基于证书的抗泄漏的安全加密方案*

于启红[1]，李继国[2]
（1. 宿迁学院 计算机科学系，江苏 宿迁 223800；2. 河海大学 计算机与信息学院，南京 210098）

摘 要：近期实践表明密码系统容易受到各种攻击而泄漏密钥等相关秘密信息，泄漏的秘密信息破坏了以前的已证明安全的方案，因此设计抗泄漏的密码学方案是当前密码研究领域的一个热点研究方向。设计一个基于证书的加密方案，总的设计思想是使用一个基于证书的哈希证明系统，这个证明系统包含一个密钥封装算法，用这个密钥封装算法结合一个提取器去加密一个对称加密所用的密钥，那么得到的加密方案就是可以抵抗熵泄漏并且是安全的。对方案的安全性分析和抗泄漏性能分析，表明本方案在抵抗一定量的密钥泄漏和熵泄漏时可以保持安全性。

关键词：熵泄漏；密钥泄漏；基于证书加密；提取器
中图分类号：TP309 **文献标志码**：A **文章编号**：1001-3695(2014)01-0210-03
doi:10.3969/j.issn.1001-3695.2014.01.049

Secure certificate-based encryption against entropy and key leakage

YU Qi-hong[1], LI Ji-guo[2]
(1. *Dept. of Computer Science, Suqian College, Suqian Jiangsu* 223800, *China*; 2. *College of Computer & Information Engineering, Hehai University, Nanjing* 210098, *China*)

Abstract: Some attacks which can get some key information from the cryptosystem break the security of the entire cryptosystem. How to design secure cryptosystems is getting more and more attention of the researchers in cryptography community. The paper presented an encryption scheme which was based on certificate-based encryption. It designed a certificate-based hash proof system which contained a key encapsulation algorithm. Then it used this key encapsulation algorithm which was combined with an extractor to encrypt a symmetric encryption key. The scheme was resilient to entropy and secret key leakage. It slso gare the proof of security and analysis of the capability resilient to entropy and secret key leakage.

Key words: entropy leakage; key leakage; certificate-based encryption; extractor

0 引 言

传统的密码系统设计是以密钥的绝对保密为前提的，并且在没有考虑密钥泄漏的情况下，设计了很多可以证明安全的密码系统。但事实并非如此，从 1996 年时序攻击被提出以来，密码系统就逐渐被发现遭受诸如边信道攻击（故障分析[1,2]、电磁分析[3]、时序攻击[4]等）和冷启动攻击[5]等多种攻击。在这些攻击中攻击者可以通过各种手段获得密码系统的相关信息，甚至是最关键的密钥信息，因此就破坏了原来设计的系统的安全性。

自从 1999 年 Chari 等人在文献[6]中提出第一个从算法模型角度来设计抗泄漏的密码系统之后，密码学领域掀起了一股针对能抵抗信息泄漏的密码学原语的研究热潮，尤其最近几年，对抗泄漏方案研究取得一定的进展，如抗泄漏的加密方案[7~10]，抗泄漏签名方案[11,12]等。但这些方案要么没有考虑到密钥泄漏情况，要么没有考虑到熵泄漏情况。另外，笔者所知目前还没有基于证书的抗泄漏的密码方案。

本文提出了一种基于证书加密[13]的抗泄漏的加密方案，设计的方案可以有效地抵抗密钥泄漏和熵的泄漏，并给出了安全性证明和抗泄漏性能指标。

1 基本知识

定义 1 随机变量 A、B 间统计距离定义为

$$SD=\frac{1}{2}\sum_{\omega\in\Omega}|\Pr(A=\omega)-\Pr(B=\omega)|$$

定义 2 熵和最小熵，随机变量 A 最小熵定义为

$$H_\infty(A)=-\log(\max_x\Pr(A=x))$$

表示 A 的不确定性度量，平均最小熵为

$$\tilde{H}_\infty(A|B)=-\log(E_{y\leftarrow B}(\max_x\Pr(A=x|B=y)))$$

表示 A 在 B 的条件下剩余不确定性度量。

引理 1[14] 若 A、B、C 是随机变量，B 最多有 2^λ 个值，那么

$$\tilde{H}_\infty(A|(B,C))\geqslant\tilde{H}_\infty(A|C)-\lambda$$

定义 3[15] 一个函数：$\mathrm{Ext}:\{0,1\}^n\times\{0,1\}^r\rightarrow\{0,1\}^m$ 称为强度为 (k,ε_1) 的提取器，只要满足条件：U 是 $\{0,1\}^m$ 上的均匀分布，S 是 $\{0,1\}^r$ 上的均匀分布，若对于 $A\in\{0,1\}^n$ 且 $H_\infty(A)>k$，就有 $SD((\mathrm{Ext}(A,S),S),(U,S))\leqslant\varepsilon_1$。其中 ε_1 为一个可以忽略的值。

