增强出版文本复制检测报告单(全文标明引文)

ADBD2017R_20170322170021201703221700598031928660003 检测时间：2017-03-22 17:00:59

检测文献: 李臣意_计算机科学与技术_硕士

作者: 李臣意

检测范围:

中国学术期刊网络出版总库
中国博士学位论文全文数据库/中国优秀硕士学位论文全文数据库
中国重要会议论文全文数据库
中国重要报纸全文数据库
中国专利全文数据库
互联网资源(包含贴吧等论坛资源)
英文数据库(涵盖期刊、博硕、会议的英文数据以及德国Springer、英国Taylor&Francis 期刊数据库等)
港澳台学术文献库
优先出版文献库
互联网文档资源
图书资源
CNKI大成编客-原创作品库
学术论文联合比对库
个人比对库

时间范围: 1900-01-01至2017-03-22

检测结果

总文字复制比：22.1% 跨语言检测结果：0%

去除引用文献复制比：21.4% 去除本人已发表文献复制比：21.6%

单篇最大文字复制比：15.6%

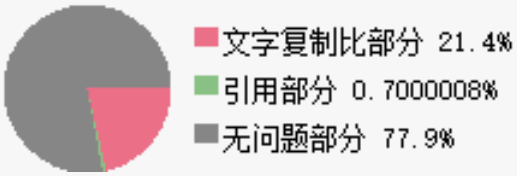
重复字数： [9569] 总段落数： [4]

总字数： [43298] 疑似段落数： [4]

单篇最大重复字数： [6776] 前部重合字数： [1011]

疑似段落最大重合字数：[3932] 后部重合字数： [8558]

疑似段落最小重合字数：[1581]



指 标：□疑似剽窃观点 ☑疑似剽窃文字表述 □疑似自我剽窃 □疑似整体剽窃 □过度引用

表格：0 脚注与尾注：0

13.4%（1625） 李臣意_计算机科学与技术_硕士_第1部分（总12090字）
19.9%（2431） 李臣意_计算机科学与技术_硕士_第2部分（总12200字）
31.6%（3932） 李臣意_计算机科学与技术_硕士_第3部分（总12436字）
24.1%（1581） 李臣意_计算机科学与技术_硕士_第4部分（总6572字）

（注释：无问题部分 文字复制比部分 引用部分）

1. 李臣意_计算机科学与技术_硕士_第1部分

总字数：12090

相似文献列表 文字复制比：13.4%(1625) 疑似剽窃观点：(0)

1	10736_070101_2011100043_LW	8.0%（964）
	LW -《学术论文联合比对库》- 2015-04-10	是否引证：否
2	具有特殊性质的认证协议设计及应用研究	2.0%（246）

	金春花(导师：许春香) -《电子科技大学博士论文》- 2016-04-01	是否引证：否
3	数字图像恢复	1.8%（215）
	-《学术论文联合比对库》- 2013-10-11	是否引证：否
4	适用于物联网应用的密码体制设计与分析	1.5%（182）
	郑朝慧(导师：李发根) -《电子科技大学硕士论文》- 2016-03-29	是否引证：否
5	无证书数字签名方案研究	1.3%（154）
	周冬瑞(导师：张玉磊) -《西北师范大学硕士论文》- 2015-05-01	是否引证：否
6	基于身份部分盲签名方案的分析与改进	0.5%（60）
	何俊杰;孙芳;祁传达; -《计算机应用》- 2013-03-01	是否引证：否
7	helongPBH	0.5%（59）
	-《学术论文联合比对库》- 2014-03-19	是否引证：否
8	正文	0.5%（56）
	-《学术论文联合比对库》- 2012-02-06	是否引证：否
9	门限密码体制的形式化安全研究	0.3%（34）
	龙宇(导师：陈克非) -《上海交通大学博士论文》- 2007-12-01	是否引证：否
10	适用于智能电网的组合密码体制研究	0.3%（31）
	韩亚楠(导师：李发根) -《电子科技大学硕士论文》- 2016-03-29	是否引证：否

原文内容　红色文字表示存在文字复制现象的内容; 绿色文字表示其中标明了引用的内容

分类号 TP309 密级

U D C 编号 10736

硕士学位论文几类异构签密方案的研究研究生姓名：李臣意指导教师姓名、职称：张玉磊副教授专业名称：计算机科学与技术研究方向：网络信息安全

二〇一七年三月

Research on several kinds of heterogeneous signcryption schemes

Li Chenyi

郑重声明

本人的学位论文是在导师指导下独立撰写并完成的，学位论文没有剽窃、抄袭、造假等违反学术道德、学术规范和侵权行为，否则，

本人愿意承担由此而产生的法律责任和法律后果，特此郑重声明。

学位论文作者（签名）：

年月日

学位论文使用授权书

本论文作者完全了解学校关于保存、使用学位论文的管理办法及规定，即学校有权保留并向国家有关部门或机构送交论文的复印件和电子版，允许论文被查阅

和借阅，接受社会监督。本人授权西北师范大学可以将本学位论文的全部或部分

内容编入学校有关数据库和收录到《中国博士/硕士学位论文全文数据库》进行信息服务，也可以采用影印、缩印或扫描等复制手段保存或汇编本学位论文。

本论文提交□当年/□一年/□两年/□三年以后，同意发布。

若不选填则视为一年以后同意发布。

注：保密学位论文，在解密后适用于本授权书。

作者签名：

导师签名：

年月日西北师范大学研究生学位论文作者信息论文题目几类异构签密方案的研究

姓名李臣意学号 201421161217

专业名称计算机科学与技术答辩日期

联系电话 13893319940 E_mail 675989124@qq.com
通信地址(邮编)：西北师范大学安宁区西北师范大学 967 号
备注：

目录

摘要

密码学是信息安全的核心技术。随着大数据、云计算、5G 异构网络等平台的展开，跨平台操作越来越广泛。如果要在不同的密码系统之间进行通信，就需要支持异构通信的密码体制。

签密能够同时实现信息通信过程中的机密性和不可伪造性，大多数密码方案只考虑同类公钥密码系统之间的签密问题，而在现实生活中，不同的应用平台采用不同密码技术。因此对于签密方案的设计、分析问题，必须考虑异构密码体制如何实现的。

本文主要是从以下三方面进行研究，具体如下:

(1) 本章提出了一个从传统的公钥密码(Tradational Public Key Cryptography，TPKC)到基于身份的公钥密码 (Identity Public Key Cryptography ，IDPKC)的异构签密方案。该方案实现了通信过程中机密性和不可伪造性两个目标。而且，在进行签密操作时，不需要对运算和幂运算；进行解签密操作时，仅需要 1 个对运算，效率有了一定的提高。在安全性方面，该方案满足通信过程中的内部安全性。在随机预言模型下，证明该方案满足 IND-SC-CCA2 安全性和 EUF-SC-CMA 安全性。

(2)提出了一个从无证书公钥密码(Certificateless Public Key Cryptography，CLPKC)到传统公钥密码(TPKC)的异构签密方案。该方案在签密过程中仅一个幂运算，在解签密的过程中仅需要一个对运算和幂运算，具有较高的效。同时也满足通信过程中的内部安全性。在随机预言模型下，基于 q-SDH 困难问题，证明能够抵抗适应性选择消息攻击下的存在性伪造和适应性选择密文攻击下不可区分性。

(3)提出了一个匿名的从身份公钥密码系统(IDPKC) 到传统公钥密码系统（TPKC）异构签密方案。本文方案有以下特点：首先，不仅保证在安全通信过程中信息的机密性和不可伪造性，而且在随机预言模型下，该文方案满足签密过程中的内部安全性；其次，与同类方案相比效率有了一定的提高。同时，方案实现了密文的匿名性，有效保护了接收方与发送方的隐私；最后，方案中 IDPKC 和TPKC 密码环境中应用了不同的系统参数，从而更加有效的模拟了实际的应用场景。

关键词：异构签密，匿名性，传统公钥密码体制，无证书公钥密码体制，身份公钥密码体制

Abstract

Cryptography is the core technology of information security. With big data, cloud computing, 5G heterogeneous network platform to expand, cross-platform operation more and more widely. If you want to communicate between different cryptographic systems, you need to support heterogeneous communication password system.

