仲恺农业工程学院学报,22(3):33~35,2009
Journal of Zhongkai University of Agriculture and Engineering
文章编号:1674-5663(2009)03-0033-03

ElGamal 算法安全性分析

刘 佳,陈 勇,谢芳清,杜淑琴
(仲恺农业工程学院 计算机科学与工程学院,广东 广州 510225)

摘要:利用 Alice 和一个预言机之间进行的合理交互,通过把明文的二次剩余特性与对应的密文联系起来,详尽论证了 ElGamal 密码算法在自适应选择明文攻击下的不安全性,同时给出改进型 ElGamal 算法在自适应选择明文攻击下的形式化安全性证明.

关键词:公钥密码;ElGamal;选择明文攻击
中图分类号:TP309.7 **文献标识码**:A

ElGamal algorithm security analysis

LIU Jia, CHEN Yong, XIE Fang-qing, Du Shu-qing
(College of Computer Science and Engineering, Zhongkai University of Agriculture and Engineering, Guangzhou 510225, China)

Abstract: Using the construction of reasonable interaction between Alice and a random oracle, ElGamal was claimed to be not an security algorithm by analysis on the correlative relation in plaintext's quadratic residue and its cipher-text. The modification of ElGamal algorithm was analyzed as well, in which the security against adaptive chosen-plaintext attack was given.

Key words: public-key cryptography; ElGamal; adaptive chosen-plaintext attack

1 前言

公钥密码体制设计有两个重要的原则[1]:其一是要求在加密算法和公钥都公开的前提下,其加密的密文必须是安全的;其次是要求所有加密者和解密者计算或处理都应比较简单,但对其他不掌握秘密密钥的人,破译应是极困难的.

由于 RSA 和 Rabin 算法是确定性算法,无法抵抗选择明文攻击,ElGamal 算法[2]加密时可以随机选择整数 k,因此可以抵抗选择明文攻击,但还是存在安全问题. Mao[3]提出利用二次剩余性对 ElGamal 算法进行选择明文攻击. 作者更详尽地模拟了整个攻击过程,同时利用可证明安全理论给出了改进型 ElGamal 算法[2]在自适应选择明文攻击下的安全性分析.

2 ElGamal 算法理论基础

ElGamal 密码体制是单向陷门函数的一个成功应用,把函数转化为公钥加密体制[2]. ElGamal 密码体制的原型如下:

发送者向接收者发送消息 m,他需利用接收者的公钥加密消息 m,生成密文并发送给接收者,接收者收到发送者的密文后,利用自己的私钥解密.

(1) 创建密钥

收稿日期:2009-04-01
基金项目:仲恺农业工程学院校级科研基金(G3081804)资助项目.
作者简介:刘佳(1983-),女,吉林梅河口人,助教,硕士. E-mail:liujia_1116@163.com

①随机生成一个比较大的素数 p；

②生成一个模 p 的整数乘法群：$Z_p^* = \{1, 2, 3\cdots\cdots p-1\}$，计算生成元 g，且 $g<p$，g^0，g^1，…，g^{p-2}分别模 p 得到 $p-1$ 个不同的结果；

③随机选择 $x \in {}_uZ_{p-1}$作为接收者的私钥；计算接收者的公钥 $y \equiv g^x \pmod p$；

④（p，g，y）作为公开密钥公开，把 x 作为接收者的私钥保存.

（2）加密过程

如果发送者要把消息 $m<p$ 秘密地发送给接收者，首先选取 $k \in {}_uZ_{P-1}$，利用接收者的公钥（p，g，y）生成密文对（c_1，c_2），其中 $c_1 \equiv g^k \pmod p$，$c_2 \equiv y^k m \pmod p$. 传输密文对（c_1，c_2）给接收者.

（3）解密过程

为了解密密文对（c_1，c_2），接收者只需要利用其私钥计算 $m \equiv c_2/c_1^x \pmod p$.

基于离散对数的性质，仅知道公钥（p，g，y）和消息对（c_1，c_2）要得到 m 是极其困难的. 只有拥有私钥才能得到消息 m，因此别人没有办法进行解密，达到秘密传送消息的目的.

3 ElGamal 算法的选择明文攻击方案

由于 ElGamal 体制不能隐藏明文的二次剩余特性，因此它在不可区分性选择明文攻击（Indistinguishability under Chosen Plaintext Attack，IND-CPA）下是不安全的. 在该算法中，设定公开参数（g，p），g 是整数乘法群 Z_p^* 的生成元. 在这种参数背景下，明文的二次剩余特性可以与对应的密文联系起来.

假设随机预言机 O 为 ElGamal 体制建立了（p，g，y）作为公钥材料，则由欧拉准则[3]，$g \in QNR_P$（即 g 是一个模 p 的非二次剩余）. 假设 Alice 是一个 IND-CPA 攻击者，他可以提交一条消息 $m_0 \in QR_P$，另一条消息 $m_1 \in QNR_P$. 设（c_1^*，c_2^*）是从 O 返回的密文对，则有

$$\begin{cases} c_1^* = g^k \pmod p, \\ c_2^* = \begin{cases} y^k m_0 \pmod p & 50\% \text{ 的概率}, \\ y^k m_1 \pmod p & 50\% \text{ 的概率}. \end{cases} \end{cases}$$

因为 g 是 Z_P^* 的生成元，因此 $g^{p-1} \equiv 1 \pmod p$，根据欧拉准则[3]，如果 $g \in QR_P$，即 $g^{(p-1)/2} \equiv 1 \pmod p$ 与生成元的性质矛盾，因此 $g \in QNR_P$.

