Step 1 V computes:

$$M' = y^{s+t} r g^{r} s^{-1}$$
$$= g^{x(s+t)} M s g^{-k} g^{r} s^{-1}$$
$$= g^{k-r} M g^{-k+r} (\mathrm{mod}\ p)$$

step 2 V checks whether $s = y^{M} \bmod p$.

If it holds, V is convinced that (r, s, t) is the signature generated by U of the recovered message.

The following section is aimed at finding forgery attack scheme to show the Chang et al:'s signature scheme is not secure.

3. One new Forgery Attacks Way on Chang et al:'s Signature Scheme

In this section, one new forgery attack is proposed to show that Chang et al.'s signature scheme is not secure and forged easily.

Assume A is an attacker and suppose that A already had a valid signature (r,s,t) generated by the legal signer U of the message M. Then, A can forge valid signature (r', s', t') as following forgery attack.

A Randomly chooses $r', a, b \in z_p^*$,

A Computes:

$$M = y^{a*b} r' g^{r'} \bmod p$$

$$s' = y^{M} \bmod p \quad t' = a*b - s' + M \bmod (p-1)$$

(r', s', t') is a forged signature of message M.

And (r', s', t') is a valid signature of message M, because:

$$M' = y^{s'+t'} r' g^{r'} (s')^{-1}$$
$$= y^{a*b} y^{M} r' g^{r'} y^{-M}$$
$$= y^{a*b} r' g^{r'}$$

Thus, $y^{M'} = y^{M} = s \bmod p$, (r', s', t') is a valid signature of message M.

4. Conclusion

One new forgery attack is proposed to show that Chang et al:'s signature scheme without using one-way hash function and message redundancy scheme is not as secure as thy claimed, and the signature can be forged on any uncontrolled messages easily. To overcome these attacks, how to set up a safe digital signature scheme without using hash functions and message redundancy is still a serious academic problem.

Acknowledgment

The work is supported by the by Scientific Research Fund of SiChuan Provincial Education Department(No:10SB095), National Statistical Research Program(No: 2012LY007), Annual Statistics Information Technology and Key Laboratory of Data Mining Program(No:SDL201207)

References

[1] Chang C C,Chang Y F(2004). Signing a digital signature without using one-way hash functions and message rudundancy schemes.IEEE Commun Lett, 8(8): 485-487.

[2] FU X T, XU C X, XIAO G Z(2004). Forgery attacks on Chang et al.'s signature scheme with message recovery. http://epring.iac.org.

[3] K. Nyberg, R.A(1995). Message Recovery for Signature Schemes Based on the Discrete Logarithm Problem, Proc. of Eurocrypt94.Springer-Verlag, LNCS 950, pp.182-193.

[4] S.P.Shih, C.-T. Lin, W.-B. Yang, H.-M. Sun.(2000). Digital multisignature schemes for authenticating delegates in mobile code systems. IEEE Trans. Veh. Technol, vol.49, pp. 1464-1473, July.

[5] S.-J. Hwang and E.-T. Li.(2003) Cryptanalysis of Shieh-Lin-Yang-Sun signature scheme. IEEE Commun. Lett, vol. 7, pp. 195-196, Apr.

[6] XuanHong,ChenKefei.(2009). Secure Multiple-Times Proxy Signature Scheme. Computer Standards and Interfaces, 31(2009), pp.19-23.

[7] Wang C T, Chang C C, Lin C H.(2000). Generalization of threshold signature an authenticated encryption for group communications. IEICE Transactions on Fundamentals, 2000, E83-A(6): 1228-1237.

[8] Kuo W-C, Chen M-Y(2005). A modified(t,n) threshold proxy signature scheme based on the RSA crypto-system. Information technology and applicatons, ICITA 2005, 2(4-7), 5769.

[9] Tan Z W, Liu Z J, Tang C M.(2003). A Proxy Blind Signature Schemes Based on DLP. Journal of Software,14(11): 1931-1935 (Ch).

[10] Zhang T, Wang Y M.(2004). Design of Several Partial Blind Signatures and the Security Analyse. Journal of Xidian University, 31(6): 963-966(Ch).

[11] Peng B,Yang Z K, Tan Y M.(2003). The Application of Blind Signature in E-Cash. Computer Engineering and Application,39(19): 31-33(Ch).

[12] Pointcheval D, Stem J.(2000). Security Arguments for Digital Signatures and Blind Signatures. Journal of Cryptology, 13(3):361-369.

[13] Long Yu, Li X-X, Chen K-F, Hongxuan.(2009). Distributed Certificateless Key Encapsulation Mechanism Secure Against the Adaptive Adversary. Journal of Shanghai Jiaotong University(Science). 14(1):102-106.

[14] Xiong H, Hua J, Chen Z, Li F(2011). On the security of an identity based multi-proxy signature scheme. Computer and Electrical Engineering, 37(2): 129-135.