exchange. For simplicity, we assume that A and B want to share four secrets.

(i) A generates two random short-term secret keys, $k_{A_1}$ and $k_{A_2}$, and two corresponding public keys, $r_{A_1}$ and $r_{A_2}$, $r_{A_1} < r_{A_2}$. Then, A computes the signature $s_A$ for $\{r_{A_1}, r_{A_2}\}$ based on any signature variant as listed in Table 1. For example, A obtains $s_A$ by solving the following equation

$$x_A = r_{A_1}k_{A_1} + r_{A_2}k_{A_2} + s_A \bmod p - 1$$

A sends $\{r_{A_1}, r_{A_2}, s_A, cert(y_A)\}$ to B, where $cert(y_A)$ is the public-key certificate of $y_A$ signed by a trusted party.

(ii) Similarly, $B$ generates $k_{B_1}$, $k_{B_2}$, $r_{B_1}$, $r_{B_2}$, $s_B$ and sends $\{r_{B_1}, r_{B_2}, s_B, cert(y_B)\}$ to A.

(iii) A verifies $\{r_{B_1}, r_{B_2}\}$ based on the signature $s_B$ and B's public key $y_B$ by checking

$$y_B = r_{B_1}^{r_{B_1}} r_{B_2}^{r_{B_2}} \alpha^{s_B} \bmod p$$

Then A computes the shared secret keys as

$$K_1 = r_{B_1}^k A_1 \bmod p$$
$$K_2 = r_{B_1}^k A_2 \bmod p$$
$$K_3 = r_{B_2}^k A_1 \bmod p$$
$$K_4 = r_{B_2}^k A_2 \bmod p$$

(iv) Similarly, B computes $\alpha^{r_{A_1}r_{A_2}} \bmod p$ first and verifies $\{r_{A_1}, r_{A_2}\}$. Then, B computes the shared secret keys as

$$K_1 = r_{A_1}^k B_1 \bmod p$$
$$K_2 = r_{A_2}^k B_1 \bmod p$$
$$K_3 = r_{A_1}^k B_2 \bmod p$$
$$K_4 = r_{A_2}^k B_2 \bmod p$$

*Discussion:* We point out here that we have modified the original protocol [8] in signature signing and verification equations. Two recent attacks [10, 11] on the original protocol cannot work successfully in this modified protocol. This modified protocol does not increase any computational load and the key agreement protocol does not involve any additional one-way hash function.

The signatures, $x_A$ and $x_B$, satisfy the following equations as

$$x_A = r_{A_1}k_{A_1} + r_{A_2}k_{A_2} + s_A \bmod p - 1 \quad \text{and}$$
$$x_B = r_{B_1}k_{B_1} + r_{B_2}k_{B_2} + s_B \bmod p - 1$$

By multiplying these two equations together, we obtain

$$\begin{aligned} x_A x_B = {} & r_{A_1}r_{B_1}k_{A_1}k_{B_1} + r_{A_1}r_{B_2}k_{A_1}k_{B_2} + r_{A_1}s_B k_{A_1} \\ & + r_{A_2}r_{B_1}k_{A_2}k_{B_1} + r_{A_2}r_{B_2}k_{A_2}k_{B_2} + r_{A_2}s_B k_{A_2} \\ & + s_A r_{B_1}k_{B_1} + s_A r_{B_2}k_{B_2} + s_A s_B \bmod p - 1 \end{aligned}$$

In other words, we have

$$\begin{aligned} K_{AB} = {} & K_1^{r_{A_1}r_{B_1}} K_2^{r_{A_2}r_{B_1}} K_3^{r_{A_1}r_{B_2}} K_4^{r_{A_2}r_{B_2}} \\ & \times r_{A_1}^{r_{A_1}s_B} r_{A_2}^{r_{A_2}s_B} r_{B_1}^{r_{B_1}s_A} r_{B_2}^{r_{B_2}s_A} \alpha^{s_A s_B} \bmod p \end{aligned}$$

If the adversary knows four consecutive shared secret keys, he can solve the long-term shared secret $K_{AB}$. Thus, to achieve the perfect forward secrecy, we should limit ourselves to use only three out of the four shared secret keys. The protocol can be generalised to enable A and B to share $n^2 - 1$ secrets if each user computes and sends $n$ Diffie-Hellman public keys in each pass. Since each user only needs to generate (verify) one signature for $n$ different Diffie-Hellman public keys to establish $n^2 - 1$ shared secret keys, this new protocol is very efficient.

