VULNERABILITY OF A NON-MEMBERSHIP PROOF SCHEME

Kun Peng and Feng Bao
Institute for Infocomm Research, Connexis, Singapore

Keywords: Attack, Non-membership proof.

Abstract: An accumulator system used for a special application of anonymous credential is extended by Li *et al* to a much wider range of applications: membership proof and non-membership proof. Given a committed secret integer and a public finite set of prime integers, two proof protocols, membership proof and non-membership proof are proposed in the extended scheme. The former proves that the integer is in the set when it is really in, while the latter proves that the integer is not in the set when it is really not in. Although the original accumulator technique works well in its appointed special application, the extension is insecure and vulnerable to attacks. Several attacks against membership proof and non-membership proof in the extended work is proposed in this paper to show its vulnerability in security. The attacks show that an attacker can employ various methods to give membership proof to an integer not in the set and non-membership proof to an integer in the set.

1 INTRODUCTION

An accumulator system is designed in (Camenisch and Lysyanskaya, 2002) for application to anonymous credential. The original design is very efficient and achieves provable security in its special application. In (Li et al., 2007), the technique in (Camenisch and Lysyanskaya, 2002) is generalized and extended to solve a much more general question: membership proof and non-membership proof. Membership proof proves a secret committed integer is in a finite set, while non-membership proof proves a secret committed integer is not in a finite set. These two proofs have a much wider range of applications than the original special accumulator system in (Camenisch and Lysyanskaya, 2002) and are frequently used in various cryptographic applications.

In (Li et al., 2007) an accumulator is generated for the set, which stands for the integers in the set in a more brief form. For any integer in the set, a membership witness is generated, which can show membership of the integer when checked against the accumulator. When proving membership of an integer, a prover only needs to show knowledge of the membership witness in a zero knowledge proof. For any integer not in the set, a non-membership witness is generated, which can show non-membership of the integer when checked against the accumulator. When proving non-membership of an integer, a prover only needs to show knowledge of the non-membership witness in a zero knowledge proof.

As the original accumulator system (Camenisch and Lysyanskaya, 2002) works in a special application with strict limitations on parameter setting, participants' roles and application environment, the simple extension (Li et al., 2007) is too wide and not secure. In this paper, the extended work is demonstrated to be vulnerable to attacks against its soundness, where soundness of membership proof and non-membership proof are defined as follows.

Definition 1. *(Soundness of membership proof). If a committed integer is not in the set, the probability that the prover can pass the verification in the membership proof protocol is negligible.*

Definition 2. *(Soundness of non-membership proof). If a committed integer is in the set, the probability that the prover can pass the verification in the non-membership proof protocol is negligible.*

In this paper, firstly an attacking algorithm is proposed to employ Euclidean algorithm and the Chinese remainder theorem to extract a secret parameter called $\phi(n)$ in (Li et al., 2007). Then four attacks are designed, two to compromise soundness of membership proof in (Li et al., 2007) and two to compromise soundness of non-membership proof in (Li et al., 2007). The attacks show that even if a prover commits to an integer not in the set, he can still pass the membership proof with a non-negligible probability. Moreover, using the attacks, even if a prover com-

Peng K. and Bao F. (2010).
VULNERABILITY OF A NON-MEMBERSHIP PROOF SCHEME.
In *Proceedings of the International Conference on Security and Cryptography*, pages 419-422
DOI: 10.5220/0002912904190422

mits to an integer in the set, he can still pass the non-membership proof with a non-negligible probability.

It is demonstrated that membership proof and non-membership proof in (Li et al., 2007) are vulnerable to even more attacks. The main reason for vulnerability of the membership proof and non-membership proof in (Li et al., 2007) is that it bases a general and wide-range solution on a very special and strictly limited technique. Actually the technique in (Camenisch and Lysyanskaya, 2002) is not suitable for the general applications in (Li et al., 2007). The author of (Camenisch and Lysyanskaya, 2002) suggests that in general membership proof, the general-purpose technique in (Camenisch et al., 2008) should be used.

2 THE NON-MEMBERSHIP PROOF SCHEME IN (Li et al., 2007)

In (Li et al., 2007), a non-membership proof scheme is proposed, which shows non-membership of an integer using its non-membership witness. As we state before, besides non-membership witness it provides membership witness, so supports membership proof as well. Its design includes generation and update of accumulator, generation and update of membership witnesses and non-membership witnesses and the proof protocols to use them. Firstly, the important symbols used in (Li et al., 2007) are as follows.

