Cryptanalysis of a Digital Signature Scheme on ID-Based Key-Sharing Infrastructures

Hongjun Wu, Feng Bao, and Robert H. Deng

Kent Ridge Digital Labs
21 Heng Mui Keng Terrace, Singapore 119613
{hongjun,baofeng,deng}@krdl.org.sg

Abstract. At ISW'99, Nishioka, Hanaoka and Imai proposed a digital signature scheme on ID-based key-sharing infrastructures. That signature scheme is claimed to be secure if the discrete logarithm problem is hard to solve. Two schemes (the ID-type and the random-type schemes) based on the linear scheme for the Key Predistribution Systems (KPS) and the discrete logarithm problem (DLP) were given.

In this paper we show that those two schemes fail to meet the non-repudiation requirement: with negligible amount of computation, a signature could be forged. For the ID-type signature scheme, any verifier could forge a signature to raise repudiation between that verifier and the signer. The random type signature scheme has the same weakness. Furthermore, for the random-type signature scheme, once a signer issued a signature, anyone (not only the user in the scheme) could forge that signer's signature for a n arbitrary message.

1 Introduction

Digital signature plays an important role in authenticating digital documents. The commonly used digital signature schemes [5,11,13] are all belong to the public key cryptosystem (PKC). There is a kind of digital signature scheme that is based on the ID-Based cryptosystem [14] instead of on PKC. The first such digital signature scheme was proposed by Shamir [14]. Some other digital signature schemes [3,10,12] are based on the Key Predistribution Systems (KPS). The KPS is a kind of ID-based cryptosystem and it solves the key distribution problem with simple calculation [1,2,4,6,7,8,9].

Nishioka, Hanaoka and Imai recently proposed a new signature scheme [12] on the KPS infrastructure. This scheme is to satisfy the main signature requirements: authenticity, unforgeability, and non-repudiation [12]. Two examples were given and they are claimed to be secure if the discrete logarithm problem is hard to solve. As will be shown in this paper, those two examples are insecure: a signature could be easily forged with negligible amount of computation.

Nishioka, Hanaoka and Imai also claimed that if an ID-based key sharing system exists, an ID-based digital signature system could be easily implemented [12]. By breaking their proposed concrete signature schemes, it is shown that

K. Kim (Ed.): PKC 2001, LNCS 1992, pp. 173–179, 2001.

the implementation of secure ID-based digital signature system might not be as easy as claimed in [12].

This paper is organised as follows. Section 2 introduces the KPS and the linear KPS scheme. Section 3 introduces the KPS based signature scheme. The attacks against the ID-type signature scheme and the random-type signature scheme are given in Section 4 and Section 5, respectively. Section 6 concludes this paper.

2 KPS and the Linear KPS Scheme

2.1 KPS

The KPS Key Predistribution System [9] consists of one centre and a number of users. The KPS centre keeps in secret a bi-symmetric "center-algorithm" $G(\cdot,\cdot)$. The centre computes each user's secret algorithm as $X_i(\cdot) = G(ID_i, \cdot)$, where ID_i is the identifier of the user U_i and is publicly authenticated. The algorithm X_i is pre-distributed to the user U_i secretly and confidentially. The user U_i could establish a secret common key k_{ij} with the user U_j by computing $k_{ij} = X_i(ID_j)$ (the user U_j computes it as $X_j(ID_i)$).

2.2 The Linear KPS Scheme

The linear KPS scheme is one of the basic schemes of the KPS. In this scheme the symmetric centre algorithm is represented as 2nd degree covariant tensor G where each element $G_{ij} (i, j = 0, \cdots, m-1)$ is in $GF(q)$. A public function f transforms each ID into an m-dimension vector x on $GF(q)$ as $x_i = f(ID_i)$, where $x_i = (x_i^0, x_i^1, \cdots, x_i^{m-1})^T$. The user U_i's secret algorithm is an m-dimension vector X_i over $GF(q)$ and is generated as

$$X_i = G \cdot x_i$$

The common key k_{ij} established between U_i and U_j is computed by U_i as

$$k_{ij} = X_i^T \cdot x_j$$

or computed by U_j as

$$k_{ij} = X_j^T \cdot x_i$$

As long as the number of users is less than m, this linear KPS scheme is secure since no user(s) could recover the centre algorithm G.

