Cryptanalysis of the Cryptosystem Based on DLP $\gamma = \alpha^a \beta^b$

Michal Sramka
Center for Cryptology and Information Security, Florida Atlantic University
777 Glades Road, Boca Raton, FL 33431, USA (Email: sramka@math.fau.edu)

(Received Jan. 18, 2006; revised and accepted Apr. 26, 2006)

Abstract

A critique of the proposed encryption scheme based on the DLP $\gamma = \alpha^a \beta^b$ is provided. It is described how a plaintext can be obtained from a valid ciphertext by computing a single traditional discrete logarithm in a cyclic group. Furthermore, it is shown that the proposed encryption scheme is in fact equivalent to the ElGamal encryption scheme.

Keywords: Cryptanalysis, DLP, ElGamal

1 Introduction

In 2006, Sunil Kumar Kashyap, Birendra Kumar Sharma, and Amitabh Banerjee proposed [4] a discrete logarithm problem in cyclic groups based on two generators and a public-key encryption scheme based on this discrete logarithm problem. In the proposal, the authors claim that it is necessary to compute two traditional discrete logarithms to solve their discrete logarithm.

This contribution shows that the proposed asymmetric cryptosystem - an encryption scheme which is a modification of the ElGamal encryption scheme - can be in fact broken by computing a single traditional discrete logarithm. In addition, a careful analysis of the ciphertext allows for selection and computation of particular values that render the proposed encryption scheme equivalent to the ElGamal encryption scheme.

1.1 The Traditional DLP and the ElGamal Encryption Scheme

Let G be a finite cyclic multiplicatively written group of order n, α a generator of this group, and β any group element. The traditional [1] *discrete logarithm problem* (DLP) is defined to be the problem of finding a $(0 \leq a < n)$ such that $\alpha^a = \beta$.

The complexity of the DLP is based on the group representation. For example, the DLP in cyclic additive group $\mathbb{Z}_n$ of order n is of polynomial complexity. The groups that have a "hard" DLP and are commonly used [3, 5] are:

- a (prime order) subgroup of $\mathbb{Z}_p^*$, where p is a prime, and
- a (prime order) subgroup of the group of points on an elliptic curve over a finite field.

The first encryption scheme that takes an advantage of this DLP was the *ElGamal encryption scheme* [2]. A brief description follows:

Key generation: Let G be a finite cyclic multiplicatively written group of order n. Let α be a generator of G. Choose a random integer a $(0 \leq a < n)$ and set $\beta := \alpha^a$. The private key is a, the public key consists of G, α, and β.

Encryption: To encrypt a message $x \in G$, one randomly chooses integer k $(0 \leq k < n)$ and computes the ciphertext (y_1, y_2), where $y_1 := \alpha^k$ and $y_2 := x\beta^k$.

Decryption: To decrypt a ciphertext (y_1, y_2), one computes $y_1^{-a} y_2$ in order to obtain the plaintext.

2 The Proposed DLP $\gamma = \alpha^a \beta^b$ in Cyclic Groups

In 2006, Sunil Kumar Kashyap, Birendra Kumar Sharma, and Amitabh Banerjee proposed [4] a discrete logarithms problem in cyclic groups based on two generators and an encryption scheme based on this discrete logarithm problem.

They [4] define the *discrete logarithm with two different exponentiations and two distinct integers* (2DL) to be $\gamma = \alpha^a \beta^b$ in a finite cyclic group G of order n, such that $\alpha \neq \beta^i$ and $a \neq b^i$, where α and β are two distinct generators of G, $\gamma \in G$, and a, b are two distinct integers to be determined. In other words, the 2DL problem is: given two distinct generators α and β of G and $\gamma \in G$, determine integers a and b such that $\gamma = \alpha^a \beta^b$.

Based on this 2DL problem in a group $G = \mathbb{Z}_p^*$, where p is a prime, Kashyap, Sharma, and Banerjee proposed a public-key encryption scheme [4]. The scheme is a modification of the original ElGamal encryption scheme. A description follows:

Key generation: Let α and β be two distinct generators of the multiplicatively written group $\mathbb{Z}_p^*$ of the integers modulo prime p such that $\alpha \not\equiv \beta^i \pmod{p}$. Select two random integers a and b such that $a \neq b^i$ and $0 \leq a, b < p-1$. Compute $\gamma := \alpha^a$ and $\delta := \beta^b$, all computations modulo p. The public key is p, α, β, γ, and δ. The private key is a and b.