*Conclusion:* We have proposed an authenticated key agreement protocol that utilises a digital signature to authenticate Diffie-Hellman public keys. We summarise features in this new protocol as follows:

(i) Since we integrate the Diffie-Hellman public key in the signature scheme, this approach reduces overall computation.

(ii) Since the protocol does not use any one-way hash function, the security assumption relies solely on solving the discrete logarithm problem.

(iii) This protocol allows two communication parties to share multiple secret keys in two-pass interaction.

(iv) The computation for shared secret keys is simpler than the MQV protocol.


*14 March 2001*
*Electronics Letters Online No: 20010441*
*DOI: 10.1049/el:20010441*

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

H.-Y. Lin (*Computer Science Department, California State University, San Marcos, CA 92096-0001, USA*)

### References

1 DIFFIE, W., and HELLMAN, M.E.: 'New directions in cryptography', *IEEE Trans. Inf. Theory*, 1976, **IT-22**, (6), pp. 644–654
2 ARAZI, A.: 'Integrating a key cryptosystem into the digital signature standard', *Electron. Lett.*, 1993, **29**, (11), pp. 966–967
3 NYBERG, K., and RUEPPEL, R.A.: 'Message recovery for signature scheme based on the discrete logarithm problem'. Proc. Eurocrypt '94, May 1994, pp. 175–190
4 ELGAMAL, T.: 'A public-key cryptosystem and a signature scheme based on discrete logarithms', *IEEE Trans. Inf. Theory*, 1985, **IT-31**, pp. 469–472
5 DOBBERTIN, H.: 'The status of MD5 after a recent attack', *CryptoBytes*, 1996, **2**, (2), pp. 1–6
6 MENEZES, A.J., QU, M., and VANSTONE, S.A.: 'Some key agreement protocols providing implicit authentication'. 2nd Workshop Selected Areas in Cryptography, 1995
7 IEEE P1363/Editorial Contribution (Draft). In http://stdsbbs.ieee.org/groups/1363/edcont.html
8 HARN, L., and LIN, H.Y.: 'An authenticated key agreement protocol without using one-way function'. Proc. 8th Nat. Conf. Information Security, Kaohsiung, Taiwan, May 1998, pp. 155–160
9 HARN, L.: 'Digital signatures for Diffie-Hellman public keys without using one-way function', *Electron. Lett.*, 1997, **33**, (2), pp. 125–126
10 YEN, S.M., and JOYE, M.: 'Improved authenticated multiple-key agreement protocol', *Electron. Lett.*, 1998, **34**, (18), pp. 1738–1739
11 WU, T.S., HE, W.H., and HSU, C.L.: 'Security of authenticated multiple-key agreement protocols', *Electron. Lett.*, 1999, **35**, (5), pp. 391–392
12 LIM, C.H., and LEE, P.J.: 'Security of interactive DSA batch verification', *Electron. Lett.*, 1994, **30**, (19), pp. 1592–1593

## Cryptanalysis on improved user efficient blind signatures

C.-I. Fan and C.-L. Lei

Shao proposed a blind signature scheme based on the Fan-Lei scheme. It is shown here that Shao's scheme is not secure. Also, Shao claimed that the Fan-Lei scheme is not really blind, however this claim is demonstrated as not being true.

*Introduction:* In 1996, Fan and Lei proposed a blind signature scheme based on quadratic residues (QRs) [1], and they also presented an enhanced version of the scheme to reduce the computation for requesters or users [2]. In [3], Shao proposed a blind signature scheme based on the Fan-Lei scheme [2]. However, we find that Shao's scheme cannot withstand Pollard-Schnorr attacks [4]. Besides, Shao claimed that the Fan-Lei blind signature scheme [2] is not really blind. In this Letter, we also show that Shao's claim is not true.

*Attacks on Shao's blind signature scheme:* Shao proposed a blind signature scheme based on the Fan-Lei scheme in [3]. We show that Pollard-Schnorr attacks [4] are valid on Shao's scheme as follows. In the scheme of [3], the tuple $(c, s)$ is a signature of $m$ and they can be verified by checking if

$$H(m)s^2(c^2 + 1) = 1 \bmod n \qquad (1)$$

An attacker can choose a message $m$ and then derive $(w, y)$ in polynomial time such that

$$w^2 + y^2 = H(m)^{-1} \bmod n$$

through the method introduced by [4] without knowing the factorisation of $n$. Thus, the attacker has that $H(m)y^2((y^{-1}w)^2 + 1) = 1 \bmod n$. Let $s = y \bmod n$ and $c = y^{-1}w \bmod n$. The attacker can form a valid signature $(c, s)$ of $m$ such that eqn. 1 is satisfied without knowing $p$ or $q$. Hence, Shao's scheme cannot withstand Pollard-Schnorr attacks [4].

