View metadata, citation and similar papers at core.ac.uk
brought to you by CORE
provided by Elsevier - Publisher Connector

ELSEVIER
CrossMark
Available online at www.sciencedirect.com
ScienceDirect
Procedia Computer Science 32 (2014) 485 – 488
Procedia
Computer Science

5th International Conference on Ambient Systems, Networks and Technologies (ANT-2014)

Security Analysis of Liu-Zhang-Deng Digital Signature Scheme

Chenglian Liu

School of Mathematics and Computer Science, Longyan University, Longyan 364012, China.

Abstract

In 2010, Liu et al.[1] proposed an improvement of Liu-Li digital signature scheme without one-way hash function and message redundancy. In this paper, we demonstrate that Liu et al.'s scheme exist ℓ-wDH problem. Using Baby-Step Giant Step, we can compute $a \equiv x_i^{T_i-T_j} \pmod{p-1}$ in $O(\log p \cdot (\sqrt{q/d}))$ polynomial time, it is therefore insecure and can not against forgery attack.

© 2014 The Authors. Published by Elsevier B.V. Open access under CC BY-NC-ND license.
Selection and Peer-review under responsibility of the Program Chairs.

Keywords: ℓ-wDH problem; Algebraic structure defects; Forgery attack;

1. Introduction

In 2010, Liu et al.[1] enhanced the Shieh et al.[2] scheme and propose a new scheme without using one-way hash functions or message redundancy. They used dual public key y_1 and y_2 based on Liu-Li signature scheme[3] to protect their data. The secondary public key y_2 suppose upon on square root exponential of hard computation problem, it is easy to calculate the output value if known the input; otherwise, it is very hard to guess input value if known the output. In this article, we will point out the ℓ-wDH problem[4,5] in Liu et al.'s scheme, and state the vulnerability situation in their paper. Section 2 reviews Liu et al. scheme, Section 3 describes our methodology and security analysis. The conclusion draws in final section.

2. Review of Liu-Zhang-Deng Scheme

(Discrete Logarithm Problem, DLP)

Discrete Logarithm Problem DLP (p, g, y_i) is a problem that on input a prime p and integers $g, y_i \in \mathbb{Z}_p^*$, outputs $x_i \in \mathbb{Z}_{p-1}$ satisfying $g^{x_i} \equiv y_i \pmod{p}$ if such an x_i exists. Otherwise, it outputs $\perp$. The above function, which outputs $\perp$ if there is no solution to the query, should be expressed as DLP and the notation DLP should be used only for a weaker function such that nothing is specified for the behavior of the function in the case when there is no solution to

---

E-mail address: chenglian.liu@gmail.com

1877-0509 © 2014 The Authors. Published by Elsevier B.V. Open access under CC BY-NC-ND license.
Selection and Peer-review under responsibility of the Program Chairs.
doi:10.1016/j.procs.2014.05.451

the query. (Computational Square-Root Exponent, CSRE)
Computational Square-Root Exponent $CSRE(p, g, y_i)$ is a problem that on input a prime p and integers $g, y_i \in \mathbb{Z}_p^*$, outputs g^{x_i} (mod p) for $x_i \in \mathbb{Z}_{p-1}^*$ satisfying $y_i \equiv g^{x_i^2}$ (mod p) if such an x_i exists. Otherwise, it outputs $\perp$. According to the notation used in[6], the above function, which outputs $\perp$ if there is no solution to the query, should be expressed as CSRE. And the notation CSRE should be used only for a weaker function such that nothing is specified for the behavior of the function in the case when there is no solution to the query. However, since they evaluate only stronger problems, they omit asterisk throughout the paper for the sake of simplicity.

2.1. ***A. System Initial Phase:***

Let p be a large prime such as 1024 bits length, and $g \in \mathbb{Z}_p^*$ is a random multiplicative generator element. Signer U_i chooses his/her private key x_i, where $x_i \in [1, p-1]$, $gcd(x_i, p-1) = 1$ and computes the public keys

$$y_1 \equiv g^{x_i} \pmod{p}, \tag{1}$$

$$y_2 \equiv g^{x_i^2} \pmod{p}. \tag{2}$$

2.2. ***B. Signature Generation Phase:***

Step 1: U_i computes

$$s_i \equiv (y_2)^{m_i} \pmod{p} \tag{3}$$

Step 2: U_i randomly selects an integer $k_i \in [1, p-1]$ and computes

$$r_i \equiv (s_i + m_i \cdot y_1^{-k_i}) \pmod{p} \tag{4}$$

Step 3: U_i computes

$$t_i \equiv x_i^{-1} \cdot (k_i - r_i - x_i^{-1} \cdot s_i) \pmod{p-1} \tag{5}$$

Step 4: U_i sends the signature (s_i, r_i, t_i) of m_i to the verifier V.