Encryption: To encrypt a message $x \in \mathbb{Z}_p^*$, one randomly chooses an integer k with $0 \leq k < p-1$ and computes the ciphertext (y_1, y_2, y_3), where $y_1 := \alpha^k$, $y_2 := \beta^k$, and $y_3 := x\gamma^k\delta^k$ (again, all computations modulo p).

Decryption: To decrypt a ciphertext (y_1, y_2, y_3), one obtains the corresponding plaintext by computing $y_1^{-a} y_2^{-b} y_3 \bmod p$.

3 Critique and Cryptanalysis

The authors claim [4] that their 2DL problem involves two traditional DLPs. This is however not true. We now describe an attack against the proposed encryption scheme that needs only one solution of the traditional DLP. Note, that the attack is described for an abstract multiplicatively written cyclic group G, since it holds in general setting, not just for the group $\mathbb{Z}_p^*$ and its subgroups.

Suppose an attacker has a ciphertext (y_1, y_2, y_3). Then from the definition of the encryption we have

$$y_1 y_2 = \alpha^k \beta^k = (\alpha\beta)^k,$$

therefore we can obtain the integer k as a single traditional DLP of $y_1 y_2$ to the base $\alpha\beta$. Having k, we can then easily proceed to recover the plaintext message as $\gamma^{-k}\delta^{-k} y_3$ since γ and δ are public.

Moreover, the condition $\alpha \neq \beta^i$ of the 2DL problem and of the proposed encryption scheme cannot be satisfied in any cyclic group. Since α is a generator of the finite cyclic group, every element can be expressed as some power of α, say $\beta = \alpha^m$. Therefore the 2DL problem $\gamma\delta = \alpha^a\beta^b$ can be always rewritten as

$$\gamma\delta = \alpha^a\beta^b = \alpha^a(\alpha^m)^b = \alpha^{a+mb}. \quad (1)$$

In particular, we show that the proposed encryption scheme described in the previous chapter is equivalent to the ElGamal encryption scheme.

We show this by reduction: Using the notation from above, consider the ciphertext pair (y_1, y_3). We have $y_1 = \alpha^k$ and

$$\begin{aligned} y_3 &= x\gamma^k\delta^k = x(\alpha^a)^k(\beta^b)^k = x(\alpha^a)^k((\alpha^m)^b)^k \\ &= x\alpha^{ak+mbk} = x(\alpha^t)^k, \end{aligned}$$

for some integer t. In reality, $t := a+mb$. Hence (y_1, y_3) is exactly the definition of ElGamal encryption of the message x using random integer k, private key t, and the public key α and α^t.

Note, that even without knowing m, we can obtain t as a traditional single discrete logarithm of $\gamma\delta$ to the base α as shown in the Equation (1). In addition, the obtained knowledge of t leads to decryption of every other ciphertext.

In other words, this argument shows that the proposed encryption scheme has the same security as the original ElGamal encryption scheme. Hence the known problems, vulnerabilities, and attacks that are valid for ElGamal encryption scheme are valid for the new scheme, too.

4 Conclusion

The idea of extending the traditional discrete logarithm problem to two (or more) generators in highly interesting. However, the cryptanalysis of the proposed encryption scheme described here shows that the scheme is not superior to the ElGamal encryption scheme. The proposed encryption scheme requires more computations than the ElGamal encryption scheme while maintaining the same security and this effectively renders it obsolete.

References

[1] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, pp. 644-654, 1976.

[2] T. ElGamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," *IEEE Transactions on Information Theory*, vol. 31, pp. 469-472, 1985.

[3] Institute of Electrical and Electronics Engineers, *P1363: Standard Specifications for Public Key Cryptography*, 1999.

[4] S. K. Kashyap, B. K. Sharma and A. Banerjee, "A Cryptosystem Based on DLP $\gamma \equiv \alpha^a\beta^b \bmod p$," *International Journal of Network Security*, vol. 3, no. 1, pp. 95-100, 2006.

[5] U.S. Department of Commerce, National Institute of Standards and Technology, *FIPS PUB 186-2: Digital Signature Standard*, Jan. 2000. (http://csrc.nist.gov/publications/fips/fips 186-2/fips186-2-change1.pdf)

Michal Sramka received his Ph.D. degree from Slovak University of Technology in Bratislava, Slovakia. Currently he is a research assistant at Center for Cryptology and Information Security at Florida Atlantic University. His research interests are in cryptography and cryptanalysis, including related mathematics and engineering issues.