Sungkyunkwan University

Department of Information Engineering
Information & Communications Security Laboratory

Technical Report
TR-98-2

On the security of cryptographic techniques based on D.L.P.

Soo hyun Oh, Seungjoo Kim and Dongho Won

Aug 1998
Limited distribution notes:

This report has been issued as a Research Report for early dissemination of its contents. In view of the transfer of copyright to the outside publisher its distribution outside Sungkyunkwan University prior to publication should be limited to peer communications and specific requests. After outside publication, requests should be filled only by reprints or legally obtained copies of the article.
On the security of cryptographic techniques based on D.L.P. 1)

Soohyun Oh, Seungjoo Kim, Dongho Won

Dept. of Information Engineering, Sungkyunkwan Univ.,
300 Chunchun-dong, Suwon, Kyunggi-do, 440-746, Korea
E-mail : (shoh, sjkim, dhwon}@dosan.skku.ac.kr

Abstract

Public-key cryptosystems are usually based on the NP-problems such as discrete logarithm problem, factorization problem, etc. Although these problems are known as computationally infeasible, no proofs have been made about their security. Therefore, in this paper, we will analyze the architecture of previous cryptosystems and their weaknesses, and show the criterion to design cryptosystems based on the discrete logarithm problem.

1 Introduction

Recently, with the rapid expansion of network, we are interested in information security more and more. And the best known technique of information security is a cryptography. Public-key cryptosystems are based on NP-problems such as discrete logarithm problem, factorization problem and so on. While these problems are known as computationally infeasible, no proofs have been made about the asymptotic lower bound on the complexity. Therefore, to design secure cryptosystem, we usually use the heuristic approach to the choice of public parameters of systems, etc. Generally, discrete logarithm problem is defined as follows:

Definition 1. Discrete Logarithm Problem (D.L.P.) is the following : given a prime \( p \), a generator \( a \) of \( \mathbb{Z}_p^* \) and an element \( \beta \in \mathbb{Z}_p^* \), find the integer \( x, 0 \leq x \leq p-2 \), such that \( a^x = \beta \mod p \).

In this paper, we analyze the security of public-key cryptosystems based on discrete logarithm problem and think about their countermeasures. The next section discusses about the algorithms computing the discrete logarithms. In section 3, we analyze the security of public parameters of systems and in section 4 we analyze the security of special digital signatures based on D.L.P..

2 The algorithms for the D.L.P.

The known algorithm for the DLP can be categorized as follows: (1) Algorithms which work in arbitrary groups (e.g., exhaustive search, the baby-step giant-step algorithm, Pollard's rho algorithm, Pollard's lambda algorithm). (2) Algorithms which work if the order of the group has only small factors (i.e., smooth) (e.g., Pohlig–Hellman algorithm). (3) Index-calculus algorithms which are efficient only in certain groups.

Firstly, Shanks' baby-step giant-step algorithm\[9\] is a time-memory trade-off of the exhaustive search method. For this, compute \( a^j (1 \leq j \leq \sqrt{\phi(p)}) \), store the ordered pair \((a^j, j)\) in table, and find \( i \) by exhaustive search. Then \( x = i \cdot \lfloor \sqrt{\phi(p)} \rfloor + j \) is the desired logarithm (see Fig. 1.).

\[ \beta = a^x \]

\[ x = i \cdot \lfloor \sqrt{\phi(p)} \rfloor + j \]

(\text{where, the order of } a \text{ is } p-1, 0 \leq i, j < \sqrt{\phi(p)})

\[ \beta \cdot (a^{(x-j)/i})^i = a^j \]

\[ \text{exhaustive search} \]

\[ \text{pre-computation} \]

\[ \text{Fig. 1. Shanks' method} \]

Pollard's rho method\[28\] is preferable to Shanks. Given \( a \) and \( \beta \), find the pair \((i, j)\) and \((k, l)\) such that \( a^i \cdot \beta^j = a^k \cdot \beta^l \) by using Floyd's cycle-finding algorithm. Then we can find the logarithm \( x \), since \( a^i = a^j \cdot a^{x-j} \), \( x = \log_a \beta = (i-k)/(j-l) \) (see Fig. 2.).