Signing can be achieved at the same time in the process of information communication confidentiality and unforgeability, most of the password scheme only consider the same type of public key cryptography between the signcryption problem, and in real life, different application platform using different cryptography. Therefore, for the design of signcryption program, analysis of the problem, we must consider how to achieve heterogeneous cryptography.

This paper is mainly from the following three aspects of research, as follows:

(1) This chapter presents a heterogeneous signcryption scheme from the traditional public key cryptography (TPKC) to the Identity Public Key Cryptography (IDPKC).

The scheme achieves two goals of confidentiality and unforgeability in the communication process. Moreover, when performing a signcryption operation, there is no need for an operation and a power operation. When performing a deblocking operation, only one pair of operations is required, and the efficiency is improved. In terms of security, the program meets the internal security in the communication process.

In the stochastic prediction model, it is proved that the scheme meets the safety of IND-SC-CCA2 and EUF-SC-CMA.

(2) Propose a heterogeneous signcryption scheme from Certificateless Public Key Cryptography (CLPKC) to Traditional Public Key Cryptography (TPKC). The scheme has only one exponentiation in the process of signcryption, and only one pair of operations and exponential operations are required in the process of deconvolution. But also to meet the internal security of the communication process. Under the stochastic prediction model, based on the problem of q-SDH, it is proved that it can resist the indistinguishability of ciphertext attacks under adaptive attack and adaptive selection under adaptive attack.

(3) Proposed an anonymous from the identity of the public key cryptography

(IDPKC) to the traditional public key cryptosystem (TPKC) heterogeneous signcryption program. Firstly, it not only guarantees the confidentiality and unforgeability of information in the process of secure communication, but also in the random prediction model, which satisfies the internal security in the process of signcryption. Secondly,

Than the efficiency has been improved. At the same time, the scheme realizes the anonymity of the ciphertext and effectively protects the privacy of the receiver and the sender. Finally, the IDPKC and TPKC cryptographic environments use different system parameters to simulate the actual application scene more effectively.

Keywords: Heterogeneous signcryption, Anonymity, Traditional public key

cryptography, Certificateless public key cryptography, Identity public key cryptography

1

1 绪论

1.1 研究背景和意义

签密能够同时实现信息通信过程中的机密性和不可伪造性，大多数密码方案只考虑同类公钥密码系统之间的签密问题，而在现实生活中，不同的应用平台采用不同密码技术。因此对于签密方案的设计、分析问题，必须考虑，在异构密码体制下是如何实现的。

目前，大多数的签密方案都是基于同一种密码系统，即接收方与发送方属于同一种密码系统。随着大数据

[1]

、云计算

[2]

、5G 异构网络

[3]

等实际应用场景的变化，跨平台的操作将会越来越频繁。例如，大型电子邮件系统

[7]

、无线移动网络

[8]

的跨系统访问等，这些应用都必须考虑有别于“同构密码体制”。对于签密

[5]

而言，我们要考虑异构密码环境

[4]

下方案的设计、分析以及实现。

不同的计算机和通信系统可能采用不同的安全技术，在异构网络中自然也需要考虑异构密码环境（即发送方和接收方具有不同的公钥密码环境）。因此，研究异构密码环境之间的签密问题将是最值得研究的问题之一。

1.2 研究现状

基于传统的公钥密码体制

[6]

(TPKC)不仅能够提供不可否认性、机密性和完整性

[9]

。在随机预言模型下基于传统的签密体制已经比较成熟，但是在标准模型下安全的基于 TPKC 的签密体制还比较少，这也是未来的一个重要研究方向。

2008 年，Tan

[10]

利用了 Boneh 和 Boyen 设计了基本身份的加密方案

[11]

以及 Boneh

和 Boyen 的短签名方案

[12]

设计了一个在标准模型下安全签密方案。但是，这个方案的发送者密钥生成方法和接收者密钥生成方法是不同的。如果一个用户既是发送者又是接收者，那么他需要拥有两对密钥，同时需要申请两个公钥证书，这对于实际的应用是不利的。

为了解决基于身份的密码体制的密钥托管问题，Al-Riyami 和 Paterson

[13]

提出了无证书密码体制(CLPKC)的概念。实际上，无证书密码体制并不一定要使用双

线性对来构造，如文献[14]和[15]中构造的无证书加密方案就没有用使用双线性

对 ，他们利用一个非对称的签名方案来生成部分私钥。另外一个重要的方向是
构造标准模型下无证书签密体制。2010 年，Liu
[16]
等人在无证书模型下建立设计无证书的签密体制。
2
现代计算机和通信系统形成了一个全球覆盖的基础设施。不同的计算机和通信系统可能采用不同的安全技术。有的采用基于传统公钥的密码体制，有的采用
采用基于身份的公钥密码体制。2010 年，Sun 和 Li
[17]
等人提出了基于传统的公钥密码体制和基于身份的公钥密码体制双向异构签密方案，但是他的方案仅仅满
足外部安全性，不能满足内部安全性，更没有提供否认性。2011 年，Huang、
Wong 和 Yang 提出了一个具有密钥隐私的异构签密方案
[18]
。2013 年，Fu 等
[19]
人在Sun的基础上提出了一个IDPKC → TPKIC多接收者的异构签密方案，2013
年，Li、Zhang 和 Takagi 提出一个新的基于传统的公钥密码体制和基于身份的公钥密码体制双向异构签密方案
[20]
。
1.3 本文的主要工作和内容安排
第一章：研究背景和意义。主要介绍了密码学的发展、公钥密码体制、及异
构签密
[22]
的发展现状。
第二章：基础知识。主要介绍包括双线性对、随机预言模型、哈希函数、公
钥密码体制等密码学知识和数学知识。
第三章：设计了一个高效的 TPKC→IDPKC 的异构签密方案。本方案相对于
同类方案效率方面总体上有了一定的提高，同时也满足通信过程中的内部安全性，但是解签密操作在效率上仍有可以改进的空间。
第四章：提出了基于双线性对 CLPKC→TPKC 的异构签密方案。本方案在
进行签密操作的时候不需要对运算，而进行解签密操作的时候只需要一个对运算，同时本方案也满足通信过程中内部安全性；但是本方案在基于无证书的密码体制与传统的密码体制所采用的系统参数都是一致的，不能更好的模拟实际的应用场景。
第五章：匿名 IDPKC→TPKC 异构签密方案。IDPKC→TPKC 异构签密方案
不仅保证在安全通信过程中信息的机密性和不可伪造性，而且在随机预言模型下，该文方案满足签密过程中的内部安全性；其次，与同类方案相比效率有了一定的提高；最后，方案中 IDPKC 和 TPKC 密码环境中使用了不同的系统参数，
从而更加有效的模拟了实际的应用场景；同时方案满足匿名性
[24]
，可以有效保护发送方和接收方的隐私。
第六章：总结展望。对几类异构签密方案的效率、匿名性以及安全性研究进
行一个总结，并对未来的研究工作进行展望。
3
2 基础知识
2.1 双线性对
设
1
G 为 P 生成的循环加法群
[23]
，阶为，
2
G 为具有相同阶q 的循环乘法群，
a
和b是