2 基于证书的哈希证明系统

文献[8]给出了一个基于身份的哈希证明系统（IB-HPS），

收稿日期：2013-03-06；**修回日期**：2013-04-28 **基金项目**：国家自然科学基金资助项目(61272542)

作者简介：于启红(1979-)，男，江苏宿迁人，博士研究生，主要研究方向为计算机网络与信息安全(qihong-yu@163.com)；李继国 (1970-)，男，教授，博导，博士，主要研究方向为信息安全、密码学理论与技术.

在文献[16]给出了基于身份的加密方案到基于证书的加密方案的通用构造方法,因此,可以得到一个基于证书的哈希证明系统 CBE-HPS。本质上这个论证系统包含一个密钥封装机制,由六个多项式时间(PPT)算法构成:

$$\Phi = (\text{Setup}, \text{UserkeyGen}, \text{Certify}, \text{Encap}, \text{Encap}^*, \text{Decap})$$

1)Setup　系统配置算法,由认证中心(CA)运行,以安全参数 ν 为输入,输出系统的主私钥 msk 以及系统参数 params(包括主公钥 mpk 等), *CA* 把 params 公开,即(params,msk)←Setup(1^{ν})。

2)UserkeyGen　身份为 ID 的用户,以 params 为输入参数,输出对应的公钥 pk_{ID}和私钥 sk_{ID},(pk_{ID},sk_{ID})←UserkeyGen(params)。

3)Certify　对于身份为 ID 的用户和 pk_{ID},输入(params,msk,ID,pk_{ID}),输出证书 Cert_{ID},即 Cert_{ID}←Certify(params,msk,ID,pk_{ID})。

4)Encap　输入参数(params,Cert_{ID},pk_{ID}),输出得到(c,k),c 为密文,k 为封装密钥,即(c,k)←Encap(params,Cert_{ID},pk_{ID})。

5)Encap*　输入(params,Cert_{ID},pk_{ID}),输出 c'为密文,即 c'←Encap*(params,Cert_{ID},pk_{ID})。

6)Decap　输入(params,Cert_{ID},sk_{ID},c),输出 k,k←Dncap(params,Cert_{ID},sk_{ID},c)。

CBE-HPS 具有如下特点:

性质 1　正确性

$\Pr[k \neq k' \mid k \leftarrow \text{Dncap}(\text{params}, \text{Cert}_{\text{ID}}, sk_{\text{ID}}, c), k' \leftarrow \text{Decap}(\text{params}, \text{Cert}_{\text{ID}}, sk_{\text{ID}}, c')] < \varepsilon_2$,也就是说不能正确解密的概率是可以忽略的。

性质 2　有效密文与无效密文的不可区分性。在给定私钥情况下,敌手能区分密文是由无效封装算法 Encap 产生还是由有效封装算法 Encap* 产生的概率是可以忽略的值 ε_3。

性质 3　光滑性。若 c 由 Eecap*(params,Cert_{ID},pk_{ID})得到,k'取自均匀分布 U,k 由 Encap(params,Cert_{ID},pk_{ID})得到,那么 $SD((c,k),(c,k')) \leqslant \varepsilon_1$。

3　语义安全的抗泄漏的基于证书的加密方案

定义 4　熵的泄漏。在一个加密方案中敌手选取泄漏函数从挑战密文获得信息,若虽然敌手能获得 k bit 的信息量(即泄漏函数的输出为 k bit),但是从所对应的明文中恢复的信息量不多于 k bit,则称这个方案是可以抵抗熵泄漏的。

一个抵抗熵泄漏的基于证书的加密方案(LR-CBE)Π 通常由五个多项式算法构成:

$$\Pi = (\text{Setup}^*, \text{UserkeyGen}^*, \text{Certify}^*, \text{Encrypt}, \text{Decrypt})$$