3 The KPS-Based Signature Scheme

In [12], two examples based on the linear scheme for the KPS and the discrete logarithm problem (DLP) are given. These two signature schemes are introduced in this section. In the rest of this paper, H denotes an ideal hash function.

3.1 The ID-Type Scheme

Choose two sufficiently large primes p and q such that $p = 2q + 1$.

Signature Generation. The user U_i signs a message M as follows.

1. Compute $h = H(M||ID_i) \bmod p$
2. The signature S is an m-dimension vector on $GF(p)$ computed as $S = h^{X_i}$, i.e., $S_\ell = h^{X_i^\ell} \bmod p$ for $\ell = 0, 1, \cdots, m-1$.

Verification. The user U_j verifies the signature as follows:

1. Compute $V_1 = \prod_{\ell=0}^{m-1} (S_\ell)^{x_j^\ell} \bmod p$
2. Compute $V_2 = h^{k_{ij}} \bmod p$ where k_{ij} is the common key shared by U_i and U_j.
3. If $V_1 = V_2$ or $V_1 = V_2 \cdot h^q \bmod p$, the signature is accepted; otherwise, it is rejected.

Remarks. In the signature verification process,

$$\begin{aligned} V_1 &= \prod_{\ell=0}^{m-1} (S_\ell)^{x_j^\ell} \bmod p \\ &= h^{\sum_{\ell=0}^{m-1} X_i^\ell \cdot x_j^\ell \bmod p-1} \bmod p \\ &= \begin{cases} h^{k_{ij}} \bmod p & \text{if } \widetilde{k}_{ij} < q \\ h^{k_{ij}} \cdot h^q \bmod p & \text{otherwise} \end{cases} \end{aligned}$$

where $\widetilde{k}_{ij} = \sum_{\ell=0}^{m-1} X_i^\ell \cdot x_j^\ell \bmod p-1$. Thus for a signature generated by U_i, $V_1 = V_2$ or $V_1 = V_2 \cdot h^q \bmod p$.

3.2 The Random-Type Scheme

Choose two sufficiently large primes p and q satisfying $q|p-1$. Pick up g with order q on the multiplicative group $\mathbf{Z}_p^*$.

Signature Generation. The user U_i signs the message M as follows:

1. Generate m random numbers $z_\ell \in \mathbf{Z}_q$ $(\ell = 0, 1, \cdots, m-1)$.
2. Let $z = \sum_{\ell=0}^{m-1} z_\ell \bmod q$, and $r_\ell = g^{z_\ell} \bmod p$.
3. Compute $s_\ell = (H(M) \cdot z_\ell + X_i^\ell) \cdot z^{-1} \bmod q$.
4. The signature of the message M is given as (r_ℓ, s_ℓ) $(\ell = 0, 1, \cdots, m-1)$.

Verification. The user U_j verifies the signature as follows:

1. Let $s = \sum_{\ell=0}^{m-1} s_\ell \cdot x_j^\ell \bmod q$, and $r = \prod_{\ell=0}^{m-1} r_\ell^{x_j^\ell} \bmod p$.
2. Let $k_{ij} = \sum_{\ell=0}^{m-1} X_j^\ell \cdot x_i^\ell \bmod q$.
3. Compute $V_1 = r^{H(M)s^{-1}} \cdot g^{k_{ij} \cdot s^{-1}} \bmod p$.
4. Compute $V_2 = \prod_{\ell=0}^{m-1} r_\ell \bmod p$.
5. The user U_j accepts the signature only if $V_1 = V_2$.

Remarks. It is not difficult to verify that for a signature generated by U_i, $V_1 = V_2$.

4 Cryptanalysis of the ID-type Signature Scheme

In this section, we show that it is easy for a verifier to forge a signature. This signature could pass this verifier's verification process while it could not pass the verification processes of the other verifiers. However it is sufficient to cause repudiation between the signer and the verifier since the signer, on the other hand, can also forge such a signature to cheat that verifier.