*
q
Z 中的元素，存在两个群
1
G 和
2
G 上的双线性对
[21]
映射
1 1 2
e :G G G，且满足以下性质：
(1)双线性：对于任意的
1
P, Q G和
*
,
p
a b Z
，(,) (,)
ab
e aP bQ e P Q成立。
(2)非退化性：
1
P, Q G，使得 e (P , Q) 1。
(3)可计算性：对于所有的
1
P， Q G，存在有效的计算 e (P , Q)
2.2 相关困难问题
(1) 计算 Diffie-Hellman 问题(Computable Diffie-Hellman Problem):给定一个
阶为 q 的循环加法群
1
G 和一个生成元 P ，输入 (p , aP ,bP)，计算 abP 。这里
*
,
q
a b Z
是未知的整数。
(2) 双线性对 Diffie-Hellman 问题(Bilinear Diffie-Hellman Problem):给定两个
阶都为 q 的循环加法群
1
G 和循环乘法群
2
G 、双线对映射
1 1 2
e :G G G和群
1
G 的生成元P，输入
(p , aP , bP ,cP)，计算
2
(,)
abc
e P Q G，这里

*

, ,

q

a b c Z

是未知的整数。

(3)

q

强 Diffie-Hellman 问题(q-Strong Diffie-Hellman Problem)：给定两个阶都为 q 的循环加法群

1

G 和循环乘法群

2

G ，双线性对映射

1 1 2

e :G G G，输入

2

1 1 1

(, , ,...)

n

P P P，计算

*

1

1

(,)

p

Z G

。

2.3 随机预言模型

在随机预言机

[22]

中，仿真器(挑战者)按照某种方式仿真用户(攻击者)的预言机行为。如果用户需要对某个输入值使用预言机，用户需要对仿真器提出预言机请求，然后才从仿真器得到结果。

1986 年，Fiat 和 Shamir

[25]

首次提出了随机预言的概念。后来，Rogaway 和

Bellare 于 1993 年从文献[25]的思想中的到启迪，将随机预言机的概念转换成了

随预言模型。在随机预言模型下进行安全证明：假设有一个能够让各方共同使用的公开的随机参数，即就是随机预言机，且随机预言机需要满足下列下列三个性

4

质：

(1) 一致性，针对同样的输入，得出的回答一定是一样的；

(2) 有效性，对于所有询问输入，输出的回答结果是可以在多项式时间内计

算完成的。

(3) 随机性，对于所有询问，预言机的输出呈现出均匀分布，无碰撞。

2.4 哈希函数

定义 2.2 哈希函数

[26]

，又可以叫做杂凑函数，他可以把任意长度的消息压缩转换程固定长度的比特串，它在消息完整性检验、数字签密

[4]

等领域被广泛应用。

为了实现对消息的认证，哈希函数 h 必须具备以下性质：

(1) 散列性：对于任意的输入 x， h (x)在[0, 2]

k

中均匀分布。
(2) 有效性：对于任意输入 x，可以在低阶多项式时间内计算 h (x)，即可计算 h (x)。
(3) 抗弱碰撞攻击性：已知 x，找到
x y
满足 h (x) h (y)
在计算上是不可行的。
5
3 高效的 TPKC→IDPKC 的异构签密方案
3.1 高效的 TPKC→IDPKC 异构签密方案形式化定义
(1)TPKC 系统建立算法
该算法通过 CA 来实现，输入参数1
k
，并公开产生系统参数 params ，其中k 是安全参数。
(2)TPKC 密钥生成算法
TPKC 系统中的用户使用该算法生成公钥
s pk 和私钥
s
sk 。
(3)IDPKC 密钥提取算法
用户提交身份给 PKG，计算私钥
r sk 并发送给这个用户。用户的公钥是身份
U
ID 。这种公钥不需要数字证书。
(4)签密算法
该算法输入系统参数params
、TPKC 环境下发送者的私钥
s
sk 、IDPKC 境下
接收者的公钥
r pk 和消息m ， 输出密文 ， 该算法可以表示为
(, ,)
s r
Signcrypt sk pk m。
(5)解签密算法
该算法输入系统参数、TPKC 环境下发送者的公钥
s
pk ,IDPKC 环境下的接
收者的私钥
r
sk 和签密密文
,输出消息m
或者“⊥”。
这些算法必须满足异构签密一致性
[27]
要求 ， 即如果
(, ,)
s r
Signcr y p tsk pkm
，那么
,
(,)

s r
m Unsigncrypt pk sk
。
3.2 高效的 TPKC→IDPKC 的异构签密安全模型
机密性
游戏 3.1
TPKC→IDPKC 异构签密方案的适应性选择密文攻击由以下五个阶段组成，挑战者C和敌手 A之间进行以下游戏。
(1)初始阶段：C 执行系统“TPKC 建立算法”，输入安全参数，并将获得的系统参数params
发送给 A。同时运行“TPKC 密钥生成算法”，可以得到发送者的公钥
s pk 和发送者的私钥
s
sk ，并将其发送给 A 。
(2)挑战阶段： A 决定阶段 1 何时结束并进入挑战阶段。 A 得出两个长度一样的明文
0
m 、
1
m 和接收者身份
u ID 并将它们发送者 C 。C 首先对
u
ID 调用“TPKC
6
密钥生成算法”，获得发送者的私钥
s sk 但
u
ID 不能是已经执行过密钥提取询问的身份。随机选择一个比特 {0,1}
并计算
*
(, ,)
s u
Signcrypt sk ID m
。(3)猜测阶
段： A输出一个比特
。如果
`
，那么 A赢得这个游戏。
A 赢得上述游戏的优势被定义为
`
Adv (A) Pr( ) 1/ 2
，其中
`
Pr( )
表示
`
的概率。
定义 3.1 如果没有任何多项式有界的敌手在t 时间内，在经过
k q 次签密和
u