Alice 可以通过判定 y、c_1^*、c_2^* 的二次剩余特性，明确指出被加密的明文. 首先考虑 $y \in QR_P$ 的情况，容易得到：$y^k \in QR_P$，$m_0 \in QR_P$，$m_1 \in QNR_P$，因此当 $c_2^* \in QR_P$ 时，被加密明文是 m_0，当 $c_2^* \in QNR_P$ 时，被加密明文是 m_1；对于 $y \in QNR_P$ 的情况，需要分析 c_1^*，当 $c_1^* \in QR_P$ 时，由于 $g \in QNR_P$，因此 k 一定是偶数，即 $y^k \in QR_P$，由 $m_0 \in QR_P$，$m_1 \in QNR_P$，因此当 $c_2^* \in QR_P$ 时，被加密明文是 m_0，当 $c_2^* \in QNR_P$ 时，被加密明文是 m_1；当 $c_1^* \in QNR_P$ 时，k 一定是奇数，因此 $y^k \in QNR_P$，即 $(\frac{y^k}{p}) = -1$，由 $m_0 \in QR_P$，$m_1 \in QNR_P$，可以得到，$(\frac{m_0}{p}) = 1$，$(\frac{m_1}{p}) = -1$，因此当 $c_2^* \in QR_P$ 时，即只有是 $(-1) \times (-1) = 1$ 这种情况，所以被加密明文是 m_1；当 $c_2^* \in QNR_P$ 时，即是 $(-1) \times (-1) = -1$ 这种情况，因此被加密明文是 m_0.

总结如下：

$$\begin{cases} y \in QR_P \begin{cases} m_0 \text{ 是被加密明文} & \text{当 } c_2^* \in QR_P, \\ m_1 \text{ 是被加密明文} & \text{当 } c_2^* \in QNR_P, \end{cases} \\ y \in QNR_P \begin{cases} c_1^* \in QR_P \begin{cases} m_0 \text{ 是被加密明文} & \text{当 } c_2^* \in QR_P, \\ m_1 \text{ 是被加密明文} & \text{当 } c_2^* \in QNR_P, \end{cases} \\ c_1^* \in QNR_P \begin{cases} m_0 \text{ 是被加密明文} & \text{当 } c_2^* \in QNR_P, \\ m_1 \text{ 是被加密明文} & \text{当 } c_2^* \in QR_P. \end{cases} \end{cases} \end{cases}$$

4　ElGamal改进型算法及安全性证明

ElGamal的语义攻击利用了明文的二次剩余特性，如果限制该密码体制只工作在QR_p中，那么ElGamal的语义攻击就不会成功了．下面是对ElGamal体制的一种修改[2]．

假设G是一个阿尔贝群，其描述如下：

(1) 找一个随机素数q，$|q|=k$；检测$p=2q+1$的素性，如果p不是素数，则返回；

(2) 选择一个随机生成元$h\in Z_p^*$；令$g=h^2 \pmod p$；

(3) 由g生成群G；

(4) (p, g)是ElGamal体制的公开参数；

(5) G是其明文消息空间．

由于$g=h^2(\bmod p)$，因此$g\in QR_p$，由g生成的群G的元素都是模p的二次剩余，并且G作为明文空间，Alice所选择的明文只可能是$m_0\in QR_p$，$m_1\in QR_p$，因此O产生的询问密文也一定是模p的二次剩余．从而，ElGamal的二次剩余语义攻击将不再成功．

改进后的ElGamal在IND-CPA下是安全的，具体证明如下：

定理1：假设判决性Diffie Hellman问题（Decisional Diffie Hellman Problem，DDHP）是困难的，则改进型ElGamal算法在自适应选择明文攻击下是安全的．

证明：等价地证明逆否命题“若改进型ElGamal算法在自适应选择明文攻击下是不安全的，则DDHP可求解．”

假设改进型ElGamal算法在自适应选择明文攻击下是安全的，即存在Adversary能以大于二分之一的概率猜测已知密文所对应的明文，则Simulator能以不可忽略的概率对DDHP求解．

(1) Adversary选择两个消息m_0，$m_1\in QR_p$并发送给Simulator；

(2) Simulator随机选择$b\in\{0,1\}$，构造$(c_1^*=g^k,\ c_2^*=m_b y^k)$，并发送密文对$(c_1^*,\ c_2^*)$给Adversary；

(3) Adversary发送$b'\in\{0,1\}$给Simulator，若Adversary能以大于二分之一的概率猜测已知密文对$(c_1^*,\ c_2^*)$所对应的明文，即$prb[b=b']>\frac{1}{2}+\frac{1}{p(n)}$，其中$\frac{1}{p(n)}$是可忽略的，则Simulator以不可忽略的概率通过计算$y^k=\frac{c_2^*}{m_b}$可以验证三元组$(g^k,\ g^*,\ \frac{c_2^*}{m_b})$的关系，即给出了DDHP的求解．

由于DDHP求解是困难性问题，因此假设不成立，即改进型ElGamal算法在自适应选择明文攻击下是安全的．

5　结束语

本文在文献[3]的基础上详尽分析了ElGamal密码算法在自适应选择明文攻击是不安全性，同时利用“DDHP是困难的，则改进型ElGamal算法在IND-CPA下是安全的”，给出了改进型ElGamal算法的形式化安全证明，证明改进型ElGamal算法在自适应选择明文攻击下是安全的，为安全应用算法提供了理论依据．

参考文献：

[1] DIFFIE W, HELLMAN M. New directions in cryptography[J]. IEEE Transactions on Information Theory, 1976, 22(6): 644-654.

[2] ELGAMAL T. A public key cryptosystem and a signature scheme based on the discrete logarithm[J]. IEEE Transactions on Information Theory, 1985, 31(4): 469-472.

[3] MAO W B. 现代密码学：理论与实践[M]. 王继林，等译. 北京：电子工业出版社，2004.

【责任编辑　夏成锋】