17 June 1996
Electronics Letters Online No: 19961045

B. Preneel (*Katholieke Universiteit Leuven, Department Electrical Engineering-ESAT, COSIC, Kardinaal Mercierlaan 94, B-3001 Heverlee, Belgium*)

P.C. van Oorschot (*Bell-Northern Research/Nortel Secure Networks, PO Box 3511, Station C, Ottawa, K1Y 4H7, Canada*)

References

1 DAVIES, D., and PRICE, W.: 'Security for computer networks' (Wiley, 1989, 2nd edn.)
2 ANXI X9.9 (revised): 'Financial institution message authentication (wholesale)' (American Bankers Association, April 7, 1986)
3 ANXI X9.19: 'Financial institution retail message authentication' (American Bankers Association, April 13, 1986)
4 ISO 8731: 'Banking - approved algorithms for message authentication, Part 1, DEA, Part 2, Message authentication algorithm (MAA)' (ISO, 1987)
5 ISO/IEC 9797: 'Information technology - Data cryptographic techniques - Data integrity mechanisms using a cryptographic check function employing a block cipher algorithm' (ISO/IEC, 1993)
6 FIPS 46: 'Data encryption standard' (NBS, US, Department of Commerce, January 1977)
7 PRENEEL, B., and VAN OORSCHOT, P.C.: 'MDx-MAC and building fast MACs from hash functions'. Advances in Cryptology, CRYPTO'95, Paper Lect. Notes Comput. Sci. 963, 1995, (Springer-Verlag), pp. 1–14
8 WIENER, M.J.: 'Efficient DES key search'. Technical Report TR-244, School of Computer Science, Carleton University, Ottawa, Canada, May 1994
9 FELLER, W.: 'An introduction to probability theory and its applications, Vol. 1' (Wiley, 1968)

Low-computation blind signature schemes based on quadratic residues

Chun-I Fan and Chin-Laung Lei

Indexing terms: Cryptography, Residue arithmetic

The authors propose a low-computation blind signature scheme based on quadratic residues. In the scheme, only a small number of modular computations need to be performed by every signature requester, and the privacy of the requester is protected against the signer.

Introduction: Blind signature schemes are used to protect the privacy of users in many advanced communication services, such as untraceable electronic election and untraceable payment systems [1, 3]. Owing to the fast progress of mobile computing, low-computation software and low-power hardware suitable for wireless communications have been widely studied. In this Letter, we present a low-computation blind signature scheme based on the scheme proposed in [2]. In our proposed scheme, only a few arithmetic modular computations are necessary to obtain a legal signature. Also, to verify a signature, only a small number of modular computations are required. Our blind signature scheme satisfies low-computation requirements and is suitable for low-power mobile communications. The security of our scheme relies on the difficulty of computing the square roots of an integer in Z^*_n, where Z^*_n is the set of all positive integers less than and relatively prime to n. It is infeasible for the signer to derive the exact correspondence between the message he actually signs and the signature submitted by a requester for verification. Compared with the scheme of [2], the security is strengthened, and the size of a legal signature is greatly reduced in our proposed scheme.

Low-computation blind signature scheme: Our blind signature scheme is based on the theory of quadratic residues. Under a modulus n, x is a quadratic residue (QR) in Z^*_n iff there exists an integer y in Z^*_n such that $y^2 \equiv_n x$. Given x, it is infeasible to compute the square root y if n contains large prime factors and the factorisation of n is unknown [6].

There are two kinds of participants, signers and requesters, in our blind signature scheme. A requester requests signatures from the signer, and the signer issues blind signatures to the requester. The proposed protocol consists of four phases: initialisation, requesting, signing, and extraction. The signer publishes the necessary information in the initialisation phase. To obtain the signature of a message, a requester 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 requester. Finally, the requester extracts the signature from the result he receives in the extraction phase. The details of our proposed scheme are presented as follows.