其中包含一个身份集 Ξ 和消息空间 M,被封装的对称密钥假设为 $t_3$bit。

Ext:$\{0,1\}^{t_1} \times \{0,1\}^{t_2} \rightarrow \{0,1\}^{t_3}$是($t_4$,$\varepsilon_1$)提取器,输入长度为 $t_1$bit,随机数种子 $t_2$bit,输出为 $t_3$bit,只要输入 t_1 的最小熵不小于 t_4,则提取器的输出就是接近 $t_3$bit 的均匀分布。

1)Setup*　系统配置算法,调用 Φ 的 Setup 算法生成系统的主私钥 msk 以及系统参数 params(包括主私钥等),公开 params。

2)UserkeyGen*　用户 ID 的公钥和私钥生成算法,调用 Φ 的 UserkeyGen 算法以 params 为参数输出对应的公钥 pk_{ID}和私钥 sk_{ID}。

3)Certify*　证书生成算法,调用 Φ 的 Certify 算法,为身份 ID 的用户产生证书 Cert_{ID}。

4)Encrypt　加密算法,给定 $m \in \{0,1\}^{t_3}$和 ID $\in \Xi$。首先,调用 Φ 的 Encap 算法,(c_1,k)←Encap(params,Cert_{ID},pk_{ID}),c_1 为中间密文(不是 m 对应的密文),k 为被封装的对称密钥;接着,随机取一个值 $s \in \{0,1\}^{t_2}$,计算消息密文(是 m 对应的密文)$c_m = \text{Ext}(k,s) \otimes m$,输出总的密文(包含几部分)$c = (c_1, s, c_m)$。

5)Decrypt　解密算法,首先把总的密文 c 划分为(c_1,s,c_m),再调用 Φ 的 Dncap 算法,k←Dncap(params,Cert_{ID},sk_{ID},c_1),得到 k,接着计算 $m = \text{Ext}(k,s) \otimes c_m$。

正确性分析　这个方案显然是一个加密方案,该结论可以由它所依赖的 Φ 的正确性直接得到,而 Φ 的正确性可以由 CBE-HPS 来保证,所以这是一个正确的加密方案。为了分析方案的性能,特定义如下安全的实验 EXP。

4　基于证书抵抗泄漏的实验

1)初值设定　挑战者执行 Setup*,生成系统的主私钥 msk 以及系统参数 params(包括主私钥等),把 msk 通过公共信道传给敌手 A。

2)查询阶段 1　获得挑战密文前的查询,敌手 A 可以进行两类查询:

a)私钥查询。敌手给定 ID,希望得到相应的私钥,挑战者运行 UserkeyGen*,获得私钥 sk_{ID},返回给敌手。

b)泄漏查询。给定一个 ID,对于一个概率多项式时间(PPT)泄漏函数 $f(.)$,挑战者计算 $f(sk_{\text{ID}})$且返回给敌手。

这个过程可以进行若干次,泄漏函数总输出长度记为 L_{pre},自适应地查询体现在后一次查询可以依赖前面的查询结果。

3)挑战阶段　敌手 A 选定 $m_0, m_1 \in M$,和一个没有被询问过的 ID* 发送给挑战者,挑战者随机地选取 $b \leftarrow \{0,1\}$,执行算法 Encrypt,加密 m_b,得到密文 c_m。

4)查询阶段 2　与查询阶段 1 类似,只是提交的 ID 不能为挑战用的 ID*,且这一阶段主要是获得关于 c_m 的信息,敌手获得的信息量为 L_{post}bit,或者可以说是密文熵泄漏 L_{post}。

输出:敌手给出 $b^* \in \{0,1\}$,若 $b^* = b$ 敌手获胜。敌手优势记为 $\text{ADV}_A^{\text{EXP}}(.)$。

5　安全性能与抗泄漏性能分析

定理 1　加密方案 Π 是一个能抵抗泄漏为 $L_{\text{pre}} \leqslant t_1 - t_4$ 和 $L_{\text{post}} \leqslant t_3 - \delta$ 的安全的加密方案。其中,L_{pre}表示获得挑战密文前的密钥泄漏,L_{post}表示获得挑战密文后的熵泄漏,其中 $\delta < t_3 - \log(\frac{1}{t_3} + \varepsilon_1)$是一个额外开销量(事实上是提取器的损失)。