q 解签密询问后，以至少
的优势赢得游戏 3.1，那么称本文方案是
(, , ,) 2
k u
t q q IND HSC CCA
(Indistinguishability against adaptive-Hetero
geneous Selected Chosen-Chosen Ciphertext Attack)安全的。
不可伪造性游戏 3.2
初始阶段：C运行“IDPKC 系统建立算法”，并将产生的系统参数params 发送给F 。C同时运行“IDPKC 密钥提取算法”以获得接收者的公钥
r
pk 和接收者
私钥
r sk ，并将
r
pk 发送给 F 。
攻击阶段：在一个签密询问中，F 提交一个接收者的公钥
w pk 和一个消息给
C 。如果
r pk 不等于
w pk ，并且
w
pk 是一个合法的公钥，那么 C 运行“签密算法”
并返回密文 (, ,)
r w
Signcrypt sk pk m
给F ；否则返回错误符号“⊥”。在一个解签密询问中，F 提交一个密文
给C，输出解签密密文 (, ,)
w r
Unsigncrypt pk sk
。
伪造阶段：F 产生新的密文
*
和密钥对(,)
t t
pk pk 。当满足下列两个条件，F
赢得这个游戏。
(1)
*
(,)
t Unsigncrypt sk 输出 (, ,)
r m s pk 且满足 (, ,)
r
Verrify pk m s
。
(2) F 没有询问过涉及消息 m 和接收者公钥
w
pk 的签密询问，这个询问会返
回密文并且 (, ,)
r pk m s 成立。这里的
w pk 可能不等于
r

pk 。
定义 3.2 如果没有任何多项式有界的敌手在t时间内，在经过
s q 签密询问和
u
q 次解签密询问后，以至少
的优势赢得了游戏 3.2，那么就称这个具有密钥隐
私性质的 (, , ,)
s u
t q q EUF HSC CMA
(Existential Unforgeability against
adaptive-Hetero geneous Selected Chosen-Chosen Message Attack)安全的。
3.3 高效的 TPKC→IDPKC 的异构签密方案详细描述
(1)系统建立算法
设
1
G 为 P 生成的循环加法群，阶为q
(
q
为k 特素数，k 为安全参数)，定义生成元
1
P G
，
2
G 为具有相同阶的q
的循环乘法群，存在一个双线性映射
7
1 1 2
e :G G G
。定义三个 Hash 函数
1
*
1
3
: 0,1
m q l
H G Z、
2 2
:{0,1}
m l
H G 、
3 2
:{0,1}
m l H G ，
m l 是签密消息的长度,， PKG 随机选择一个主密钥
pub
P sP
，
计算
pub
P sP
。 设 g e(P, P)
， PKG 公开系统参数

1 2
{ , , , , ,
pub
G G e P P
1 2 3
, , , , }
m
l g H H H 保密主密钥 s 。
(2) TPKC 密钥生成算法
TPKC 系统中的用户随机选择
*
q
u Z
，作为自己的私钥，并且设置公钥
s s
pk sk p
。
(3) IDPKC 密钥提取算法
IDPKC 系统中的用户提交身份
r
ID 给 PKG，PKG 计算用户的用户的私钥
1
1
( )
r r sk P
H ID s
。
(4)签密算法
假设用户 Alice 属于 TPKC 系统，作为发送者。它的公钥为
s s
pk sk P
，私
钥为
s
sk ；用户 Bob 属于 IDPKC 系统，作为接收者。它的公钥就是身份信息
2
( )
r r
pk H ID 和私钥
r
sk 。当 Alice希望通过签密方式发送消息 m 交给 Bob 时，
执行以下步骤：
① 随机选择
*
q
r Z
，并计算W rP和
2
( )
r r
pk H ID
。

② 计算
1
(, ,)
s r
V sk H m W pk
。
③ 计算
r
x g和
3
c m H (x)
。
④ 计算
1
[( )]
r pub
T r H ID P P。
⑤ 消息m的签密密文：(c , T , W , V)。
(5)解签密算法
① 计算 (,)
r
x e T sk
和
3
m c H (x)
② 计算
1
(, ,)
r
N H m W pk
和
2
( )
r u
pk H ID
6)验证算法
① 如果
r1
pk G
，那么输出错误符号“⊥”，检查等式 (,) (,)
r
e pk N eP V
,是
否成立，如果成立，那么输出(,(, ,),)
r r
m W Q V pk ，否则输出错误符号“⊥”。
3.4 高效的 TPKC→IDPKC 的异构签密方案的性质
3.4.1 正确性
本方案满足一致性要求:接收者 Bob 可以正确的解密，密文也可以被正确的
8
验证。
(1) 正确的解密：当 Bob 收到密文 (c , T , W , V)

时，可以正确的解密。
1
1
1
(,)
((( )),)
1
((( )),)
( )
(,)
r u pub r u pub r r e T sk e r H ID P P sk e r H ID P P P H ID s e rP P
g x
(2) 正确的验证：当 Bob 收到密文 (c , T , W , V)
和 Alice 的公钥，可以通过
验证等式： (,) (,)
u
e pk N e P V
。
1
1
(,)
(,(, ,))
(, (, ,))
(,)
s s r u r e sk P e P sk e pk N H m W pk H m W pk
e P V
3.4.2 机密性
定理 3.1 在随机预言模型中，若存在一个敌手 A够在t 时间内，以
优势解
决游戏 3.1，则存在一个算法 C，能够在
2
' 2
1
( ) ( ) ( )
u p m u H e
t t O q t O q H t O q q t
时间内，以
1 2 3
'
(1)
(2) 2
u k H H H q
q q q
的优势解决 n-BDHI 问题(这里
1
n qH
)。

指　标
疑似剽窃文字表述

1. 一个全球覆盖的基础设施。不同的计算机和通信系统可能采用不同的安全技术。有的采用基于传统公钥的密码体制，有

的采用
采用基于身份的公钥密码体制。

2. 如果用户需要对某个输入值使用预言机，用户需要对仿真器提出预言机请求，然后才从仿真器得到结果。

3. TPKC→IDPKC 异构签密方案的适应性选择密文攻击由以下五个阶段组成，
挑战者C和敌手 A之间进行以下游戏。
(1)初始阶段：C 执行系统“TPKC 建立算法”，输入安全参数，并将获得的
系统参数params
发送给

4. 阶段： A 决定阶段 1 何时结束并进入挑战阶段。 A 得出两个长度一
样的明文
0
m

5. 初始阶段：C运行“IDPKC 系统建立算法”，并将产生的系统参数params 发送给F

6. IDPKC 密钥提取算法
IDPKC 系统中的用户提交身份
r
ID 给 PKG，PKG 计算用户的用户的私钥
1
1
(

7. 签密方式发送消息 m 交给 Bob 时，
执行以下步骤：
① 随机选择
*
q
r

证明：
初始阶段：C随机选择
1
{1,..., }
H
q
,
*

p
e Z
和
1
，…，
1
，
1
，
*
n p
Z
。
对于 i 1，…, 1, 1,…, n , C 计算
i i
e e
,并使用它的输入计算一个生成元
1
Q G
,以至于它知道 n 1对
1
(,)
i i
Vi Q
，i {1,..., n} \{ }
。C 为了获得这样的元素，C 展开多项式:
1
1,0
( ) ( )
n n j i j i ij
f z z c z
，生成元Q 和元素 X 可以分别通过
1
0
( ) ( )
n j j j
Q c P f P
和
1
1
( ) ( )
n j j j
X c P f Q 得到。同时(,)
i i
V
可以通过
2
0
( )
( )
n j i j j i f z f z d z
z

