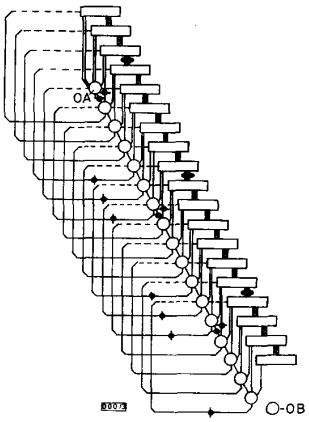

Fig. 3 *New MAC processor, latency 1, pipelined every six rows*

Performance of new circuit: The original circuit has a clock rate of 30MHz and a sampling rate of 15MHz. While the clock rate of the new circuit would be only 20MHz, the sampling rate is now also 20MHz which is 33% faster than the old circuit. Moreover, the power consumption has reduced as the circuit only operates at two-thirds the previous clock rate and has considerably lower number of gates switching every cycle. The reduction in latches also acts to reduce the overall area. Most significantly, the fundamental bottleneck of having to clock the circuit at twice the sampling rate has been removed which will allow filters to be designed with sampling rates up to 100MHz.

25 July 1994
Electronics Letters Online No: 19950823

B.P. McGovern, R.F. Woods and C. McAllister (*Institute of Advanced Microelectronics, Department of Electrical and Electronic Engineering, The Queen's University of Belfast, Belfast, BT9 5AH, Northern Ireland, United Kingdom*)

References

1 RENFORS, M., and NEUVO, Y.: 'The maximum sampling rate of digital filters under hardware constraints', *IEEE Trans.*, 1981, **CAS-28**, (3), pp. 196–202
2 KNOWLES, S.C., WOODS, R.F., MCWHIRTER, J.G., and MCCANNY, J.V.: 'Bit-level systolic architectures for high performance IIR filtering', *J. VLSI Signal Process.*, 1989, **1**, (1), pp. 9–24
3 AVIZIENIS, A.A.: 'Signed-digit number representations for fast parallel arithmetic', *IRE Trans.*, 1960, **EC-10**, pp. 389–400
4 WOODS, R.F., FLOYD, G., WOOD, K., MCCANNY, J.V., and EVANS, R.: 'A programmable high performance IIR filter chip'. IEE Colloq. DSP in Communication Systems, London, England, 22 March 1993

Cryptanalysis of the blind signatures based on the discrete logarithm problem

L. Harn

Indexing terms: Cryptography, Public key cryptography

Carmenisch *et al.* proposed a blind signature scheme based on the discrete logarithm during at the rump session of Eurocrypt'94. Horster *et al.* generalised this approach to design the Meta blind signature schemes. The author of this Letters points out that these schemes cannot provide true blind signatures.

Introduction: Chaum proposed the first blind signature scheme [1] in 1982 and the security of this scheme is based on the difficulty of factoring a large composite integer. The blind signature is a regular digital signature; but it needs to satisfy two additional requirements:

(*a*) the content of the message should be blind to the signer.

(*b*) the signed signature should not be able to be traced by the signer after the signature has been revealed to the public by the owner.

There are cryptographic applications, such as electronic voting and electronic cash systems, developed recently that require the use of blind signatures. Carmenisch *et al.* proposed the first blind signature scheme [2] based on the discrete logarithm during the rump session of Eurocrypt'94. Later, Horster *et al.* [3] generalised this approach to design the Meta blind signature schemes. In this Letter we would like to point out that these schemes cannot provide true blind signatures. More specifically, we want to show that the signatures are traceable by the signer.

Review of scheme proposed by Carmenisch et al.: There are two public-known large primes, p and q, where $q|p-1$, and an integer $\alpha \in Z_p^*$ of order q. The signer selects a secret key x and publishes his public key $y = \alpha^x \bmod p$. The signer of the blind signature randomly chooses an integer k and computes $\tilde{r} = \alpha^k \bmod p$. $\tilde{r}$ is sent to the owner of the signature. The owner randomly chooses two integers $a, b \in Z_q^*$ and computes $r = \tilde{r}^a \alpha^b \bmod p$. The owner of the blind signature blinds the message m by computing $\tilde{m} = am\tilde{r}r^{-1} \bmod q$. The owner sends $\tilde{m}$ to the signer. With the knowledge of the secret key x, the signer computes $\tilde{s} = x\tilde{r} + k\tilde{m} \bmod q$. $\tilde{s}$ is sent to the owner. The owner computes the signature as $s = s\tilde{r}r^{-1} + bm \bmod q$. $\{r, s\}$ becomes the signature of the message m by checking $\alpha^s = y^r r^m \bmod p$.