(*i*) *Initialisation phase* (*the signer*): The signer randomly selects $n = p_1p_2p_3p_4$ where all the p_i's are distinct large primes and $p_1 \equiv p_2 \equiv p_3 \equiv p_4 \equiv 3 \pmod 4$. Let $[g|h]$ denote the Jacobi symbol g over h. The signer randomly chooses b_0, b_1, b_2, and b_3 in Z^*_n such that $[b_0|p_1] = [b_0|p_2] = [b_1|p_1] = [b_2|p_2] = 1$ and $[b_1|p_2] = [b_2|p_1] = [b_3|p_1] = [b_3|p_2] = -1$. Compute $A = p_1p_2$. The signer publishes n, A and $B = \{b_0, b_1, b_2, b_3\}$.

(*ii*) *Requesting phase* (*a requester*): To request the signature of a plaintext m in Z^*_n, a requester randomly chooses r and (u^2+Av^2) in Z^*_n, and then sends $(r^2m(u^2+Av^2) \bmod n)$ to the signer. If m has no redundancy, a suitable one-way hash function F should be applied to m to avoid multiplicative attacks.

(iii) *Signing phase* (*the signer*): After receiving $(r^2m(u^2+Av^2) \bmod n)$, the signer randomly selects x and chooses an appropriate integer $b_k \in B$, $0 \le k \le 3$, such that $r^2mb_k(u^2+Av^2)(x^2+A)$ is a QR in Z^*_n. Since the signer knows p_1, p_2, p_3 and p_4, the signer can derive a square root t of $r^2mb_k(u^2+Av^2)(x^2+A)$ in Z^*_n such that $t^2 \equiv_n r^2mb_k(u^2+Av^2)(x^2+A)$ [4, 6]. The signer sends k, t, and x to the requester, where k can be represented by a two-bit string.
(iv) *Extraction phase* (*the requester*): After receiving k, t, and x, the requester computes $e = (r(u-vx))^{-1} \bmod n$, $c = er(ux+Av) \bmod n$, and $s = et \bmod n$. The signature of m is (s, m, c, k). To verify the signature (s, m, c, k), we can examine whether $s^2 \equiv_n mb_k(c^2+A)$.

Analysis: We discuss the correctness, the security and the performance of our proposed scheme in this Section. Theorem 1 ensures its correctness.

(i) *Theorem 1*: Every (s, m, c, k) produced in our protocol satisfies

$$s \equiv_n mb_k(c^2 + A)$$

(ii) *Proof of theorem 1*: By the Chinese remainder theorem, every w in Z^*_n can be represented by $<w_1, w_2, w_3, w_4>$ where $w_1 = w \bmod p_1$, $w_2 = w \bmod p_2$, $w_3 = w \bmod p_3$, and $w_4 = w \bmod p_4$. For convenience, $<w_1, w_2, w_3, w_4>$ is denoted by $<w>$. For every $<a> = <a_1, a_2, a_3, a_4>$ and $<w> = <w_1, w_2, w_3, w_4>$ in Z^*_n, $<aw \bmod n> = <a_1w_1 \bmod p_1, a_2w_2 \bmod p_2, a_3w_3 \bmod p_3, a_4w_4 \bmod p_4>$, $<a^{-1} \bmod n> = <a_1^{-1} \bmod p_1, a_2^{-1} \bmod p_2, a_3^{-1} \bmod p_3, a_4^{-1}$ and $p_4>$.