并计算
2
0
( )
( ) ( )
n j i j j i f
V d P fi P P
1
i
Q 得到。PKG 的公钥设为 ( )
pub
Q X e Q e Q
，相应的私钥为
9
*
p
s e Z
。对于 i {1,..., n} \{ }
，这里有
1
(,) (,)
i i i i e V e Q
e s
。
C 将系统参数[包括 Q 、 ( )
pub
Q e Q
]和 g e (Q , Q)]发送给A 。C 同时运
行密钥生成算法获得发送者的公钥/私钥对(,)
u u
pk sk 并发送给 A
。
阶段 1：C模拟游戏 1 中 A的挑战者。C 维护
1
L 、
2
L 、
3
L 三张列表，分别用于跟踪 A对预言机
1
H 、
2
H 、
3
H 的询问。这里假设每次
1
H 询问是不同的，目
标身份
v
ID 在某个时候被询问过
1
H 和身份

v
ID 在被使用到其它询问之前已经询问过
1
H 预言机。
1
H 询问：对于
1
H 询问， C 首先检查元组
1 2 3
(m, P , P , P)是否已经存在于列表
1
L
中。如果已经存在，那么返回结果。如果不存在并且等式
1 2 3
e (P , P) e (P , P)
成立和
1, 2
(P P ,)
已经存在列表
1
L 中，C 用
3
P 代替“┬”并将存在的结果返回给 F 。对其
他的情况，C随机选择
p
t Z
并返回tP给F 。询问的元素和返回的值都将存储在列表
1
L 中。
2
H 询问：设计计数器 v ，初始值为 1。对于一个
1
( )
v H ID 询问，C 返回
v
e 作为
回答，将(,)
v v
ID e 存进列表
2
L 并将计数器 v 的值的加 1。
密钥提取询问：当 A询问
i
ID 的私钥时，如果 i
，那么C 失败并停止；否则C知道
1
( )
i i
H ID e
，并返回
1
i i V Q

e s 给A
。
解签密询问：A提交一个接收者身份
j
ID 和一个密文给挑战者 C 。如果 j
，
那么C 知道接收者的私钥
j j
S V
，可以按照正常的解签密步骤来回答这个询
问。如果j
，那么对于所有合法的密文，有
log ( ) log u j u pub sk u e Q Q
V hsk T
，这里这里的
2
h H (m, x)
。因此，等式 (,) (,)
u j u pub u
e T sk e e Q Q V hsk
成立。C 首
先计算 (,)
j u p u b
e V e Q Q
并在
2
L 中查找形式为
2, ,
{ , , , }
i i i
m x h c
的条目，这里
2
{1,..., }
H
i q
。如果没有这样的条目，那么C拒绝回答的解签密询问；否则C 进一步检查等式
(,)
(,)
(,)
u j u pub u j u pub e T sk e e Q Q V hsk
e e Q Q V
。如果唯一满足上述方程的
2
{1,..., }
H
i q 已找到，那么C返回匹配的消息
i
m 。
挑战阶段：A产生两个一样长度的明文
0
m 和

1
m 和接收者身份
B
ID ID
并将
他们发送给C。如果
B
ID ID
，那么C终止；否则C随机选择
*
{0,1}
m l
c 、
*
1
V G
10
和
*
T Q并计算
*
T Q。 C 返回密文
* * * *
(c , V , W)给 A 。如果定义
2
H 且s e
，那么就有
*
- -
pub
T Q Q e Q Q
除非 A 对进行
*
和
3
H 询问，否则他（她）不能辨别出
*
是一个不合法的密文。
猜测阶段： A输出一个比特
'
-
，C 忽略这个输出。
C 从列表
2
L 或者
3
L 中提取一个随机的条目
2,
(, , ,)
i i i i i
m x h c
或者
3,

(,)
i i
x h 。既然
3
L 包含的条目至多为
2 3
2
H H
q q
，那么随机选择的条目包含了正确元素
2
( )
(,) (.)
f i
x e Q Q e P P
的概率为
2 3
1
2
H H
q q
。如果
* 1
e(P, P)
，那么n-BDHI 问题可以通过下式解决:
0
2
2 2
1
*( )
1 0 1
0 0
(,) (( ),) (, ( ))
n n c j j j j j j
e Q Q e c P c P e Q c P
下面分析C的优势，定义以下三个事件
1
E : A 在挑战阶段没有选择 ID
为接收者的身份。
2
E : A 对身份 ID
进行了秘钥提取询问。
3
E : A 由于在解签密询问中拒绝了一个合法的的密文而终止。
由上面的分析来看：不终止的概率为
1 2 3
Pr[e nd]=P r[E E E]
，
1
1
H
1

[ ]
q
Pr E
和
3
[ ]
2
u k q
Pr E ， 此外 ，
1
E
意味着
2
E
。 所以 ， 有
1
H
1
[ ] (1)
q 2
u k q
Pr e nd
。另外，C从
2
L 或者
3
L 中选择正确元素的概率为
2 3
1
2
H H
q q
。
因此有
1 2 3
' (1)
(2 q) 2
u k H H H q
q q
。
3.4.3 不可伪造性
定理 3.2 在随机预言模型中，若存在一个敌手
F 能够以的优势攻破本方案EUF-HSC-CMA 的安全性，则存在一个算法 C ，以
1
( ) ( )
(1 2)(1 2)
poly k poly k u H s
q q q 的优势解决 CDH 问题。其中，
u
q 表示最大的解签密询问次数；
1
H

q 表示最大的
1
H 询问次数；
s
q 表示最大的签密询问次数， ploy 表示一个多项式； k 为安全参数。
证明：
初始阶段：C运行“IDPKC 系统建立算法”，得到系统参数并发送给F ，
同时将主密钥s
也发送给F ，同时运行“TPKC 密钥生成算法”获得发送者的公钥/
11
私钥(,)
s s pk sk 发送给 F 并且设
v
pk bP
为挑战公钥。
1
H 询问：对于一个
1, 2
(P P ,)
询问，C 首先检查元组
1 2 3
(m, P , P , P)是否已经存在于列表
1
L 中。如果已经存在，那么返回结果。如果不存在并且等式
1 2 3
e (P , P) e (P , P)
成立和
1, 2
(P P ,)
已经存在列表
1
L 中， C 用
3
P 代替“ ”并将存在的结果返回给F 。
2
H 询问：这些询问用一个计数器 v 来标记，其初始值为 1。对于一个
1
( )
v
H ID 询问，C返回
v e 作为回答，将 (,)
v v
ID e 存进列表
2
L 并将计数器 v 的值的加 1。
签密询问：F 提交接收者的公钥
w pk 和消息 m 给 C 。如果
w
pk 不合法或者等
于
u pk ，那么返回一个错误符号“⊥”；否则 C 随机选择
p

r Z
，计算W rP。如果(m, W , pk , rpk)
经存在于
1
L 中且相应的 Hash 值是 taP ，那么 C 失败并停止。
否则，C随机选择
'
p
t Z
并返回
‘
t P 作为
1
H (m, W , pk , rpk)
的值，询问元组、返回值和
‘
t 都被存进列表
1
L 中 。 C 计算 (, ,)
s
W P k
， 同理可以获得
2
H (m, W , pk, rpk)
并计算
`
2
(| | | |) (, ,)
u u
T m pk t pk H W PkrPk
得到密文
(c , T , W , V)
。
解签密询问：F 提交一个签密密文
(T , W)
给挑战者C ，得出解签密密文
(,)
u
Unsigncrypt sk
。执行下面的步骤：
(1)在列表
2
L 中查找元组 (, ,)
u
W pk 使得 (,) (,)
u
e P e U pk
成立或
T
。如果列表
2
L 中不存在元组 ，那么在