- k is a system parameter and n is a composite of length k. $n = pq$, $p = 2p' + 1$, $q = 2q' + 1$, p and q have equal length and p, q, p', q' are all prime integers.
- Set G_f contains all the quadratic residues in Z_n. Integers g and h are in G_f such that $\log_g h$ is unknown to any prover to carry out membership proof or non-membership proof.
- X_k denotes all the primes in Z_{2^l} where $l = \lfloor k/2 \rfloor - 2$.
- The set X regarding which membership proof and non-membership proof are performed may be any subset of X_k. Namely, $X = \{x_1, x_2, \ldots, x_m\}$ where $x_i \in X_k$ for $i = 1, 2, \ldots, m$ and m is no more than the cardinality of X_k.
- n_1 is a special RSA modulus of length k_1.
- h_1 is a random value in QR_{n_1}, the subset containing all the quadratic residues in Z_{n_1}. g_1 is a random value in the group generated by h_1.
- A secret integer s is committed in $c_1 = g_1^s h_1^r \bmod n_1$ where r is randomly chosen form Z_{n_1}.

For each integer $x \in X$, there is a membership witness c_x such that $c_x^x = c \bmod n$ where c is a public integer called the accumulator value in (Camenisch and Lysyanskaya, 2002). To prove that the integer committed in c_1 is in X, a prover has to prove knowledge of secret integers x, r and c_x such that

$$c_1 = g_1^x h_1^r \bmod n_1 \quad (1)$$

$$c_x^x = c \bmod n \quad (2)$$

$$x \in Z_{2^l} \quad (3)$$

The accumulator value c is equal to $g^{\prod_{i=1}^m x_i} \bmod n$, which is public information once X is published. Different parties may have different methods to calculate c_x, which should be equal to $g^{\prod_{1 \le i \le m}^{x_i \neq x} x_i} \bmod n$. For example, once X is published, a prover can calculate $c_x = g^{\prod_{1 \le i \le m}^{x_i \neq x} x_i} \bmod n$.

For each integer $x \notin X$ but in X_k, there is a non-membership witness (a, d) such that $c^a = d^x g \bmod n$. To prove that the integer committed in c_1 is not in X, a prover has to prove knowledge of secret integers x, r, a and d such that

$$c_1 = g_1^x h_1^r \bmod n_1 \quad (4)$$

$$c^a = d^x g \bmod n \quad (5)$$

$$x \in Z_{2^l} \quad (6)$$

$$a \in Z_{2^l} \quad (7)$$

The method to generate a and d for x in (Li et al., 2007) is as follows where $u' = u \bmod \phi(n)$ and $u = \prod_{i=1}^m x_i$.

- If $gcd(x, u') = 1$, integers a and b are calculated such that $au' + bx = 1$, and $d = g^{-b} \bmod n$.
- If $gcd(x, u') \neq 1$, integers a and b are calculated such that $au + bx = 1$. Then $b' = b \bmod \phi(n)$ and $d = g^{-b'} \bmod n$.

3 ATTACKS TO COMPROMISE SOUNDNESS OF MEMBERSHIP PROOF AND NON-MEMBERSHIP PROOF

Firstly, an attacking algorithm is proposed to extract a multiple of $\phi(n)$. Then Four attacks are designed to compromise soundness of membership proof and non-membership proof in (Li et al., 2007). Finally, less important attacks easier to prevent are mentioned.

3.1 An Attacking Algorithm

With a non-negligible probability, an attacker can calculate a multiple of $\phi(n)$ in polynomial time using

some non-membership witnesses. Firstly, using the following attacking algorithm, the attacker can calculate the remainder of n modulo an integer when $gcd(x,u') = 1$.

