Remarks on new Digital Signature Algorithm based on Factorization and Discrete Logarithm problem

Shin-Yan Chiou[1], Yi-Xuan He[2]
Department of Electrical Engineering, Chang Gung University,
259 Wen-Hwa 1st Road, Kwei-Shan Tao-Yuan, Taiwan, 333, R.O.C.

***Abstract*—Most digital signature schemes have the common feature that they are based on a single cryptographic assumption, like integer factorization problem (IFP) or discrete logarithm problem (DLP). For example, RSA scheme is based on the IFP, and ElGamal scheme is based on the DLP. So far, these hard problems still cannot be solved efficiently and we believe that the schemes are secure. However, if these problems can be solved by an efficient method in the future, the associated cryptographic scheme will no longer be secure. Thus, people try to enhance the security of cryptographic schemes by constructing them based on multiple hard problems simultaneously. Recently, S. Vishnoi and V. Shrivastava proposed a new signature scheme which is based on factorization and discrete logarithm problem, denoted as V & S scheme in this paper. S. Vishnoi and V. Shrivastava claimed that their scheme is secure and its security is based on the difficulty of computing factoring and discrete logarithms. In this paper, we show that this scheme is not secure and is not based on any hard problems; a simple attack is given.**

***Keywords*—Digital signature, Discrete logarithm, Factorization, Cryptanalysis, Forge**

I. Introduction

MOST digital signature schemes have the common feature that they are based on a single cryptographic assumption [1], like integer factorization problem (IFP) or discrete logarithm problem (DLP). For example, RSA scheme [2] is based on the IFP, and ElGamal scheme [3] is based on the DLP. So far, these hard problems still cannot be solved efficiently and we believe that the schemes are secure. However, if these problems can be solved by an efficient method in the future, the associated cryptographic scheme will no longer be secure. Thus, people try to enhance the security of cryptographic schemes by constructing them based on multiple hard problems simultaneously.

Integer factorization problem means that no efficient, non-quantum integer factorization algorithms known when the numbers are very large. The presumed difficulty of this problem is at the heart of widely used algorithms in cryptography such as RSA.

Discrete logarithm problem is defined as: given a group G, a generator g of the group and an element h of G, to find the discrete logarithm to the base g of h in the group G. Discrete logarithm problem is not always hard. The hardness of finding discrete logarithms depends on the groups. For example, a popular choice of groups for discrete logarithm based crypto-systems is Z_p^* where p is a prime number. However, if $p-1$ is a product of small primes, then the Pohlig–Hellman algorithm [4] can solve the discrete logarithm problem in this group very efficiently.

In 1988, McCurley firstly proposed a secret key distribution scheme based on the IFP and the DLP [5]. Later, many digital signature schemes based on the IFP and the DLP have been proposed [6-16]. However, to design such schemes is not an easy task since many of them have been proven to be insecure [8-11, 13, 14, 17-24], or their security is not really based on two hard problems simultaneously.

Recently, S. Vishnoi and V. Shrivastava proposed a new signature scheme which is based on factorization and discrete logarithm problem [25], denoted as V & S scheme in this paper. S. Vishnoi and V. Shrivastava claimed that their scheme is secure and its security is based on the difficulty of computing factoring and discrete logarithms. In this paper, we show that this scheme is not secure and is not based on any hard problems; a simple attack is given.

The paper is organized as follows: In Section 2, we review the V & S scheme. In Section 3, we will propose a method which forging the signature of the V & S scheme and verify it. Finally, in Section 4, we conclude the paper.

II. Review of the V & S Scheme

There are three phases in this scheme: key generation, signature generation, and signature verification. The following parameters and notations will be used throughout the scheme unless otherwise specified:

- p : is a large prime such that computing discrete logarithms modulo p is difficult.
- n : is the product of two safe prime p_1 and q_1 such that $p < n$.
- $\varphi(.)$: is a Euler-phi function.
- $\gcd(a,b)$: is the greatest common divisor of a and b.
- Z_n^* : reduced set of residues modulo n.
- $H(.)$: is a one way hash function.
- z^{-1} : is the multiplicative inverse of z with respect to $\bmod\ (p\text{-}1)$.