2
L 中插入一个新的条目，这个条目以
(, ,)
s
U pk 为询问元组。符号“ ”表示 (, ,)
s
P U pk 的 CDH 问题的解。这一步确保
了(,) (,)
s
P W pk
，在
解签密前确定下来。如果元组(, ,)
s
W pk
已经存在于
2
L
中，那么存在的结果将为
2
(, ,)
s
H W pk
的值。
(2)计算
2
(||) (, ,)
s s
m pk V T H W pk
并在列表
1
L 中查找 (, , ,)
s
m W pk
使
得(,) (,)
s
P W pk
成立或者 。如果
1
L 中不存在
1
(, ,,)
s
H m W pk
，那么
1
L 中
插入一个新的条目，这个条目以(, , ,)
s
m W pk
为询问元组，以一个随机值taP为
返回值。这里

p
t Z
。值得注意的是， 可能已经从上面的
2
L 获得，等式
(,) (,)
s
e P e W pk 可能成立。如果元组 (, (, , ,)
s
m W pk V
已经存在于
1
L 中并且等
式 (,) (,)
s
e P e W pk
成立，那么存在的值作
1
(, ,,)
s
H m W pk
的值， 也用于更新
2
L 中相应的条目。如果
1
abP t V
存在于
1
L 中。如果可以从
2
L 中获得，那么
(, , ,)
s
m W pk 也应该被更新为(, , ,)
s
m W pk
。
(3)检查等式
1
(, (, , ,)) (,)
s s
e pk H m W pk e P V
是否成立。若不成立，则输出错误符号“
⊥
”否则进一步检查等式 (,) (,)
s
e P e W pk
是否成立。若成立，则输出消
12
息/签名 (, (, , ,)
s
m W pk V 发送者的公钥

s
pk 。若 ，则 C 失败并停止。
伪造阶段：当F 产生一个密文和一个密钥对
(,)
v v
sk pk 时，V taP按照上述解签密模拟的步骤对密文进行解签密。如果这个伪造是合法的，那么有
1
(, (, , ,)) (,) (,)
s s
e pk H U pk V e P V e bP taP
。C 可以得到V taP并解决 CDH 问题
1
abP t V
,C 输出abP并停止。
由上面的解签密模拟可以看出，
1
L 中必定存在一个针对
1
(, ,,)
s
H m W pk
的条目且相应的返回值一定是taP形式。如果说
1
(, ,,)
v
H m W pk
的值为
‘
t P ，即从签密
询问中生成，那么也应该在签密询问阶段生成。这于游戏 2 中的限制条件 (
不
是由签密预言机输出的）相矛盾。
C 失败的情况有两种。第一种在签密询问中，选择了
p
r Z
，(m, W rp , pk)
已经询问过了
1
H 了，这种事件发生的概率为
1
H s1
q q l 。 C 不失败的概率至少为abP 。第二种在解签密询问中，同理也可以得出 C 在解签密询问中不失败的概率至少为
( )
1 2
poly k u
q
。如果C不失败并且F 赢得了这个游戏，那么C能够解决 CDH
问题。因此，
1
( ) ( )
Pr[ ] (1 2)(1 2)
poly k poly k u H u

win q q q
。
3.5 效率分析
表 1 列出了该文方案与其他方案所需要的运算量，其中
p 表示对运算，
e
表示幂运算。
表 1 该文方案与其他方案所需的运算量
方案签密操作解签密操作内部安全性
文献[19] 1p+1e 2p+1e 不满足
文献[17] 1p 2p+1e 满足
本文方案 1e 1p 满足
3.6 本章小结
本章提出了高效的 TPKC→IDPKC 的异构签密方案，虽然基于不同的公钥密码系统实现的，但是两种系统所采用的参数都是相同的，得出的效果并不是很理想，所以在以后异构签密的研究中，不同的密码系统采用不同的参数，满足现实生活中的应用场景；虽然该文方案效率上有了一定的提高，但是仍有可以改进的空间。
13
4 改进的 CLPKC→TPKC 的异构签密方案
4.1 CLPKC→TPKC 异构签密方案的定义及安全模型
4.1.1 形式化定义
(1) CLPKC ***系统建立算法：获取安全参数 l ，选择系统主密钥 s ，得到系统密钥***
pub
P 和参数 Params
。
(2) CLPKC 部分私钥提取算法：获取用户
i
ID 、主密钥 s 和系统参数 Params ，
获取部分私钥
i D ，并将
i
D 以安全的方式发送给用户。
(3) CLPKC 私钥生成算法：获取秘密值
i x 、系统参数 Params 、部分私钥
i
ID ，
得到用户完整私钥，
i i i S x D和公钥
i
P 。
(4) TPKC 密钥提取算法：运行算法产生 TPKC系统中该用户的公私钥对
/
r r
sk pk 。
(5) 签密算法：输入消息 m 、CLPKC 系统中发送者的公私钥对 /
i i
S P 、TPKC 系统中接收方的公钥
r
pk 和系统的参数 Params ，获得消息 m 的密文 。
(6) 解签密算法：输入签密的密文 、发送者身份和公钥 /
i i ID P 和系统参数
Params 和接收者的私钥

r
sk ，输出消息 m 或者符号“⊥”。
以上的算法必须满足一致性约束，即如果 (, , , ,)
i i i r
signcr ypt m ID P Ssk，则必
有 (, , ,)
i i r
m Unsig ncrypt IDPsk成立。
4.1.2 安全模型
机密性游戏 4.1
(1) 初始阶段
F 运行“CLPKC 系统建立算法”，提供安全参数 l 和主密钥 s 和系统参数Params ，并发送给攻击者 A 。
(2) 阶段 1
① 完全私钥询问：攻击者 A提交用户身份
i
ID ，若列表中存在对应完全私钥信息，则直接返回，否则，F 运行“CLPKC 用户部分私钥生成算法”，获得对应的部分私钥
i D ；输入
i ID 和部分私钥
i
D ，运行“CLPKC 密钥生成算法” 获取完全
私钥
i
S 并返回给攻击者 A 。
14
② 解签密询问：攻击者 A提交一个密文给F ，F 获取接收方的私钥
r
sk ，
运行“解签密算法”，并返回给 A。
(3) 挑战阶段
攻击者 A决定在什么时候终止“阶段 1”，并进入“挑战阶段”。 A选择消息
0
m
和
1
m ，并且长度相同，发送方
i ID 、接收方公钥
r
pk 作为要挑战的信息，并提交
给F 。
A 首先对
i
ID 调用“CLPKC 用户部分私钥生成算法”和“CLPKC 密钥生成算法”获得发送者的私钥
i S ，然后随机选择
b 0 ,1 ，获得消息
b
m ，运行“签密算法”
得到密文
*
(, ,)
b b i r