Cryptanalysis: The signer will keep a set of record $\{\tilde{m}, \tilde{r}, \tilde{k}, \tilde{s}\}$ for all blinding signed messages. After revealing the signature $\{r, s\}$ of message m to the public by the owner, the signer will try to compute a pair of integers $\{a', b'\}$, where $a' = \tilde{m}mr^{-1}\tilde{r}^{-1}r \bmod q$ and $b' = m^{-1}(s - \tilde{s}r\tilde{r}^{-1}) \bmod q$, corresponding to each stored value $\{\tilde{m}, \tilde{r}, \tilde{k}, \tilde{s}\}$. The true blind signature can be traced by the signer by checking $r = \tilde{r}^{a'}\alpha^{b'} \bmod p$. This result violates requirement (*b*) of the blind signature.

Conclusion: In this Letter we show a cryptanalysis of the blind signature schemes proposed recently. How to design a secure blind signature based on the discrete logarithm is still an open problem.

10 March 1995
Electronics Letters Online No: 19950815

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

References

1 CHAUM, D.: 'Blind signature for untraceable payments' *in*: 'Advances in cryptology: Proc. Crypto '82' (Plenum Press, New York, 1983), pp. 199–203
2 CARMENISCH, J.L., PIVETEAU, J.-M., and STADLER, M.A.: 'Blind signatures based on the discrete logarithm problem'. Rump Session of Eurocrypt'94, Perugia, Italy, 1994
3 HORSTER, P., MICHELS, M., and PETERSEN, H.: 'Meta message recovery and Meta blind signature based on the discrete logarithm problem and their applications'. Pre-Proceedings Asiacrypt'94, pp. 185–196

Comment

Digital signature with (*t*, *n*) shared verification based on discrete logarithms

P. Horster, M. Michels and H. Petersen

Indexing term: Cryptography

The digital signature scheme with (t, n) shared verification proposed by Harn [1] can be easily forged universally [2]. In the reply of Harn, two different solutions to overcome this attack were presented [3]. We discuss the first solution and show that the second solution (and related ones) are flawed, because with a simple attack we can forge this scheme and related ones universally. Finally we propose a simple solution to countermeasure all attacks. We assume that the reader is familar with the scheme in the notation of [1, 3].

The first solution suggested by Harn to overcome the attack is to choose the parameters g and β in the initialisation and publish them as public keys, certified by the trusted authority. The attack mentioned above is then avoided, but for each signature, new parameters g and β are necessary. Thus the disadvantage of this approach is that the size of the public file depends on the number of signatures the signer might sign in future. As a result, this countermeasure is not practical.

The second solution suggested by Harn to overcome the attack is to use the AMV scheme [5] instead of the ElGamal scheme [4] as the underlying conventional signature scheme. The signature for the message m is then given by (z, r, g, β) and the verification is done by checking the congruence

$$\beta^{H(m)} \equiv y^z r^r \pmod{p}$$

The public key y can be computed by at least t out of n verifiers and the relationship

$$y \equiv g^{\alpha^s} \pmod{p}$$

holds, where α is a fixed secret parameter and s is the secret key of the signer. We assume that the signature (z, r, g, β) for the message m is known. To obtain a (forged) signature for the message $\tilde{m}$, the attacker computes $u := H(\tilde{m})^{-1}H(m) \pmod{w}$ and $\beta := \beta^u \pmod{p}$. Now the signature for the message $\tilde{m}$ is then given by (z, r, g, β), because

$$\tilde{\beta}^{H(\tilde{m})} \equiv \beta^{uH(\tilde{m})} \equiv \beta^{H(m)} \equiv y^z r^r \pmod{p}$$

This attack (and also the attack of [2]) might be noticed by those verifiers who know all previous signatures of the signer. As the parameter r is not modified in the forged signature, the verifierers can reject those signatures where the parameter r was used before. However, this assumption is not realistic and therefore the scheme is insecure. Obviously, the described attack can also be used to forge a signature in the original scheme [1]. The attack does not work in the conventional signature schemes [4, 5] if the (fixed) generator is certified by the trusted authority. Another insider attack on both schemes for an attacker who knows a pair (g, y) is to choose r and s at random and solve the verification equation for parameter β.