证明

1)先进行安全性分析

为此定义如下三个归约实验:

a)EXP1。稍微修改挑战阶段,挑战者用 sk_{ID}去计算密文,过程为

(c,k)←Encap(params,Cert_{ID},pk_{ID}),k'←Decap(params,

$Cert_{ID}, sk_{ID}, c)$, $c_m = k' \otimes m_b$。

b)EXP2。进一步修改 EXP1 挑战阶段,挑战者用无效封装算法代替有效封装算法

$c \leftarrow \text{Encap}^*(\text{params}, \text{Cert}_{ID}, pk_{ID})$, $k' \leftarrow \text{Decap}(\text{params}, \text{Cert}_{ID}, sk_{ID}, c)$, $c_m = k' \otimes m_b$。

c)EXP3。挑战者在 EXP2 的基础上,挑战者无须解封装算法且直接从均匀分布获取密文

$c \leftarrow \text{Encap}^*(\text{params}, \text{Cert}_{ID}, pk_{ID})$, $k \leftarrow U_{t3}$。

证明总体思路,对任一个 EXP 中语意安全的敌手 A,只要证明,一方面 A 在 EXP 和 EXP3 获得的优势的区别是一个可以忽略的数值;另一方面 A 在 EXP3 中的优势是可以忽略的,则综合考虑在 EXP 中语意安全的敌手 A 的优势就可以忽略,故所需的安全性可以获得。

具体如下:

EXP 和 EXP1 唯一区别是用于加密的 k 和 k'的计算不同,但由性质 1(CBD-HPS 的正确性)可知, k 和 k'不等的概率为 ε_2,所以 EXP 和 EXP1 敌手的优势区别为 $|ADV_A^{EXP}(.) - ADV_A^{EXP1}(.)| < \varepsilon_2$。

EXP1 和 EXP2 的区别在于 EXP2 用了一个无效的对称密钥封装算法,由性质 2(有效密文与无效密文的不可区分性)可知,敌手在这两个实验中的优势区别为 $|ADV_A^{EXP1}(.) - ADV_A^{EXP2}(.)| < \varepsilon_3$。

EXP 2 和 EXP3 区别在于两个方面:a)没有使用解封装操作,由性质 1 可知,敌手因此在这两个实验中的优势区别为 ε_2;b)直接从均匀分布 U_{t3}取元素而不是从提取器的结果中取元素,根据性质 3 可知,这会造成敌手在这两个实验中的优势有 ε_1 的不一致。考虑到这两个方面,可知敌手在这两个实验 EXP2 和 EXP3 中的优势相差为 $\varepsilon_1 + \varepsilon_2$,即 $|ADV_A^{EXP2}(.) - ADV_A^{EXP3}(.)| < \varepsilon_1 + \varepsilon_2$。

所以敌手在 EXP 和 EXP3 中的优势总的区别为

$$|ADV_A^{EXP}(.) - ADV_A^{EXP3}(.)| \leqslant |ADV_A^{EXP}(.) - ADV_A^{EXP1}(.)| + |ADV_A^{EXP1}(.) - ADV_A^{EXP2}(.)| + |ADV_A^{EXP2}(.) - ADV_A^{EXP3}(.)| \leqslant \varepsilon_1 + 2\varepsilon_2 + \varepsilon_3$$

那么敌手 A 在实验 EXP 中的优势为 $ADV_A^{EXP}(.) \leqslant ADV_A^{EXP3}(.) + \varepsilon_1 + 2\varepsilon_2 + \varepsilon_3$,而敌手 A 在 EXP3 中的优势 $ADV_A^{EXP3}(.)$就是其在 CBD-HPS 的优势。因为 CBD-HPS 中的敌手优势是可忽略的,所以 EXP 中的敌手优势 $ADV_A^{EXP}(.)$可以忽略。

2)抗泄漏性能分析

熵的泄漏 当 $L_{pre} \leqslant t_1 - t_4$,提取器 EXT 的输入在泄漏 L_{pre} 比特信息后还剩的最小熵为 $t_1 - L_{pre} \geqslant t_4$,所以由提取器的定义可知,随机选取一个 $t_2$bit 的种子,那么提取器可以得到非常近似的 $t_3$bit 均匀分布,由定义 1 可以得到提取器输出的对称密钥的熵为 $-\log(\frac{1}{t_3} + \varepsilon_1)$,所以额外的损失至多为 $\delta < t_3 - \log(\frac{1}{t_3} + \varepsilon_1)$。所以用对称密钥封装得到的密文有 $t_3 - \delta$ bit 的最小熵。