Signcrypt m S pk，最后发送
*
b
给 A作为挑战密文。
(4) 猜测阶段
A 输出一个比特 b ，如果
'
b b，那么 A 赢得游戏。 A 的优势被定义为
'
Adv (A) | Pr[b b] 1/ 2 | ，其中
'
Pr[b b]表示
'
b b的概率。
注意：游戏 1 中的定义允许攻击者了解 CLPKC 系统主密钥s ，也允许攻击者可以获得用户的秘密值，即攻击者可以获得 CLPKC 系统中所有用户的完全私钥。即使发送者的私钥泄露，攻击者也不能从密文中获得消息，这确保了机密性的内部安全性。
定义 4.1 如果在 t 时间内没有任何多项式有界攻击者，经过
u
q 次解签密询
问至少的优势赢得游戏 4.1，那么称这个 CLPKC→TPKC 异构签密方案是
(, ,)
u
t q-IND-CLPKC -TPKC-HSC-CCA2 安全的。
不可伪造性游戏 4.2
我们必须考虑 CLPKC→TPKC 异构签密***方案在适应性选择消息攻击下具有不可伪造性。***
(1)初始阶段
C 执行"CLPKC 系统建立"算法，输入安全参数 l ，产生系统参数 Params 和主密钥s ，计算系统密钥
pub
P 。运行"TPKC 密钥生成算法"计算接收者公钥/私钥
对 (,)
r r pk sk 。发送系统参数 Params、系统密钥
pub P 、接收者公钥/私钥对 (,)
r r
pk sk 给
l
A 。
(2)攻击阶段
15
① 部分私钥询问：攻击者
l A 提交用户身份
i
ID ，若列表中存在对应部分秘密值信息，则直接返回，否则，C 运行 "CLPKC 用户部分私钥生成算法"获得
i
ID ，
对应的部分私钥
i D ，返回
i
D 给 A。
② 公钥询问：攻击者

I A 输入身份
i
ID ，若列表中存在对应公钥，则直接返
回，否则，C 运行“CLPKC 用户公钥生成算法”，获得
i ID 对应的公钥
i
P ，并返回
给
I
A 。
③ 签密询问：攻击者
I A 提交发送者的身份
i
ID 、发送者的公钥
`
i
P 、接收者
公钥
r pk 和消息
i m ，挑战者 C 首先调用“CLPKC 用户秘钥生成算法”获得
i
ID 的私
钥
i
S ，然后运行“签密算法”并返回密文
*
返回给
I
A 。
(3) 伪造阶段
攻击者
I
A 提交
* *
( )
ii r m ，I D ，P ， p k ， ，当下列两个条件成立时，则
I
A 赢得这个游戏。
①
*
对于
i P 和
r
pk 是合法的密文，即
*
(, ,)
i r
Unsignc rypt IDsk。
②
A ID 不是被
I
A 执行过秘密值询问的身份。

③ 对于
*
(, ,)
i r ID m pk 的签密询问，
I
A 没有执行过。
定义 4.2：如果在 t 时间内没有任何多项式有界攻击者，经过
pr
q 次部分私钥
询问、经过
sv q 次部分私钥询问
pk q 次公钥询问和
s
q 次签密询后，至少的优势赢
得游戏 4.2 ， 那么称这个 CLPKC→TPKC 异构签密方案是
(, , , , ,)
pr sv pk s
t q q q q-EUF-CLPKC -TPKC-HSC-CMA-I 安全的。
游戏 4.3
假定 F 为挑战者， CLPKC→TPKC 异构签密方案由三个阶段组成。
(1)初始阶段
F 运行“CLPKC 系统建立”算法，输入主密钥 s ，安全参数 k ，系统参数
Params，计算系统密钥
pub
P 。运行“TPKC 密钥生成算法”计算接收者公钥/私钥对
(,)
r r
pk sk 。 F 将发送者系统参数 Params、系统密钥 s 、接收者公钥/私钥对
(,)
r r pk sk 给
II
A 。
(2)攻击阶段
①秘密值询问：攻击者
II A 提交用户身份
i
ID ，若列表中存在对应秘密值信息，
则直接返回，否则， N 运行“CLPKC 秘密值生成算法”获得
i
x 对应的秘密值 x ，
返回 x 给
II
A 。
16
②公钥询问：攻击者
II A 输入身份
i
ID ，若列表中存在对应公钥，则直接返回，
否则，F 运行“CLPKC 用户公钥生成算法”，获得
i ID 对应的公钥
i P ，返回
i P 给

II
A 。
③签密询问：攻击者
II A 提交接收者公钥
r pk 、发送者的公钥
i
P 、发送者的身
份
i ID 、和消息
i
m ，F 首先调用“CLPKC 用户公钥生成算法”和“CLPKC 用户私钥
生成算法”获得
i ID 对应私钥
i S ，然后得到密文 (, ,)
i i r
Signcrypt m S pk给
II
A 。
(3)伪造阶段
攻击者
I
A 提交
* *
( )
Ai r m ，I D ，P ， p k ， ，当下列三个条件成立时，则
I
A 赢得这个游戏。
①
*
对于
i P 和
r
pk 是合法的密文，即
*
(, ,)
A r Unsignc rypt IDsk。②
A
ID 不
是被
I
A 执行过秘密值询问的身份。③对于
*
(, ,)
A r ID m pk 的签密询问，
I
A 没有执行过。
定义 4.3：如果在 t 时间内没有任何多项式有界攻击者，经过
sv
q 次秘密值询
问、
pk q 次公钥询问和
s

q 次签密询后，至少的优势赢得游戏 4.3，那么称这个
CLPKC→TPKC 异构签密方案是 (, , , ,)
sv pk s
t q q q-EUF-CLPKC
-TPKC-HSC-CMA-II 安全的。
4.2 具体的 CLPKC→TPKC 异构签密方案
本章方案包括以下算法：CLPKC 系统建立算法、CLPKC 部分私钥算法、
TPKC 秘钥生成算法、签密算法和解签密算法。具体算法如下：
(1)CLPKC 系统建立算法。设安全参数 k 为大素数，定义阶为 q 的群
1
G 和
2
G ，
双线性映射
1 1 2
e :G G G， 选择哈希函数
*
*
1
: 0,1
q
H Z,
* *
*
2 1 1
: 0,1 0,1
p
H G G Z,
1
*2
3
:{0,1} {0,1}
m l l
H
,
m
l 表示消息的长度，
1
l 表示群
1
G 中一个元素的比特长度。KGC 选取
*
q s Z为主秘钥，计算 , (,)
pub
P sP g P P，发布系统参数
1 2 1 2 3
, , , , , , , ,
pub
Params G G e q g P H H H，消息空间
*
M 0,1，保存主秘钥 s ，
系统密钥为

pub
P sP。
(2) CLPKC 部分私钥生成算法。KGC 计算
i 1i
Q H ID、
1
i i D P
s *Q*
,
发
送
i
D 给用户。
(3) CLPKC 用户秘钥生成算法。用户选择秘密值
*
i q
x Z，计算公钥
i i p u b i i i P x P Q P x s Q P，当用户收到部分私钥
i
D ，产生用户的完全私钥
(,)
i i i
S x D。
17
(4) TPKC 密钥生成算法。TPKC 系统中的用户选择
*
r q
x Z，计算自己的私
钥
r r sk x和公钥
r r
pk x P。
(5) 签密算法
假定 CLPKC 系统中 Alice 为发送者，其身份为
i
ID 、对应的公钥和私钥为
( )
i ii P x s Q P和 (,)
i i i S x D；TPKC 系统中的用户 Bob 为接收者，其公钥
r r sk x P和私钥
r
sk 。当 Alice 给 Bob 以签密方式发送消息 m 时，Alice 执行以下过程:
① 随机选择
*
q
u Z，计算
1
( ), ,
i u i
Q H ID R gV uP。
②
r