Suppose now the signer is U_i and the verifier is U_j. With only the knowledge of k_{ij}, either the user U_i (signer) or U_j (verifier) could forge the signature as follows:

1. Compute $h = H(M||ID_i)$ and $V_2 = h^{k_{ij}} \bmod p$.
2. Solve for a_ℓ ($\ell = 0, 1, \cdots, m-1$) from the following equation:

$$V_2 = \prod_{\ell=0}^{m-1} h^{a_\ell \cdot x_j^\ell} \bmod p, \text{ or } V_2 \cdot h^q = \prod_{\ell=0}^{m-1} h^{a_\ell \cdot x_j^\ell} \bmod p$$

3. Let $S_\ell^{'} = h^{a_\ell} \bmod p$. $S_\ell^{'}$ ($\ell = 0, 1, \cdots, m-1$) are the forged signature.

In step 2, one of the equation is always solvable. And the amount of computation used in this attack is negligible. Thus either the verifier or signer could forge the signature easily.

The attack above deals with only one verifier. In the following, we consider the case in which all the verifiers are involved. All the verifiers may collude to forge a signature that could pass every verifier's verification. And the signer can also forge such a signature to cheat all the verifiers. Suppose there are n ($n < m$) users in the KPS scheme. The user U_0 is the signer and the users U_1 to U_{n-1} are the verifiers. In the KPS scheme, the signer has the knowledge of the common keys k_{0j} ($j = 1, 2, \cdots, n-1$). The colluded verifiers could also obtain the information of such common keys. The following attack shows how such a signature could be forged with the knowledge of the common keys k_{0j} ($j = 1, 2, \cdots, n-1$).

1. Compute $h = H(M||ID_0)$. Let $V_{2j} = h^{k_{0j}} \bmod p$ for $j = 1, 2, \cdots, n-1$.
2. Solve for a_ℓ ($\ell = 0, 1, \cdots, m-1$) from the following equations:

$$V_{2j} = \prod_{\ell=0}^{m-1} h^{a_\ell \cdot x_j^\ell} \bmod p, \text{ (or } V_{2j} \cdot h^q = \prod_{\ell=0}^{m-1} h^{a_\ell \cdot x_j^\ell} \bmod p) \; (j = 1, 2, \cdots, n-1)$$

3. Let $S_\ell^{'} = h^{a_\ell} \bmod p$. $S_\ell^{'}$ ($\ell = 0, 1, \cdots, m-1$) are the forged signature.

5 Cryptanalysis of the Random-Type Signature Scheme

The random-type signature scheme is more vulnerable than the ID-type scheme. In this scheme, every verifier could forge the signature. Furthermore, anyone (not only the users in the scheme) could forge a signer's signatures after that signer released a signature. In Subsection 5.1, we show how a verifier could forge a signature. In Subsection 5.2, we show how a signer's signature could be forged after one signature is issued.

5.1 A Verifier Could Forge the Signature

With the knowledge of the common key k_{ij}, either the user U_i (signer) or U_j (verifier) could forge the signature as follows:

1. Choose m random numbers b_i ($i = 0, 1, \cdots, m-1$) from $GF(q)$. Let $r_i = g^{b_i}$.
2. Let $r = \prod_{\ell=0}^{m-1} r_\ell^{x_j^\ell} \bmod p$, $v = \prod_{\ell=0}^{m-1} r_\ell \bmod p$.
3. Solve the following equation for s:

$$v = r^{H(M) \cdot s^{-1}} \cdot g^{k_{ij} \cdot s^{-1}} \bmod p$$

4. Choose m numbers s_ℓ ($\ell = 0, 1, \cdots, m-1$) to satisfy the following linear equation:

$$s = \sum_{\ell=0}^{m-1} s_\ell \cdot x_j^\ell \bmod q$$

5. (r_ℓ, s_ℓ) ($\ell = 0, 1, \cdots, m-1$) are the forged signature.

Remarks In step 3, the equation could be solved without dealing with the discrete log problem. The reason is that we only need to deal with the exponent since all the bases are the same (g). The amount of computation used in the attack is negligible.