A. Key Generation

- Calculate $\varphi(n) = (p_1 - 1) \times (q_1 - 1)$
- Choose random numbers k and v such that $1 < k, v < p - 1$.
- Choose random numbers x, r and b such that $1 < x, r, b < n - 1$. x should be relative prime to $\varphi(\text{n})$ (i.e. $\gcd(x, \varphi(\text{n})) = 1$)
- Choose a primitive root g in Z_n^*
- Calculate c such that $b^x \times c = 1 \bmod n$
- Calculate u, w, t and y as follows:

$$u = g^k \bmod p,$$ [1]

$$w = g^v \bmod p,$$

$$t = u^w \bmod p,$$ [2]

$$y = r^x \bmod n.$$

- Public key is (x, c, g) and private key is (k, v, u, w, b, r).

B. *Signature Generation*

Step-1:

Choose an integer z such that $1 < z < (p-1)$, $\gcd(z, p-1) = 1$. z should be different for every message m and is not public.

Step-2: Calculate

$$h = g^z \bmod p,$$

$$\gamma = t \times w^h \bmod p,$$

$$f = \left(r \times b^{H(m)}\right) \bmod n,$$

$$s = \left((H(m) - kw - hv + yz) \times z^{-1}\right) \bmod (p\text{-}1)$$

If $t = 0$ and/or $f = 0$ and/or $s = 0$ then repeat step 1 and 2 else tuple (γ, h, f, s) is the signature of m.

Here $-kw$, $-hv$ are additive inverse of kw and hv respectively.

C. *Signature Verification*

- Calculates $H(m)$ using the received message m at receiver's end.
- If $g^{H(m)} \times h^{(f^x \times c^{H(m)} \bmod n)} \equiv \gamma \times h^s \bmod p$ then the signature is valid else reject the signature.

III. Security Analysis of the V & S Scheme

This section shows the V & S scheme can be forged and without solving any hard problems. The forged methods and proofs are as follows:

A. *Forge Signature Method*

An adversary (Adv) tries to forge someone's signature of m' successfully. He just follows the steps and without solving any hard problems.

Step-1: Choose an integer z' such that $1 < z' < (p-1)$, $\gcd(z', p-1) = 1$. Calculate $h' = g^{z'} \bmod p$.

Step-2: Choose an integer f' such that $1 < f' < n\text{-}1$.

Step-3: Calculate $\gamma' = h'^{\left((f')^x \times c^{H(m')} \bmod n\right)} \bmod p$.

Step-4: Calculate $s' = H(m') \times (z')^{-1} \bmod p\text{-}1$.

Finally, $Sig(m') = (\gamma', h', f', s')$

B. *Proof of Correctness*

According to the verified equation:

$$g^{H(m)} \times h^{(f^x \times c^{H(m)} \bmod n)} \equiv \gamma \times h^s \bmod p$$

L.H.S.

$$= g^{H(m')} \times g^{z' \times \left((f')^x \times c^{H(m')} \bmod n\right)} \bmod p$$

$$= g^{H(m') + \left(z' \times (f')^x \times c^{H(m')} \bmod n\right)} \bmod p$$

[1]The original paper is $u = g^x \bmod p$, but we can see that this is a clerical error by studying "Proof of Correctness."

[2]The original paper is $t = u^x \bmod p$, but we can see that this is a clerical error by studying "SECURITY ANALYSIS."

R.H.S.

$$= h'^{\left((f')^{x}\times c^{H(m')} \bmod n\right)} \times g^{z'\times H(m')\times (z')^{-1}} \bmod p$$

$$= g^{z'\times\left((f')^{x}\times c^{H(m')} \bmod n\right)} \times g^{H(m')} \bmod p$$

$$= g^{H(m')+\left(z'\times (f')^{x}\times c^{H(m')} \bmod n\right)} \bmod p$$

Therefore, L.H.S. is equal to R.H.S.

IV. Conclusion

In this paper, we first reviewed the V & S scheme, and then we gave a method can forge the signature of the V & S scheme. Finally, we derived from formula to prove the validity of this method. According to the above paragraphs, it is evident that the V & S scheme is insecure. Anyone can forge the signature easily and verify successfully does not have private key.