Also, if we know integers \( b \) and \( w \) such that \( b < x < b+w \), Pollard's lambda method\[28\] can be used. If \( i \) exceeds \( i\cdot w \) the algorithm is terminated with failure, since \( x = b+w-j-i \neq b \) (see Fig. 3.).

\[ \text{loop } \]
\[ ((i-i, +i), (i+k, +l)) : a^i \cdot \beta^j = a^k \cdot \beta^l \text{ (mod } p) \]
\[ \text{until } (i = l \mod \phi(p)) \]

where, \( * * \) : randomly increasing (by Floyd’s cycle-finding algorithm) function

\[ \text{Fig. 2. Pollard rho} \]

\[ \text{loop } \]
\[ ((i-i, +i), (i+i, +j)) : a^i \cdot \beta = a^j \cdot a^{b-w} \text{ (mod } p) \]
\[ \text{until } (i = j + w) \]

where, \( * * \) : randomly increasing function

\[ \text{Fig. 3. Pollard lambda} \]

Given the prime power factorization of \( \phi(p) \), Pohlig–Hellman decomposition\[27\] can be used to find the logarithm. The original discrete logarithm problem can be reduced to one of finding discrete logarithms \( x_i \) in a subgroup of order \( q_i \) (where, \( p = q_1 \cdot q_2 \cdots \cdot q_n + 1 \)), by the way of degenerating \( a \) to \( a^{\phi(p)/q_i} \). Once \( x_i \) is found for all \( i \), the Chinese Remainder Theorem allows solution of the desired log. \( x \) (see Fig. 4.).

\[ \text{ord}(a) = p-1 \rightarrow \text{ord}(a^{\phi(p)/q_i}) = q_i \]

\[ \text{C. R. T.} \]

\[ \text{Fig. 4. Pohlig–Hellman decomposition} \]
Finally, the *index-calculus algorithm*\(^{19}\) is the most powerful method known for computing discrete logarithms. The index-calculus algorithm requires the selection of a relatively small subset \(S\) of elements of the group \(G\), called the factor base, in such a way that a significant fraction of elements of \(G\) can be efficiently expressed as products of elements from \(S\). This method does not apply to all groups, but when it does, it often gives a subexponential-time algorithm (see Fig. 5).

\[
\text{collect & solve the linear system}
\]

\[
\text{factor base } S = (s_1, s_2, \ldots, s_n) \leftrightarrow (\log s_1, \log s_2, \ldots, \log s_n)
\]

\[
\beta = \Pi_s \leftrightarrow \text{compute } x
\]

Fig. 5. Index-calculus algorithm

3 The security of public parameters

Now, let’s consider the importance of the choice of public parameters (see Fig. 6.). If \(\varphi(p)\) has only small factors, then Pohlig–Hellman algorithm can be used to find the logarithm \(x\). To provide protection against Pohlig–Hellman decomposition, we can use *safe prime* \(p\), of the form \(p = 2 \cdot p' + 1\) where \(p'\) is also large prime. However finding safe primes introduces considerable expense.

So, for its efficiency and precluding Pohlig–Hellman attacks, we can use primes \(p\) of the form \(p = q \cdot w + 1\) with \(q\) large prime and \(w\) smooth — i.e., \(\varphi(p)\) has large prime factor \(q\). But van Oorschot and Wiener discovered that, if not use the generator of order \(q\), we can adopt Pohlig–Hellman decomposition to the smooth part, \(w\) of \(\varphi(p)\) by degenerating \(a\) to \(a^q\), so this is vulnerable to the middleperson attack.\(^{11}\)

While we use \(p = q \cdot w + 1\) and \(a\) of order \(q\), C.H. Lim and P.J. Lee demonstrated that many discrete logarithm protocols may be insecure against a key recovery attack unless relevant protocol variables are properly checked, that is, unless each party checks that received numbers belong to the underlying subgroup of prime order.\(^{18}\)

Not only the modulus \(p\) but also the generator \(a\) of the system must be chosen properly. Bleichenbacher showed that ElGamal signatures can be forged without knowing secret key when \(p = q \cdot w + 1\) (where \(q\) is a large prime and \(w\) is smooth) and \(\alpha \mid w\) (called “weak generator”).\(^{21}\)

Furthermore, Vaudenay presented that, if the authority can choose \(q\) to be the difference between \(\text{SHS}(m)\) and \(\text{SHS}(m')\) for two known messages \(m\) and \(m'\), these two messages will then have the same signature. Note that this kind of attack is avoided if \(m\) is hashed together with \(r\), as in the Schnorr signature.\(^{300}\)

Diffie and Hellman proposed a key exchange scheme based on the difficulty of solving general DLP, in 1976. They conjectured that breaking their scheme would be as hard as taking discrete logarithms. However, given a way to solve Diffie–Hellman problem (shortly, D.H.P.), there is no algorithm known that solves the discrete log problem.