2.3. ***C. Verification Phase:***

After receiving signature (s_i, r_i, t_i), the receiver V can check the signature and recover message m_i' as follows:

Step 1: V computes

$$m_i' \equiv y_2^{t_i} \cdot (r_i - s_i) \cdot y_1^{r_i} \cdot g^{s_i} \pmod{p} \tag{6}$$

Step 2: V checks whether

$$s_i \equiv (y_2)^{m_i} \pmod{p} \tag{7}$$

If it holds, V can be convinced that (s_i, r_i, t_i) is indeed the signature generated by U_i in the recovered message m_i'.

Proof.

$$\begin{aligned}
m_i' &\equiv y_2^{t_i} \cdot (r_i - s_i) \cdot y^{r_i} \cdot g^{s_i} \pmod{p} \\
&\equiv y_2^{x_i^{-1}(k_i - r_i - x_i^{-1} s_i)} \cdot (r_i - s_i) \cdot y_1^{r_i} \pmod{p} \\
&\equiv y_2^{x_i^{-1}k_i - x_i^{-1}r_i - x_i^{-1}s_i} \cdot m_i \cdot y_1^{-k_i} \cdot y_1^{r_i} \cdot g^{s_i} \pmod{p} \\
&\equiv y_1^{k_i} \cdot y_1^{-r_i} \cdot g^{-s} \cdot m_i \cdot y_1^{-k_i} \cdot y_1^{r_i} \cdot g^{s} \pmod{p} \\
&\equiv m_i \pmod{p}.
\end{aligned} \tag{8}$$

□

3. Our Methdology

Let G be an abelian group of prime order p and g a generator of G. The **Discrete Logarithm (DL) Problem** in G asks to find $a \in \mathbb{Z}_p$ given g and g^a in G. many cryptosystem are designed on the basis of the DL problem, but most of them have the security equivalent to a weaker variant of the DL problem rather than the DL problem itself. Two most important weaker variants are as follows:
The Computation Diffie-Hellman (CDH) Problem. Given (g, g^a, g^b), compute g^{ab}.
The Decisional Diffie-Hellman (DDH) Problem. Given (g, g^a, g^b, g^c), decide whether $c = ab$ in $\mathbb{Z}_p$.
Recently, some weakened variants of the CDH problem are introduced and being used to construct cryptosystems[7] for various functionalities or security without random oracles. One characteristic of these problems is to disclose $g, g^\alpha, \ldots, g^{\alpha^l}$ for the secret α and some integer l. The ℓ-weak Diffie-Hellman (ℓ-wDH) Problem. Given g and g^{α^i} in G for $i = 1, 2, \ldots, \ell$, computes $g^{1/\alpha}$. This problem was introduced by Mitsunari, Sakai, and Kasahara for traitor tracing scheme[8].

Theorem 1. *Let g be an element of prime order p in an abelian group. Suppose that d is a positive divisor of $p - 1$. If $g, g_1 := g^\alpha$ and $g_d := g^{\alpha^d}$ are given, α can be computed in $O(\log p \cdot (\sqrt{(p-1)/d} + \sqrt{d}))$ group operations using $O(max\{\sqrt{(p-1)/d}, \sqrt{d}\})$ memory.*

Proof. Note that $\mathbb{Z}_p^*$ is a cycle group with $\phi(p-1)$ generators, where $\phi(\cdot)$ is the Euler totient function. Since a random element in $\mathbb{Z}_p^*$ is a generator with probability $\frac{\phi(p-1)}{(p-1)} > \frac{1}{6 \log\log(p-1)}$, which is large enough, we can easily take a generator of $\mathbb{Z}_p^*$. Let ζ_0 be a generator of $\mathbb{Z}_p^*$. Then we can compute $\zeta = \zeta_0^d$ that is an element of order $(p-1)/d$ in $\mathbb{Z}_p^*$. Since $(\alpha^d)^{(p-1)/d} = 1$ and ζ generates all $(p-1)/d$-th roots of unity in $\mathbb{Z}_p^*$, there exists a non-negative i less than $(p-1)/d$ such that $\alpha^d = \zeta^i$. If we take $d_1 = \lceil \sqrt{(p-1)/d} \rceil$, we must have

$$(\alpha^d)\zeta^{-u} = \zeta^{d_1 v} \tag{9}$$

for some $0 \le u, v < d_1$. It is equivalent to

$$g_d^{\zeta^{-u}} = g^{\zeta^{d_1 v}}. \tag{10}$$

□

We compute and store the left-hand side terms and compare them with each of right-hand side terms in Baby-Step Giant-Step style. Note that each of terms in both side can be computed by repeated exponentiation by either ζ^{-1} or ζ^{d_1}. Thus we can find all-non-negative integers u and v less than d_1 satisfying equation (10) in $O(d_1 \cdot \log p)$ group operations using $O(d_1)$ memory. For u and v which satisfies equation (10) and $u + d_1 v$ is smallest, we put $k_0 = u + d_1 v$. Then k_0 is a non-negative integers less than $(p-1)/d$.
Let $\alpha = \zeta_0^k$ for $0 \le k \le p - 1$. Then we have $dk \equiv dk_0 \pmod{p-1}$ and so $k \equiv k_0 \pmod{p-1)/d}$. There exists a non-negative integer j less than d such that $k = k_0 + j(p-1)/d$. If we take $d_2 = \lceil \sqrt{d} \rceil$, we must have