1. If $gcd(x,u') = 1$, the non-membership witness for x is a and d such that
$$au' + bx = 1 \quad (8)$$
and $d = g^{-b} \bmod n$.
2. Obviously, $gcd(a,x) = 1$, otherwise $au' + bx$ cannot be 1 but will be a multiple of $gcd(a,x)$. So using Euclidean algorithm, the attack can calculate in polynomial time integers μ and β such that
$$a\mu + \beta x = 1. \quad (9)$$
3. (8)-(9) yields
$$a(u' - \mu) = x(\beta - b)$$
As $gcd(a,x) = 1$, x must be a factor of $u' - \mu$. Namely
$$u' = \mu \bmod x$$

The attacking algorithm shows that although b is not revealed in the non-membership witness Euclidean algorithm can be employed to calculate $u' \bmod x$ from a and x. Repeating the attacking algorithm using multiple different instances of x in X_k such that the product of the multiple instances of x is larger than $\phi(n)$, the attacker can calculate u' in polynomial time using the Chinese remainder theorem. Note that $u' = u \bmod \phi(n)$. So the prover obtains a multiple of $\phi(n)$ using polynomial calculation: $u - u'$. As n is a composite of length k, X_k denotes all the primes in Z_{2^l} where $l = \lfloor k/2 \rfloor - 2$ and $x, x_1, x_2, \ldots, x_m$ are chosen from X_k, with a non-negligible probability

- $u > \phi(n)$ and thus $u - u' \neq 0$;
- the product of a small number of integers in X_k is larger than $\phi(n)$ and thus a small number of non-membership witnesses are enough to apply the Chinese remainder theorem.

So, the an attacker can obtain a multiple of $\phi(n)$ in the from $u - u'$ using polynomial calculation with a non-negligible probability.

3.2 Four Concrete Attacks

With knowledge of a multiple of $\phi(n)$, various attacks can be launched. For example, a prover can commit to an integer not in X in c' but still pass the membership proof as follows.

Algorithm 1. *The first attack against membership proof.*

1. *The prover commits to* $x = u - u' + x_I$ *in* $g_1^x h_1^r \bmod n_1$ *where* $1 \leq I \leq m$ *and* r *is randomly chosen from* Z_{n_1}.
2. *The prover calculates* $c_x = g^{\prod_{i=1}^{I-1} x_i \prod_{i=I+1}^{m} x_i} \bmod n$.
3. *The prover proves his knowledge of* x, r *and* c_x *to satisfy (1), (2) and (3). As the order of* G_f *is* $\phi(n)/4$, $u - u'$ *is a multiple of the order of* g. *So*
$$c_x^x = (g^{\prod_{i=1}^{I-1} x_i \prod_{i=I+1}^{m} x_i})^{u-u'+x_I}$$
$$= g^{(\prod_{i=1}^{I-1} x_i)(u-u'+x_I)\prod_{i=I+1}^{m} x_i} = g^{(\prod_{i=1}^{I-1} x_i)x_I \prod_{i=I+1}^{m} x_i}$$
$$= g^{\prod_{i=1}^{m} x_i} = c \bmod n.$$
Therefore, the prover can successfully prove knowledge of secret integers $x = u - u' + x_I$, r *and* c_x *such that*
$$c_1 = g_1^x h_1^r \bmod n_1$$
$$c_x^x = c \bmod n.$$
As the probability that $x \in Z_{2^l}$ *is non-negligible in the given parameter setting, especially when* x_I *is the smallest integer in* X, *the probability that this attack can satisfy (1), (2) and (3) is non-negligible.*

As $u - u'$ is not a multiple of the order of g_1, $u - u' + x_I$ and x_I are completely different messages in the commitment algorithm, and so soundness of membership proof in (Li et al., 2007) is compromised. Similarly, a prover can commit to an integer chosen from X in c' but still pass the non-membership proof as follows.

Algorithm 2. *The first attack against non-membership proof.*

1. *The prover commits to* x_I *in* $g_1^x h_1^r \bmod n_1$ *where* $1 \leq I \leq m$ *and* r *is randomly chosen form* Z_{n_1}.
2. *The prover employs Euclidean algorithm to calculate integers* a *and* b *such that*
$$a(\prod_{i=1}^{I-1} x_i)(u - u' + x_I)\prod_{i=I+1}^{m} x_i + bx = 1.$$
As
$$gcd(x, (\prod_{i=1}^{I-1} x_i)(u - u' + x_I)\prod_{i=I+1}^{m} x_i)$$
$$= gcd(x_I, (\prod_{i=1}^{I-1} x_i)(u - u' + x_I)\prod_{i=I+1}^{m} x_i) = 1$$
except for a negligible probability, the prover can calculate a *and* b *to satisfy (10) except for a negligible probability. He then calculate* $d = g^{-b} \bmod n$.
3. *The prover proves his knowledge of* x, r, a *and* d *to satisfy (4), (5), (6) and (7). More precisely, he proves* x, r *and the integers he obtains,* a *and* d, *to satisfy*
$$c_1 = g_1^x h_1^r \bmod n_1$$
$$c^a = d^x g \bmod n$$