Acknowledgment

This work is partially supported by the NSC project under Grant NSC 102-2221-E-182 -038. The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

References

[1] W.Diffie and M. E.Hellman, "New direction in cryptography," *IEEE Transaction on Information Networking and Application*, pp. 557–560, 1975.
[2] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signature and public-key cryptosystem," *Communications of the ACM*, vol. 21, no. 2, pp. 120–126, 1978.
[3] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transaction on Information Theory*, vol. IT-31, no. 4, pp. 469–472, 1985.
[4] S. Pohlig and M. Hellman, "An improved algorithm for computing logarithms over $GF(p)$," *Information Theory, IEEE Transactions on* 24.1: 106-110, 1978.
[5] K. S. McCurley, "A key distribution system equivalent to factoring," *Journal of cryptology*, 1.2 : 95-105 , 1988.
[6] L. Harn, "Public-key cryptosystem design based on factoring and discrete logarithms," *IEE Proceedings-Computers and Digital Techniques,* 141.3: 193-195, 1994.
[7] J. He and T. Kiesler, "Enhancing the security of El Gamal's signature scheme," *IEE Proceedings-Computers and Digital Techniques*, 141.4: 249-252, 1994.
[8] N. Y. Lee and T. Hwang, "Modified Harn signature scheme based on factorizing and discrete logarithms," *IEE Proceedings-Computers and Digital Techniques* 143.3:196-198, 1996.
[9] C. S. Laih and W. C. Kuo, "New signature schemes based on factoring and discrete logarithms," *IEICE TRANSACTIONS on Fundamentals of Electronics, Communications and Computer Sciences* 80.1: 46-53, 1997.
[10] Z. Shao, "Signature schemes based on factoring and discrete logarithms," *Computers and Digital Techniques, IEE Proceedings-*. Vol. 145. No. 1. IET, 1998.
[11] W. H. He, "Digital signature scheme based on factoring and discrete logarithms," *Electronics Letters* 37.4: 220-222, 2001.
[12] Z. Shao, "Digital signature schemes based on factoring and discrete logarithms," *Electronics Letters* 38.24: 1518-1519, 2002.
[13] S. F. Tzeng, C. Y. Yang, and M. S. Hwang, "A new digital signature scheme based on factoring and discrete logarithms," *International Journal of Computer Mathematics* 81.1: 9-14, 2004.
[14] S. Wei, "A New Digital Signature Scheme Based on Factoring and Discrete Logarithms," *Progress on Cryptography* : 107, 2004.
[15] E. S. Ismail, N. M. F. Tahat, and R. R. Ahmad, "A new digital signature scheme based on factoring and discrete logarithms," *Journal of Mathematics and Statistics* 4.4: 222, 2008.
[16] D. Poulakis, "A variant of digital signature algorithm," *Designs, codes and cryptography* 51.1: 99-104, 2009.
[17] L. Harn, "Enhancing the security of El Gamal's signature scheme," *Computers and Digital Techniques, IEE Proceedings-*. Vol. 142. No. 5. IET, 1995.
[18] N. Y. Lee and T. Hwang, "The security of He and Kiesler's signature schemes," *IEE Proceedings-Computers and Digital Techniques* 142.5: 370-372, 1995.
[19] J. Li and G. Xiao, "Remarks on new signature scheme based on two hard problems," *Electronics letters* 34.25: 2401, 1998.
[20] N. Y. Lee, "Security of Shao's signature schemes based on factoring and discrete logarithms," *IEE Proceedings-Computers and Digital Techniques*146.2: 119-121, 1999.
[21] M. S. Hwang, C. C. Yang, and S. F. Tzeng, "Improved digital signature scheme based on factoring and discrete logarithms," *Journal of Discrete Mathematical Sciences and Cryptography* 5.2: 151-155, 2002.
[22] C. T. Wang, C. H. Lin, and C. C. Chang, "Signature schemes based on two hard problems simultaneously," *Advanced Information Networking and Applications, 2003. AINA 2003. 17th International Conference on*. IEEE.
[23] Z. Shao, "Security of a new digital signature scheme based on factoring and discrete logarithms," *International Journal of Computer Mathematics* 82.10: 1215-1219, 2005.
[24] H. Qian, Z. Cao, and H. Bao, "Cryptanalysis of Li–Tzeng–Hwang's improved signature schemes based on factoring and discrete logarithms," *Applied mathematics and computation* 166.3: 501-505, 2005.
[25] S. Vishnoi and V. Shrivastava, "A new Digital Signature Algorithm based on Factorization and Discrete Logarithm problem," *International Journal of Computer Trends and Technology (IJCTT)* 3.4, 2012.