Assume that $[(r^2m(u^2+Av^2))|p_j] = i_j$ for every $j = 1, 2, 3, 4$. Choose an appropriate $b_k \in B$ such that $[b_k|p_1] = i_1$ and $[b_k|p_2] = i_2$. Then, randomly select x such that $[(b_k(x^2+A))|p_3] = i_3$ and $[(b_k(x^2+A))|p_4] = i_4$. Since $A = p_1p_2$, $[(b_k(x^2+A))|p_1] = [b_k|p_1]\,[x^2|p_1] = i_1$ and $[(b_k(x^2+A))|p_2] = [b_k|p_2]\,[x^2|p_2] = i_2$. $[(r^2mb_k(u^2+Av^2)(x^2+A))|p_j] = [(r^2m(u^2+Av^2))|p_j]\,[(b_k(x^2+A))|p_j] = (i_j)^2 = 1$ for every $j = 1, 2, 3, 4$, so $r^2mb_k(u^2+Av^2)(x^2+A)$ is a QR in Z^*_n. In addition, $r^2mb_k(u^2+Av^2)(x^2+A) \equiv_n r^2mb_k(ux+Av)^2+A(u-vx)^2) \equiv_n mb_k(r^2(ux+Av)^2+Ar^2(u-vx)^2) \equiv_n mb_k(r^2(ux+Av)^2+Ae^{-2}) \equiv_n e^{-2}mb_k(e^2r^2(ux+Av)^2+A) \equiv_n e^{-2}mb_k(c^2+A)$.

It is clear that $mb_k(c^2+A)$ is a QR in Z^*_n because e^{-2} and $e^{-2}mb_k(c^2+A)$ are QRs in Z^*_n. Since $<e^{-1}> = <e^{-1} \bmod p_1, e^{-1} \bmod p_2, e^{-1} \bmod p_3, e^{-1} \bmod p_4> = <(e^{-1})_1, (e^{-1})_2, (e^{-1})_3, (e^{-1})_4>$, the 16 square roots of e^{-2} in Z^*_n are $<\pm(e^{-1})_1, \pm(e^{-1})_2, \pm(e^{-1})_3, \pm(e^{-1})_4>$. Similarly, if $<d_1, d_2, d_3, d_4>$ is a square root of $mb_k(c^2+A)$ in Z^*_n, the 16 square roots of $mb_k(c^2+A)$ in Z^*_n are $<\pm d_1, \pm d_2, \pm d_3, \pm d_4>$. Thus, the set of the 16 square roots of $e^{-2}mb_k(c^2+A)$ in Z^*_n is $\{gh \bmod n \mid g$ is a square root of e^{-2} in Z^*_n and h is a square root of $mb_k(c^2+A)$ in $Z^*_n\} = \{<\pm(e^{-1})_1d_1, \pm(e^{-1})_2d_2, \pm(e^{-1})_3d_3, \pm(e^{-1})_4d_4>\}$. Since t is a square root of $e^{-2}mb_k(c^2+A)$ in Z^*_n, $<t>$ is an element of $\{<\pm(e^{-1})_1d_1, \pm(e^{-1})_2d_2, \pm(e^{-1})_3d_3, \pm(e^{-1})_4d_4>\}$. $s = (et \bmod n)$, so $<s>$ belongs to $\{<\pm e_1(e^{-1})_1d_1, \pm e_2(e^{-1})_2d_2, \pm e_3(e^{-1})_3d_3, \pm e_4(e^{-1})_4d_4>\} =$

$\{<\pm d_1, \pm d_2, \pm d_3, \pm d_4>\}$. Thus, s is a square root of $mb_k(c^2+A)$ in Z^*_n. Therefore, $s^2 \equiv_n mb_k(c^2+A)$. □

Given an integer w, it is computationally infeasible to derive any square root of w in Z^*_n without the trapdoors p_1, p_2, p_3 and p_4 [6]. In addition, given an integer w, a solution (a_1, a_2) of the congruence $a_1^2+Aa_2^2 \equiv_n w$ cannot be found by the Pollard-Schnorr algorithm since $gcd(A,n) \neq 1$ [5]. Since the plaintext message m contains appropriate redundancy, it is infeasible to construct an unauthorised signature (s, m', c', k') from a legal signature (s, m, c, k) such that $b_{k'} \in B$ and $s^2 \equiv_n m'b_{k'}(c'^2+A) \equiv_n mb_k(c^2+A)$. In our scheme, p_1, p_2, p_3 and p_4 are kept secret by the signer, so it is also infeasible for others to produce any legal signature (s, m, c, k).