*Shao's claims:* In [3], Shao claimed that the Fan-Lei blind signature scheme [2] is not really blind. We show below that Shao's claim is not true. In the Fan-Lei blind signature scheme [2], the signer can keep a set of records $\{(\alpha_i, \beta_i, x_i, t_i) \mid$ for every instance $i$ of the protocol$\}$, where

$$\alpha_i = H(m_i)(u_i^2 + v_i^2) \bmod n$$
$$\beta_i = b_i^2(u_i x_i + v_i) \bmod n$$
$$t_i^4 = \alpha_i(x_i^2 + 1)\lambda_i^2 = \frac{H(m_i)(u_i^2 + v_i^2)(x_i^2 + 1)}{b_i^4(u_i x_i + v_i)^2} \bmod n$$

Assume that the signature $(H(m), c, s)$ of a message $m$ is revealed by the requester or user, where

$$c = \delta\lambda(u - vx) \bmod n = (u - vx)/(ux + v) \bmod n$$
$$s = bt \bmod n$$
$$s^4 = H(m)(c^2 + 1) \bmod n$$

and $u$, $v$, $b$ are secret parameters selected by the requester or user. Given $(H(m), c, s)$, the signer can derive a triple $(u_i', v_i', b_i')$ for each stored record $(\alpha_i, \beta_i, x_i, t_i)$ through the following:

$$b_i' = st_i^{-1} \bmod n$$
$$u_i' x_i + v_i' = \beta_i(b_i')^2 = \beta_i t_i^2 s^{-2} \bmod n$$
$$u_i' - v_i' x_i = c(u_i' x_i + v_i') = c\beta_i t_i^2 s^{-2} \bmod n$$

From the above equations, the signer can evaluate

$$u_i' = \beta_i t_i^2 s^{-2}(x_i + c)(x_i^2 + 1)^{-1} \bmod n$$
$$v_i' = \beta_i t_i^2 s^{-2}\left(1 - x_i(x_i + c)(x_i^2 + 1)^{-1}\right) \bmod n$$

Thus, we have that

$$\begin{aligned}
&H(m)((u_i')^2 + (v_i')^2) \\
&= H(m)\beta_i^2 t_i^4 s^{-4}\Big((x_i + c)^2(x_i^2 + 1)^2 \\
&\quad + \left(1 - x_i(x_i + c)(x_i^2 + 1)^{-1}\right)^2\Big) \\
&= H(m)\beta_i^2 t_i^4 s^{-4}\left((x_i + c)^2(x_i^2 + 1)^{-2} + 1\right. \\
&\quad \left. -2x_i(x_i + c)(x_i^2 + 1)^{-1} + x_i^2(x_i + c)^2(x_i^2 + 1)^{-2}\right) \\
&= H(m)\beta_i^2 t_i^4 s^{-4}\left((x_i + c)^2(x_i^2 + 1)^{-1} + 1\right. \\
&\quad \left. -2x_i(x_i + c)(x_i^2 + 1)^{-1}\right) \\
&= H(m)\beta_i^2 t_i^4 s^{-4}\left((x_i + c)(x_i^2 + 1)^{-1}(c - x_i) + 1\right) \\
&= H(m)\beta_i^2 t_i^4 s^{-4}(x_i^2 + 1)^{-1}\left((x_i + c)(c - x_i) + (x_i^2 + 1)\right) \\
&= H(m)\beta_i^2 t_i^4 s^{-4}(x_i^2 + 1)^{-1}(c^2 + 1) \\
&= H(m)\beta_i^2 \alpha_i (x_i^2 + 1)\lambda_i^2 s^{-4}(x_i^2 + 1)^{-1}(c^2 + 1) \\
&= H(m)\beta_i^2 \alpha_i \lambda_i^2 s^{-4}(c^2 + 1) = H(m)\alpha_i s^{-4}(c^2 + 1) \\
&= H(m)\alpha_i\left(H(m)(c^2 + 1)\right)^{-1}(c^2 + 1) \\
&= \alpha_i \bmod n
\end{aligned}$$