Bert den Boer proved that there exists an algorithm to solve the DLP comprising of a (probabilistic) polynomial number of calls to an algorithm which solves the D.H.P (called a D.H. oracle) and a (probabilistic) polynomial number of “elementary” operations, for the case where \(\varphi(\varphi(p))\) is smooth. Furthermore, if this goes on for higher and higher totients we at last have proved
that either the general D.L.P. has a polynomial-time solution or there exists primes for which the D.H.P. is hard.\[^{[31]}\]

\[
p = \Pi q_i + 1 \\
\text{ord}(\alpha) = p - 1
\]

\[
p = 2p' + 1 \\
\text{ord}(\alpha) = p - 1
\]

\[
p = qw + 1 \\
\text{ord}(\alpha) = q
\]

\[\alpha \| w \]

\[r : r = (p-1)/\alpha \text{ (over } Z)\]

\[s : s = ((p-3)/2) \cdot (m - r \mod w) \mod p - 1\]

\[\beta_i \mod p\]

\[\text{ord}(\beta_i) < q\]

\[DSS(m) = DSS(m')\]

\[q = |SHS(m) - SHS(m')|\]

\[\text{Lim's key recovery attack}\]

\[\text{Obtain } f(\beta_i \mod p), \text{ where } \text{ord}(\beta_i) < q\]

\[\text{Recover } x \mod q\]

\[
\begin{array}{c}
\text{Fig. 6. The security of public parameters}
\end{array}
\]

4 The security of special digital signatures

A property of conventional digital signature schemes is that once a signature is released by the signer everybody can check its validity. But there are situations where this property (called “self-authentication”) is not desirable. In 1989 Chaum and van Antwerpen proposed the new type of digital signature, undeniable signatures, which cannot be verified without the consent of the signer.\[^{[32]}\]

A related notion is a convertible undeniable signatures, in which release of a single bit string by the signer turns all of his undeniable signatures into ordinary digital signatures.\[^{[4]}\] Also, in 1995, S.J. Kim, S.J. Park and D.H. Won proposed a nominative signatures, that is the dual signature scheme of undeniable signatures.\[^{[14][15][16]}\]

As shown in Fig. 7., undeniable signature schemes comprise of confirmation protocol, by which the signer can prove that a valid signature is indeed valid, and disavowal protocol, by which the signer can prove that a wrong signature is not valid.

However, a disadvantage of the confirmation protocol is that several verifiers not trusting each other are able to verify a signature simultaneously by secure mental game and divertible ZKIP. This attack was proposed by Desmedt and Yung,\[^{[10]}\] criticized by Chaum\[^{[8]}\] and later strengthened by Jakobsson (called “designated verifier proofs”).\[^{[13]}\] Also, since undeniable signatures rely on the signer cooperating in subsequent confirmations of the signature, if the signer should become available, then the recipient cannot make use of the signature. The concept of designated confirmer signatures was introduced by Chaum to solve this weakness of undeniable signatures.\[^{[6]}\] In designated confirmer signature schemes, if the signer is unavailable to confirm the signature, the
Furthermore, there are ways for the verifier to verify a signature not only by a confirmation protocol but also by a disavowal protocol (called "lie detector problem"). To overcome this weakness, Okamoto suggested non-transitive signature\(^{[25]}\). But, since Okamoto's scheme has no way to resolve a formal dispute, this is not a kind of signatures. So S.J. Park and D.H. Won proposed "entrusted undeniable signatures". Entrusted undeniable signatures are like undeniable signatures, except that the disavowal protocol can only be run by the court system.\(^{[26]}\) Also, M. Michels, H. Petersen and P. Horster pointed out that Boyar's ElGamal-like convertible undeniable signature scheme, which use only one authentically known parameter as base in the verification equation, can be forged universally if it is converted totally.\(^{[27]}\)

\* It is necessary that there are at least two authentication known parameters used as bases in the verification equation. In the conventional ElGamal-like signature schemes these are the generator and the public key of the signer.

**Fig. 7.** The security of special digital signatures

5 Conclusion

In this paper, we analyzed the security of public-key cryptosystem based on D.L.P. with respect to the algorithms computing the discrete logarithms, the security of public parameters of systems and the security of cryptographic protocol on D.L.P.. As mentioned above, to make a secure cryptosystem, we must pay attention to the choice of public parameters as well as the design of cryptographic protocol itself. Therefore we expect that this survey will give some guideline to the designing of secure cryptosystems.

References

1. R. Anderson and S. Vaudenay, “Minding your p’s and q’s”, In Advances in Cryptology -

3. B. den Boer, "Diffie-Hellman is as strong as discrete log for certain primes", In Advances in Cryptology - Crypto'88, LNCS, Springer-Verlag, 1988, pp.530-539


29. Bruce Schneier, "Applied Cryptography", WILEY.