In the scheme of [2], for every requester i, the signer can keep (x_i, y_i, t_i, z_i) of requester i in the signing phase where $z_i = r_i^2 m_i(u_i^2+Av_i^2) \bmod n$ and r_i, m_i, u_i, v_i are selected by requester i. Assume that some requester computes $s = r^{-1}t \bmod n$, $c = (ux+Avy) \bmod n$ and $e = (uy-vx) \bmod n$ in the extraction phase in the scheme of [2], and the signature shown for verification is (s, m, b, c, e), where $b \in B$. For every (x_i, y_i, t_i, z_i), the signer can find r'_i, u'_i, v'_i such that $s = r'^{-1}_i t_i \bmod n$, $c = (u'_i x_i + Av'_i y_i) \bmod n$ and $e = (u'_i y_i - v'_i x_i) \bmod n$. And, if $(r'^2_i m(u'^2_i + Av'^2_i) \bmod n) = z_i$, then the requester is requester i. It is quite time consuming to perform exhaustive comparisons to derive the link if the database kept by the signer is large, however, the signer can monitor a particular individual (or a small group) and quickly derive the link between a signature and its requester in the scheme proposed in [2]. Therefore, strengthening of the privacy of requesters in the scheme of [2] is greatly desired.

In our proposed scheme, the privacy of requesters is strengthened to avoid the above attack by revealing less information in the signature. If x is selected by the signer in the signing phase during a certain run of the proposed protocol, then for every signature (s, m, c, k) shown for verification, there exists a great amount of (u', v')s such that $c = (u'-v'x)^{-1}(u'x+Av') \bmod n$. In addition, since all (r, u, v)s are kept secret by the requesters, all signatures with the same k are equally likely from the signer's point of view. Therefore, it is computationally infeasible for the signer to derive the exact correspondence between the message $(r^2 mb_k(u^2+Av^2)(x^2+A) \bmod n)$ he actually signs and the message (s, m, c, k) submitted by a requester for verification later.

Only a small number of modular arithmetic computations are performed by a requester in each phase of the proposed scheme. In our scheme, to obtain a signature, a requester performs six multiplications and one addition operation in the requesting phase, and one inverse, seven multiplications, one addition, and one subtraction operation in the extraction phase. Only four multiplications, one addition, and one comparison operation are needed to verify a signature. All the above computations are performed in Z^*_n. Moreover, the signature size is greatly reduced in our scheme, since the size of the signature (s, m, c, k) is ~60% of (s, m, b, c, e) of [2], where k is a two-bit number.

Conclusions: In this Letter, a low-computation and secure blind signature technique has been presented. The correctness, security, and performance of the proposed scheme have also been discussed. The privacy of all requesters is protected against the signer. Compared with the original scheme, the security of our proposed blind signature scheme is strengthened. Furthermore, the blind signature scheme achieves the low-computation requirements for mobile requesters, and the storage required in our proposed scheme is much less than at required in the original scheme.

11 June 1996
Electronics Letters Online No: 19961084

Chun-I Fan and Chin-Laung Lei (*Department of Electrical Engineering, Room 246, New E.E. Building, National Taiwan University, Taipei, Taiwan, Republic of China*)

References

1 CHAUM, D.L.: 'Blind signatures for untraceable payments'. Advances in Cryptology – CRYPTO'82, Lecture Notes in Computer Science (Springer-Verlag, 1982), pp. 191–203

2 FAN, C.I., and LEI, C.L.: 'Efficient blind signature scheme based on quadratic residues', *Electron. Lett.*, 1996, **32**, (9), pp. 811–813

3 JUANG, W.S., LEI, C.L., and FAN, C.I.: 'A collision free secret ballot protocol for computerized general elections'. Int. Computer Symp., Taiwan, R.O.C., 1994, **1**, pp. 309–314

4 PERALTA, R.C.: 'A simple and fast probabilistic algorithm for computing square roots modulo a prime number', *IEEE Trans.*, 1986, **IT-32**, (6), pp. 846–847