Hence, given $(H(m), c, s)$, the signer can derive $(u_i', v_i')$ for each stored record $(\alpha_i, \beta_i, x_i, t_i)$ and the checking equation

$$\alpha_i = H(m)((u_i')^2 + (v_i')^2) \bmod n$$

is always satisfied. This is the blindness property in the Fan-Lei blind signature scheme [2]. Besides, Shao claimed that a quadratic residue (QR) in $Z_n^*$ possibly does not have a fourth root in $Z_n^*$. The claim is not true. Since $n = pq$ is a Blum integer, i.e. $p$ and $q$ are two distinct primes and $(p \bmod 4) = (q \bmod 4) = 3$, any QR in $Z_n^*$ has a fourth root in $Z_n^*$ [5]. In the Fan-Lei blind signature scheme [2], no modular exponentiation and inverse computations are performed by requesters or users. Moreover, only several modular additions and multiplications are required for a requester or user to obtain and verify a signature in the scheme. However, the scheme of [2] does not decrease the computation load for the signer. In almost all of the applications based on blind signatures, the signer usually possesses much more computation capacities than a requester or 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 requesters or users are limited in some situations such as mobile clients and smart-card users. Therefore, it is more urgent to reduce the computation load for the requesters or users than that for the signer.


*13 February 2001*
*Electronics Letters Online No: 20010422*
*DOI: 10.1049/el:20010422*

C.-I. Fan (*Telecommunication Laboratories, Chunghwa Telecom Co. Ltd. PO Box 8-210, Shin-Juang, Taiwan 242, Republic of China*)

E-mail: chunifan@ms35.hinet.net

C.-L. Lei (*Department of Electrical Engineering, National Taiwan University, Taipei, Taiwan 107, Republic of China*)

**References**

1 FAN, C.I., and LEI, C.L.: 'A multi-recastable ticket scheme for electronic elections'. Advances in Cryptology-ASIACRYPT'96, 1996, Springer-Verlag, LNCS 1163, pp. 116–124
2 FAN, C.I., and LEI, C.L.: 'User efficient blind signatures', *Electron. Lett.*, 1998, **34**, (6), pp. 544–546
3 SHAO, Z.: 'Improved user efficient blind signatures', *Electron. Lett.*, 2000, **36**, (16), pp. 1372–1374
4 POLLARD, J.M., and SCHNORR, C.P.: 'An efficient solution of the congruence $x^2 + ky^2 = m$ (mod $n$)', *IEEE Trans. Inf. Theory*, 1987, **33**, (5), pp. 702–709
5 MENEZES, A., VAN OORSCHOT, P., and VANSTONE, S.: 'Handbook of applied cryptography' (CRC Press LLC, 1997)

## Family size of orthogonal Oppermann sequences

Guozhen Zang and Cong Ling

A supplement is provided for Oppermann's orthogonal sequences with a wide range of correlation properties. It is shown that there exist identical sequences within the sequence set under many circumstances. The number of distinct orthogonal sequences in the sequence set is presented.

*Introduction:* Oppermann and Vucetic [1] proposed a new family of complex-valued spreading sequences for code division multiple access (CDMA) systems, the wide range of correlation properties of which offers a great variety of trade-offs between auto-correlation and cross-correlation functions. This family includes some specific sequence families, such as the Frank-Zadoff-Chu (FZC) sequences [2, 3]. A subsequent paper by Oppermann [4] proved that there exists an orthogonal subfamily of the new sequences. In this Letter, it is shown that there possibly exist identical sequences in the orthogonal set. The size of the orthogonal set, or the number of distinct sequences, is presented.

*Orthogonal Oppermann sequences:* Let $N$ be the sequence length. Let $M$ take integer values that are relatively prime to $N$ such that $1 \le M < N$. The set of sequences is defined by $U_{m,p,n}(N) = \{u_M : 1 \le M < N\}$ [1], while the $i$th element of a given sequence $u_M$ is defined by

$$u_M(i) = (-1)^{Mi} \exp\left(\frac{j\pi(M^m i^p + i^n)}{N}\right) \qquad 1 \le i \le N \tag{1}$$

where $j^2 = -1$ and $m$, $p$, and $n$ are real numbers. The triple $\{m, p, n\}$ specifies the sequence set and determines the characteristics of the sequences. If $p = 1$, each sequence in the set will have the same auto-correlation function magnitude [1]. It was stated in [1] that the maximum number of sequences is determined by Euler's