5.2 Anyone Could Forge the Signature

After a signer issued a signature, his signatures could be forged by anyone (not only the user in the KPS scheme). Suppose that a user U_i has issued a signature S of message M. We show that anyone could forge the signature of an arbitrary message M' and to convince a verifier U_j that the signature is given by U_i. The attack is given as follows:

1. Recover $g^{k_{ij}}$ from the signature: from the verification process of signature, it is easy to compute the value of $g^{k_{ij}}$ from the signature and the publicly known information.
2. Let $g' = g^{k_{ij}}$.
3. Choose m random numbers b_i $(i = 0, 1, \cdots, m-1)$ from $GF(q)$. Let $r'_i = g'^{b_i}$.
4. Let $r' = \prod_{\ell=0}^{m-1} {r'}_{\ell}^{x_j^{\ell}} \bmod p$, $v' = \prod_{\ell=0}^{m-1} r'_{\ell} \bmod p$.
5. Solve the following equation for s':
$$v' = r'^{H(M')\cdot s'^{-1}} \cdot g'^{s'^{-1}} \bmod p$$
6. Choose m numbers s'_{ℓ} $(\ell = 0, 1, \cdots, m-1)$ to satisfy the following linear equation:
$$s' = \sum_{\ell=0}^{m-1} s'_{\ell} \cdot x_j^{\ell} \bmod q$$
7. (r'_{ℓ}, s'_{ℓ}) $(\ell = 0, 1, \cdots, m-1)$ are the forged signature.

Remarks In step 5, the equation could be solved easily since the bases are all the same (g'), and only the exponent need to be considered.

Conclusion==========================

6 Conclusions

In this paper, we showed that two recently proposed KPS-based signature schemes are not secure. The design of secure signature scheme based on KPS is still an open problem.

References

1. R. Blom, "Non-public Key Distribution", in *Advances in Cryptology–Crypto'82*, Plenum Press (1983), pp. 231-236.
2. C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro and M. Yung, "Perfectly Secure Key Distribution for Dynamic Conferences", in *Advances in Cryptology–Crypto'92*, LNCS 740, Springer-Verlag, pp.471-486, 1993.
3. Y. Desmedt and J. J. Quisquater, "Public-Key Systems Based on the Difficulty of Tampering (Is There a Difference Between DES and RSA?)", in *Advances in Cryptology Crypto'86*, LNCS 263, Springer-Verlag, pp. 111-117, 1986.

4. Y. Desmedt and V. Viswanathan, "Unconditionally Secure Dynamic Conference Key Distribution", IEEE, ISIT'98, 1998.
5. T. ElGamal. "A Public Key Cryptosystem and a Signature Scheme based on Discrete Logarithms". *IEEE Transactions on Information Theory*, **31** (1985), 469-472.
6. A. Fiat and M. Naor, "Broadcast Encryption", in *Advances in Cryptology–Crypto'93*, LNCS 773, Springer-Verlag, pp. 480-491, 1994.
7. L. Gong and D. J. Wheeler, "A Matrix Key-Distribution Scheme", *Journal of Cryptology*, vol. 2, pp. 51-59, Springer-Verlag (1993).
8. W. A. Jackson, K. M. Martin, and C. M. O'keefe, "Multisecret Threshold Schemes", in *Advances in Cryptology–Crypto'93*, LNCS773, Springer-Verlag, pp. 126-135, 1994.
9. T. Matsumoto and H. Imai, "On the Key Predistribution System: A Practical Solution to the Key Distribution Problem", in *Advances in Cryptology–Crypto'87*, LNCS 293, Springer-Verlag, pp.185-193, 1987.
10. T. Matsumoto and H. Imai, "Applying the Key Predistribution Systems to Electronic Mails and Signatures", in *Proc. of SITA'87*, pp. 101-106, 1987.
11. V. Miller, "Uses of Elliptic Curves in Cryptography", in *Advances in Cryptology–Crypto'85*, LNCS 218, Springer-Verlag, pp. 417-426, 1986.
12. T. Nishioka, G. Hanaoka, and H. Imai, "A New Digital Signature Scheme on ID-Based Key-sharing Infrastructures", in *Information Security–Proc. of ISW'99*, LNCS 1729, Springer-Verlag, pp. 259-270, 1999.
13. R. L. Rivest, A, Shamir, and L. Adleman, "A method for Obtaining Digital Signatures and Public-Key Cryptosystems", *Commun. ACM*, vol. 21, no. 2, pp. 158-164, Feb. 1978.
14. A. Shamir, "Identity-Based Cryptosystems and Signature Schemes", in *Advances in Cryptology–Crypto'84*, LNCS 196, Springer-Verlag, pp. 47-53, 1985.