Note that

$$d^x g = (g^{-b})^x g = g^{1-bx} = g^{a(\prod_{i=1}^{I-1} x_i)(u-u'+x_I)\prod_{i=I+1}^{m} x_i}$$

As the order of G_f is $\phi(n)/4$, $u-u'$ is a multiple of the order of g. So (10) implies

$$d^x g = g^{a(\prod_{i=1}^{I-1} x_i)x_I \prod_{i=I+1}^{m} x_i} = (g^{\prod_{i=1}^{m} x_i})^a = c^a \bmod n.$$

So the prover can satisfy (4) and (5). Moreover, $x \in Z_{2^l}$ and as shown in (Li et al., 2007) with a non-negligible probability a calculated as above is in Z_{2^l}. So the prover can satisfy (4), (5), (6) and (7) with a non-negligible probability.

As $u-u'$ is not a multiple of the order of g_1, $u-u'+x_I$ and x_I are completely different messages in the commitment algorithm, and so soundness of non-membership proof in (Li et al., 2007) is compromised.

The two attacks above are not always successful, but only succeed with a non-negligible probability. Moreover, the attack against membership proof cannot work with any x in X_k but need to specially choose x as the sum of an integer in X and a multiple of $u-u'$. To overcome these two limitations, two more powerful attacks are proposed in the following, attacking membership proof and non-membership proof respectively.

Algorithm 3. *The second attack against membership proof.*

1. *A prover randomly chooses x in X_k but not in X and publishes $c_1 = g_1^x h_1^r \bmod n_1$ where r is randomly chosen form Z_{n_1}.*
2. *The prover calculates $z = x^{-1} \bmod u-u'$ and $c_x = c^z \bmod n$. Note that $gcd(x, u-u') = 1$ except for a negligible probability so c_x can be successfully calculated except for a negligible probability.*
3. *The prover proves his knowledge of x, r and c_x to satisfy (1), (2) and (3). As*

$$c_x^x = c^{zx} = c^{1+v(u-u')} \bmod n$$

where v is an integer and the order of c is $\phi(n)/4$, a factor of $u-u'$,

$$c_x^x = c \bmod n$$

is satisfied. As $x \in X_k \subset Z_{2^l}$, (1), (2) and (3) are satisfied. Namely, the attack is successful.

Algorithm 4. *The second attack against non-membership proof.*

1. *A prover randomly chooses x in X and publishes $c_1 = g_1^x h_1^r \bmod n_1$ where r is randomly chosen form Z_{n_1}.*
2. *The prover randomly chooses a in Z_{2^l} and calculates $z = x^{-1} \bmod u-u'$. Note that $gcd(x, u-u') = 1$ except for a negligible probability so z can be successfully calculated except for a negligible probability.*
3. *The prover calculates $d = (c^a/g)^z \bmod n$.*
4. *The prover proves his knowledge of x, r, a and d to satisfy (4), (5), (6) and (7). As*

$$d^x g = (c^a/g)^{xz} g = (c^a/g)^{1+v(u-u')} g \bmod n$$

where v is an integer and the order of c is $\phi(n)/4$, a factor of $u-u'$,

$$d^x g = c^a \bmod n$$

is satisfied. As $x \in X \subset Z_{2^l}$ and $a \in Z_{2^l}$, (4), (5), (6) and (7) are satisfied. Namely, the attack is successful.

The last two attacks compromise soundness of membership proof and non-membership proof respectively. They are more effective and harmful than the first two attacks.

4 CONCLUSIONS

The non-membership proof scheme in (Li et al., 2007) is insecure and vulnerable to various attacks. Its soundness is unreliable and its applications must be very cautious.

REFERENCES

Camenisch, J., Chaabouni, R., and Shelat, A. (2008). Efficient protocols for set membership and range proofs. In *ASIACRYPT '08, pages 234–252.*

Camenisch, J. and Lysyanskaya, A. (2002). Dynamic accumulators and application to efficient revocation of anonymous credentials. In *CRYPTO '02, pages 61–76.*

Li, J., Li, N., and Xue, R. (2007). Universal accumulators with efficient nonmembership proofs. In *ACNS '07, pages 253–269.*