5 POLLARD, J.M., and SCHNORR, C.P.: 'An efficient solution of the congruence $x^2+ky^2 = m$ (mod n)', *IEEE Trans.*, 1987, **IT-33**, (5), pp. 702–709

6 RABIN, M.O.: 'Digitalized signatures and public-key functions as intractable as factorization'. Technical Report, MIT/LCS/TR212, MIT Lab., Computer Science, Cambridge, Mass., January 1979

Verifiable signature sharing for DSA with heuristic security

D. Feng

Indexing terms: Cryptography, Security of Data

The author points out that verifiable signature sharing (VΣS) for the DSA proposed by Franklin *et al.* at Eurocrypt'95 does not possess heuristic security, and he proposes an improved scheme which does possess heuristic security.

Introduction: In [1] Franklin *et al.* introduced verifiable signature sharing (VΣS), a cryptographic primitive for protecting digital signatures. VΣS enables the holder of a digitally signed document, who may or may not be the original signer, to share the signature among a set of proxies so that the honest proxies can later reconstruct it. At the end of the sharing phase, each proxy can verify whether a valid signature for the document can be reconstructed, even if the original signature holder and / or some proxies are malicious. In addition, malicious proxies gain no information about the signature held by an honest sharer prior to reconstruction (but do see the document itself). Some efficient VΣS schemes for exponetiation based signatures (e. g. RSA, Rabin) and discrete log based signatures (e. g. ElGamal, Schnorr, DSA) have been presented in [1]. However, the VΣS scheme for the DSA is not secure at all. In this Letter I would like to point out that the VΣS scheme for the DSA does not possess heuristic security, and propose an improved scheme which possesses heuristic security.

VΣS for DSA proposed by Franklin et al.: In the DSA, the public key is g, y, p, q where p is a large prime, q is a large prime factor of $p-1$, g is a generator of Z_q^*, and $y = g^x \bmod p$ for some private key $x \in Z_q^*$. The signature of a document m is $\sigma(m) = [r, s]$, where $r = (g^k \bmod p) \bmod q$ for some $k \in_R Z_q^*$, and where $s = k^{-1}(h(m)+xr) \bmod q$ for a one-way hash function h into Z_q^*. To verify a signature, anyone can check that $r = (g^{u_1} y^{u_2} \bmod p) \bmod q$, where $u_1 = h(m)s^{-1} \bmod q$, and where $u_2 = rs^{-1} \bmod q$. A VΣS scheme for the DSA proposed by Franklin *et al.* proceeds as follows. The sharer reliably broadcasts m, s, α to all proxies, where $\alpha = y^{u_2} \bmod p$. The sharer verifiably shares u_2 to the proxies so that they are convinced it is the log of $\alpha \bmod p$ with respect to the base y. The proxies accept if they accept the log sharing protocol, and if $y^v \equiv \alpha^v \bmod p$, where $v = (g^{u_1}\alpha \bmod p) \bmod q$. The signature will be easy to reconstruct since $r = u_2 s \bmod q$.

Cryptanalysis: Any proxy who received the broadcast values m, s, α can reconstruct r. Since he can compute u_1, $u_1 = h(m)s^{-1} \bmod q$ ($h(\cdot)$ is public), thus, $r = (g^{u_1}\alpha \bmod p) \bmod q$. It is shown that any proxy who received the broadcast values m, s, α can reconstruct r without knowing u_2, i.e. the log of $\alpha \bmod p$ with respect to the base y. This result shows that VΣS for the DSA proposed by Franklin *et al.* does not possess heuristic security.

Improved scheme: An improved VΣS scheme for the DSA is as follows: the sharer reliably broadcasts m, r, α, A to all proxies, where $\alpha = y^{u_2} \bmod p$, $A = \alpha^s \bmod p$. The sharer verifiably shares s to the proxies so that they are convinced that it is the log of $s \bmod q$ with respect to the base α. The proxies accept if they accept the