemes 7 and 13 in Table 1 are broadband subliminal signature schemes.

(*c*) The technique used in the DSA can also be applied to all schemes in the Table to shorten the signature and to speed up the computation. All schemes can also be modified to have the message recovery ability as discussed by Nyberg and Rueppel [9].

© IEE 1994 30 September 1994
Electronics Letters Online No: 19941398

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

References

1 RIVEST, R.L., SHAMIR, A., and ADELMAN, L.: 'A method for obtaining digital signatures and public-key cryptosystem', *Commun. SCM*, 1978, **21**, (2), pp. 120–126

2 ELGAMAL, T.: 'A public key cryptosystem and signature scheme based on discrete logarithms', *IEEE Trans.*, 1985, **IT-31**, (4), pp. 469–472

3 AGNEW, G.B., MULLIN, R.C., and VANSTONE, S.A.: 'Improved digital signature scheme based on discrete exponentiation', *Electron. Lett.*, 1990, **26**, (14), pp. 1024–1025

4 YEN, S.M., and LAIH, C.S.: 'New digital signature scheme based on discrete logarithm', *Electron. Lett.*, 1993, **29**, (12), pp. 1120–1121

5 HARN, L.: 'Group-oriented (t, n) threshold signature and multisignature', *IEE Proc. E*, 1994

6 HARN, L.: 'New digital signature scheme based on discrete logarithm', *Electron. Lett.*, 1994, **30**, (5), pp. 396–398

7 SCHNORR, C.P.: 'Efficient identification and signatures for smart cards'. Advances in Cryptology – Crypto '89, August 1989, (Springer-Verlag, Santa Barbara), pp. 239–252

8 : 'The digital signature standard', *Commun. ACM*, 1992, **35**, (7), pp. 36–40

9 NYBERG, K., and RUEPPEL, R.A.: 'Message recovery for signature schemes based on the discrete logarithm problem'. Pre-proc. of Eurocrypt '94, May 1994, pp. 175–190

10 SIMMONS, G.J.: 'Subliminal communication is easy using the DSA'. Pre-proc. of Eurocrypt '94, May 1993, (Lofthus, Norway)

Laser optical lever for sensitive detection of trace gases

N.H. Tran, D. Jacob, A. Le Floch and F. Bretenaker

Indexing terms: Laser sensors, Methane detectors

Nonintrusive, species-selective and linear detection of trace gases is implemented with a novel intracavity laser absorption method. A first experimental realisation demonstrates a sensitivity of 3 × 10^{9} molecules of methane, which exceeds that of gas chromatography by two orders of magnitude.

Methane is a major greenhouse gas whose potential effects on climate are a subject of intense study. Although lasers have been used to detect methane with rather good sensitivities [1], both ambient [2] and fossil [3] methanes at present are still first retrieved and then analysed in gas chromatographs equipped with flame-ionisation detectors. The technique is destructive and may require time-consuming procedures. We report a novel approach to detecting trace gases that offers the nonintrusiveness and species selectivity of laser spectroscopy at a sensitivity level exceeding that of gas chromatography. The method can be used in real-time, does not require a large amount of equipment and involve complicated procedures, and, unlike classical intracavity absorption, is linear in absorber concentration; implemented here with a mid-infrared laser for the detection of methane, it can be transposed to other trace gases such as carbon dioxide.

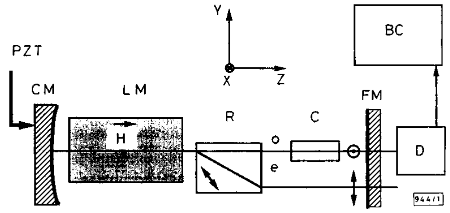

Fig. 1 *Experimental apparatus*

R: rutile crystal, LM: lasing medium, o: ordinary, e: extraordinary, C: absorption cell, CM: curved mirror, FM: flat mirror, PZT: piezoceramic transducer, D: photodetector, $\vec{H}$: DC longitudinal magnetic field, BC: boxcar averager

A custom-built helium-neon laser is employed to sense methane using the well-known coincidence between Ne emission and CH_4 absorption at 3.39μm. As shown in Fig. 1, the laser cavity contains a birefringent rutile crystal. Cut at 45° to its optical axis [4], the crystal allows the existence of two nondegenerate eigenstates, an ordinary x-polarised state and an extraordinary y-polarised state, which are spatially separated in part of the cavity. This piecewise spatial resolution permits the insertion of the methane sample onto the path of only one eigenstate, while both eigenstates remain superimposed in the gain medium. The conjunction of selective absorption and common gain thus obtained makes possible the realisation of a highly efficient optical lever, as now explained.

Although kinematically possible, the two eigenstates may not oscillate simultaneously at all times. The situation is described in