由引理 1,在获得密文后进行 L_{post}泄漏查询后还剩的熵为

$$\tilde{H}_\infty(m \mid f(sk_{ID})) \geqslant H_\infty(m) - L_{post} = t_3 - \delta - L_{post}$$

综上所述,定理得证。

6 结束语

本文提出了一个基于证书的抗泄漏的安全的加密方案,该方案结合基于证书的加密思想和 HPS 得到 CBE-HPS,再结合最近密码学领域新引入的熵泄漏概念,获得一个安全性能比较好的不仅可抵抗熵的泄漏而且还可以抵抗密钥泄漏的加密方案,给出了安全性证明和抗泄漏性能分析。由于抗泄漏研究是最近密码研究领域刚兴起的研究方向,有很多迫切需要解决的问题,如随机数的安全产生还是一个公开的问题,这将是下一步研究的重要方向。

参考文献:

[1] BONEH D, DEMILLO R, LIPTON R J. On the importance of checking cryptographic protocols for faults[C]//Proc of Advances in Cryptology - EUROCRYPT. Berlin: Springer, 1997:37-51.

[2] BIHAM E, SHAMIR A. Dierential fault analysis of secret key cryptosystems[C]//Proc of Advances in Cryptology - CRYPTO . Berlin: Springer, 1997:513-525.

[3] GANDOLFI K, MOURTEL C, OLIVIER F. Electromagnetic analysis: concrete results[C]// Proc of the 3rd International Workshop on Cryptographic Hardware and Embedded Systems. London: Springer-Verlag, 2001: 251-261.

[4] KOCHER P. Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems[C] //Proc of Advances in Cryptology - CRYPTO. Berlin: Springer , 1996:104-113 .

[5] HALDERMAN J A, SCHOEN S D, HENINGER N, *et al*. Lest we remember: cold-boot attacks on encryption keys[J]. Communications of the ACM, 2009, 52(5): 91-98.

[6] CHARI S, JUTLA C, RAO J, *et al*. Towards sound approaches to counteract power-analysis attacks[C]//Proc of Advances in Cryptology- CRYPTO. Berlin: Springer, 1999:398-412.

[7] NAOR M, SEGEV G. Public-key cryptosystems resilient to key leakage[C]//Proc of Advances in Cryptology - CRYPTO . Berlin:Springer, 2009:18-35.

[8] ALWEN J, DODIS Y, NAOR M, *et al*. Public-key encryption in the bounded-retrieval model[C]//Proc of Advances in Cryptology - EUROCRYPT. Berlin: Springer, 2010:113-134.

[9] HALEVI S, LIN Hui-jia. After-the-fact leakage in public-key encryption[C]//Proc of the 8th Theory of Cryptography Conference. Berlin: Springer, 2011:107-124.

[10] DODIS Y, HARALAMBIEV K, ADRIANA L A, *et al*. Efficient public-key cryptography in the presence of key leakage[C]//Proc of Advances in Cryptology- ASIACRYPT. Berlin: Springer, 2010:613-631.

[11] KATZ J, VAIKUNTANATHAN V. Signature schemes with bounded leakage resilience [C]//Proc of Advances in Cryptology -ASIACRYPT. Berlin: Springer , 2009:703-720.

[12] FAUST S, KILTZ E, PIETRZAK K, *et al*. Leakage-resilient signatures[C] // LNCS, vol 5978. Berlin: Springer, 2010: 343-360.

[13] GENTRY C. Certificate-based encryption and the certificate revocation problem[C]//Proc of Advances in Cryptology -EUROCRYPT. Berlin: Springer, 2003:272-293.

[14] DODIS Y, OSTROVSKY R, REYZIN L, *et al*. Fuzzy extractors: how to generate strong keys from biometrics and other noisy data [J]. SIAM Journal on Computing, 2008, 38(1): 97-139.

[15] NISAN N, ZUCKERMAN D. Randomness is linear in space[C] // Proc of Symposium on Theory of Computing. 1993:235-244.

[16] YUM D H, LEE P J. Identity-based cryptography in public key management[C]// Proc of the 1st European PKI Workshopon on Research and Applications. Berlin: Springer, 2004:71-84.