$$\alpha\zeta_0^{-u'(p-1)/d} = \zeta_0^{k_0 + d_2 v'(p-1)/d} \tag{11}$$

for some $0 \le u', v' < d_2$. It is equivalent to

$$g_1^{\zeta_0^{-u'(p-1)/d}} = g^{\zeta_0^{k_0 + d_2 v'(p-1)/d}}. \tag{12}$$

Be the same method as above, we can find non-negative integers u' and v' less than d_2 satisfying equation (12) in $O(d_2 \cdot \log p)$ group operations and $O(d_2)$ memory. This completes the proof. If attacker known y_2 and T (it doesn't matter where T=2), but does not know password x_i. These are similar ℓ-wDH issue, for this category; it easily attack successful. The detail methodology is described as follow:

Step 1. Suppose $d = gcd(T, q), d_1 = \lceil \sqrt{q/d} \rceil, \zeta \in [1, p-1], 0 \le u, v \le d_1$,

$$(g^{x_i^T})^{\zeta^{-u}} \equiv g^{\zeta^{d_1 v}} \pmod{p}, \tag{13}$$

according to Baby-Step Giant-Step method to calculate the complexity $O((\log p) \cdot \sqrt{q/d})$ to get $a \equiv x_i^T \pmod{p-1}$. The detail described in previously. Computes

$$y_2^a \equiv (g^{x_i^T})^a \equiv g^{x_i^T x_i^T} \equiv g^{x_i^{2T}} \pmod{p}, \tag{14}$$

the attacker may fake a value T successful.

Step 2. $d = gcd(T_i - T_j, q)$ where $i \neq j$, because $g^{x_i^{T_i}} \equiv g^{x_i^{T_i - T_j} \cdot x_i^{T_j}} \equiv (g^{x_i^{T_j}})^{x_i^{T_i - T_j}} \equiv y_2^{x_i^{T_i - T_j}} \pmod{p}$, the complexity is $O((\log p) \cdot \sqrt{q/d})$, we could compute $a \equiv x_i^{T_i - T_j} \pmod{p-1}$. Thus, we can calculate the sub-exponential value T successful.

4. Conclusion

In Liu et al.'s scheme, they assume their public key y_2 on computational square-rot exponent, given a output value if there is no solution to the query; it is a hard problem in practical computation environment. In this paper, we showed a mathematical model that pointed out the Liu et al.'s scheme existed an algebraic structure defects, according to this vulnerability, it can not resist ℓ-wDH forgery attack. Therefore, the Liu et al.'s model is insecure.

Acknowledgment

The authors would like to thank the reviewers for their comments that help improve the manuscript. This research was partially supported by the National Natural Science Foundation of China under grant number 61103247. This research was also partially supported by the information security team project from Longyan University.

References

1. Liu, C., Zhang, J., Deng, S.. Security analysis of Liu-Li digital signature scheme. In: *Communication and Networking*; vol. 120 of *Communications in Computer and Information Science*. ISBN 978-3-642-17603-6; 2010, p. 63–70.
2. Shieh, S.P., Lin, C.T., Yang, W.B., Sun, H.M.. Digital multisignature schemes for authenticating delegates in mobile code systems. *IEEE Transactions on Vehicular Technology* 2000;**49**(4):1464–1473.
3. Liu, J., Li, J.. Cryptanalysis and improvement on a digital signature scheme without using one-way hash and message redundancy. In: *International Conference on Information Security and Assurance (ISA 2008)*. 2008, p. 266–269.
4. Cheon, J.. Security analysis of the strong diffie-hellman problem. In: Vaudenay, S., editor. *Advances in Cryptology - EUROCRYPT 2006*; vol. 4004 of *Lecture Notes in Computer Science*. Springer Berlin /Heidelberg; ????, p. 1–11.
5. Cheon, J.. Discrete logarithm problems with auxiliary inputs. *Journal of Cryptology* 2010;.
6. KONOMA, C., MAMBO, M., SHIZUYA, H.. Complexity analysis of the cryptographic primitive problems through square-root exponent. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences* 2004;**E87-A**(5):1083–1091.
7. Liu, C., Lin, C., Harn, L., Chen, S.. Weakness a remote password authentication schemes for multiserver architecture using neural networks. *Information-An International Interdisciplinary Journal* 2012;**15**(11B):4965–4970.
8. MITSUNARI, S., SAKAI, R., KASAHARA, M.. A new traitor tracing. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences* 2002;**E85-A**(2):481–484.