The interesting question arises as to whether the resulting scheme will still be insecure if another variant of the meta-ElGamal signature scheme [6, 7] is used as the underlying signature scheme. The answer is yes, as is shown in the following. The signature for message m is (z, r, g, β), where $r' := \beta^k \pmod{p}$, $r := d(r', H(m))$ using a suitable function d, the congruence $A \equiv sB + kC \pmod{w}$ is solved for parameter z where the coefficients A, B and C can be chosen as suitable functions e, f and l with arguments $H(m)$, z, r. Furthermore, the relationship

$$g^{\alpha^s} \equiv \beta^s \pmod{p}$$

holds. The signature can be verified by checking

$$r = d(\beta^{AC^{-1}} y^{-BC^{-1}} \pmod{p}, H(m))$$

where

$$y \equiv g^{\alpha^s} \pmod{p}$$

is computed by the t verifiers. However, as an attacker can influence β and y, all schemes can be universally forged. If the signature (z, r, g, β) for the message m is known then the equation

$$r' \equiv \beta^{AC^{-1}} y^{-BC^{-1}} \pmod{p}$$

holds and the parameter r in A, B and C can be substituted by $d(r', H(m))$. We define the notations $\tilde{A}$, $\tilde{B}$ and $\tilde{C}$ which result from A, B and C respectively, where $H(m)$, r and z are substituted by $H(\tilde{m})$, $\tilde{r}$ and $\tilde{z}$, respectively. To obtain a signature ($\tilde{z}$, $\tilde{r}$, $\tilde{g}$, $\tilde{\beta}$) for the message $\tilde{m}$, we choose $\tilde{z}$ at random, and compute

$$\tilde{r} := d(r', H(\tilde{m}))$$
$$\tilde{\beta} := \beta^{AC^{-1}\tilde{A}^{-1}\tilde{C}} \pmod{p}$$
$$\tilde{g} := g^{BC^{-1}\tilde{B}^{-1}\tilde{C}} \pmod{p}$$

Thus

$$\tilde{r} = d(r', H(\tilde{m})) = d(\beta^{AC^{-1}} y^{-BC^{-1}} \pmod{p}, H(\tilde{m}))$$
$$= d(\tilde{\beta}^{\tilde{A}\tilde{C}^{-1}} \tilde{y}^{-\tilde{B}\tilde{C}^{-1}} \pmod{p}, H(\tilde{m}))$$

because

$$\tilde{y} \equiv \tilde{g}^{\alpha^s} \pmod{p}$$

Therefore, the digital signature scheme with (t, n) shared verification is insecure with any other possible signature scheme. The design problem of the scheme is that the parameters g and β are not authentic and thus could be chosen arbitrarily by an attacker.

This can be prevented if the value $H(\beta, y)$ is additionally signed by the signer using any conventional signature scheme. Thus y (and therefore g) and β are authentic. This signature can only be verified after the t verifiers have computed y. Any unauthorised verifier cannot check the validity of this additional signature, as he does not know y. Obviously, if this countermeasure is used and the functions e, f and l are chosen such that the underlying signature scheme is secure (see [6, 7] for details) then a (t, n) shared verification signature scheme can also be built using other conventional signature schemes. If such a conventional signature scheme is chosen properly, e.g. $d(r', H(m)) = r'$, $A = e(s) = s$, $B = f(H(m), r) = H(m) \oplus r$ and $C = 1$, where $\oplus$ denotes bitwise XOR and an efficient conventional signature scheme is used to authenticate y and β, then the computational costs for signature generation and verification are still reasonable.

18 April 1995

Electronics Letters Online No: 19950771

P. Horster, M. Michels and H. Petersen (*Theoretical Computer Science and Information Security, University of Technology Chemnitz-Zwickau, Straße der Nationen 62, D-09111 Chemnitz, Germany*)

References

1 HARN, L.: 'Digital signature with (t, n) shared verification based on discrete logarithms', *Electron. Lett.*, 1993, **29**, (24), pp. 2094–2095

2 LEE, W.-B., and CHANG, C.-C.: 'Comment: Digital signature with (t, n) shared verification based on discrete logarithms', *Electron. Lett.*, 1995, **31**, (3), pp. 176–177

3 HARN, L.: 'Reply: Digital signature with (t, n) shared verification based on discrete logarithms', *Electron. Lett.*, 1995, **31**, (3), pp. 177

4 ELGAMAL, T.: 'A public key cryptosystem and a signature scheme based on discrete logarithms', *IEEE Trans.*, 1985, **IT-30**, (4), pp. 469–472

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

6 HORSTER, P., MICHELS, M., and PETERSEN, H.: 'Meta-ElGamal signature scheme', Proc. 2nd ACM Conf. Computer and Communications Security, 2–4 November 1994, (Fairfax, Virginia), pp. 96–107

7 HORSTER, P., MICHELS, M., and PETERSEN, H.: 'Generalized ElGamal signatures for one message block', Post-Workshop Proc. IT-Sicherheit'94, 22–23 September 1994, (Vienna, Austria), pp. 66–81