T upk ,
2
(|| || ||)
i i
h H m ID P R ,
1
i i ii u h u h W D P
x x s Q
。
③
3
(|| || ||) (, ,)
i i r
C m ID PW H V pkT，则消息 m 的签密密文为 C , V ,R 。
(5)解签密算法
当收到密文 C , V ,R 时，Bob 执行以下操作：
①
'
r
T x V ,
`
3
(|| || ||) (, ,)
i ir
m ID P W C H V pkT。
②
1
( )
Ai
Q H ID ,
2
(|||| ||)
ii
h h m ID P R。
③ 验证 (,)
h i
e WP g R
是否成立。
4.3 CLPKC→TPKC 异构签密具体方案安全性和效率分析
4.3.1 正确性
本方案必须满足一致性要求：接收者 Bob 可以正确地解密，密文也可以被正确验证。
(1) 正确解密：当 Bob 收到密文 C , V ,R ，可以正确的解密。
3
`
3
3
3 3
(|| || ||) (, ,)
(|| || ||) ( ) (, ,)
(|| || ||) ( ) (, ,)
(|
, ,

,
| || |
,
|)
i i r i i r r r r i i r r r i i r m ID P W C H V pk T m ID P pk pk H V pk x m ID P pk H V pk x W H V u V u m W H V ID P ux P P W
(2)正确验证。当 Bob 解密密文 C , V ,R 后，可以被正确的验证。
(,) ( ))
( )
1
(,) (,
1
(,) (( ) ,)
h h h i i i pub i i i i h u h h i i i i u u h u h e P g e D P g e P x P Q P g x x s Q u h e P x s Q P g e u h P P g g g R x s Q W
18
4.3.2 机密性
定理 4.1 在随机预言机模型下，如果 CLPKC→TPKC 异构签密方案
IND-CLPKC -TPKC-HSC-CCA2 安全性，被攻击者 A 能够以的优势攻破，那么
存在算法F 能以
3 2
(1)
2
u l H H q
q q
的优势解 CDH 问题。

指　标
疑似剽窃文字表述

1. CLPKC→TPKC 的异构签密方案
   4.1 CLPKC→TPKC 异构签密方案
2. ，若列表中存在对应完全私钥信息，则直接返回，否则，F 运行“CLPKC 用户部分私钥生成算法”，获得对应的部分私钥
   i D ；输入
   i ID 和部分私钥
   i
   D ，运行“CLPKC 密钥生成算法” 获取完全
   私钥
   i
   S 并返回给攻击者 A 。
   14
   ② 解签密询问：攻击者 A提交一个密文给F ，F
3. 注意：游戏 1 中的定义允许攻击者了解 CLPKC 系统主密钥s ，也允许攻击者可以获得用户的秘密值，即攻击者可以获得 CLPKC 系统中所有用户的完全私钥。即使发送者的私钥泄露，攻击者也不能从密文中获得消息，这确保了机密性的内部安全性。
4. 系统建立”算法，输入安全参数 l ，产生系统参数 Params 和
   主密钥s ，计算系统密钥
   pub
   P 。运行“TPKC 密钥生成算法”计算接收者公钥/私钥
   对 (,)

r r pk sk 。发送系统参数 Params、系统密钥
pub P 、接收者公钥/私钥对 (,)
r r
pk sk

5. 部分私钥询问：攻击者
I A 提交用户身份
i
ID ，若列表中存在对应部分秘密
值信息，则直接返回，否则，C 运行 “CLPKC 用户部分私钥生成算法”获得
i
ID ，
对应的部分私钥
i

6. 返回
i
D 给 A。
② 公钥询问：攻击者
I A 输入身份
i
ID ，若列表中存在对应公钥，则直接返
回，否则，C 运行“CLPKC 用户公钥生成算法”，获得
i ID 对应的公钥
i
P ，并返回
给
I
A 。
③ 签密询问：攻击者
I A 提交发送者的身份
i
ID 、发送者的公钥
`
i
P

7. 消息
i m ，挑战者 C 首先调用“CLPKC 用户秘钥生成算法”获得
i
ID 的私
钥
i
S ，然后运行“签密算法”并返回密文

8. 三个阶段组成。
(1)初始阶段
F 运行“CLPKC 系统建立”算法，输入主密钥 s ，安全参数 k ，系统参数
Params，计算系统密钥

9. 秘密值询问：攻击者
II A 提交用户身份
i
ID ，若列表中存在对应秘密值信息，
则直接返回，否则， N 运行“CLPKC 秘密值生成算法”获得
i

x 对应的秘密值 x ，

10. 输入身份
i
ID ，若列表中存在对应公钥，则直接返回，
否则，F 运行“CLPKC 用户公钥生成算法”，获得
i ID 对应的公钥
i P ，

11. 方案包括以下算法：CLPKC 系统建立算法、CLPKC 部分私钥算法、
TPKC 秘钥生成算法、签密算法和解签密算法。具体算法如下：
(1)CLPKC 系统建立算法。设安全参数

12. TPKC 密钥生成算法。TPKC 系统中的用户选择
*
r q
x Z ，计算自己的私
钥
r r sk x和公钥
r r
pk x P。

13. 当 Alice 给 Bob 以签密方式发送消息 m 时，Alice 执行以下过程:
① 随机选择
*
q
u Z ，计算
1
(

14. 正确验证。
(1) 正确解密：当 Bob 收到密文 C , V ,R ，可以正确的解密。

3. 李臣意_计算机科学与技术_硕士_第3部分

总字数：12436

相似文献列表　文字复制比：31.6%(3932)　疑似剽窃观点：(0)

1	10736_070101_2011100043_LW LW - 《学术论文联合比对库》- 2015-04-10	23.5%（2918） 是否引证：否
2	匿名CLPKC-TPKI异构签密方案 张玉磊;张灵刚;张永洁;王欢;王彩芬; - 《电子学报》- 2016-10-15	2.6%（320） 是否引证：否
3	基于双线性对的签密体制研究 李发根(导师：胡予濮) - 《西安电子科技大学博士论文》- 2007-01-01	2.3%（284） 是否引证：否
4	具有特殊性质的认证协议设计及应用研究 金春花(导师：许春香) - 《电子科技大学博士论文》- 2016-04-01	2.1%（262） 是否引证：否
5	2011124071周俊 - 《学术论文联合比对库》- 2014-05-13	1.7%（211） 是否引证：否
6	基于双线性对的高效无证书签名方案 张玉磊;王彩芬;张永洁;程文华;韩亚宁; - 《计算机应用》- 2009-05-01	1.5%（183） 是否引证：否
7	基于身份的新签密方案 王彩芬;王筱娟;郝占军; - 《计算机应用研究》- 2010-12-15	0.9%（108） 是否引证：否
8	对一类基于身份签密方案的分析及改进	0.9%（106）

	汤鹏志;陈仁群;张庆兰; -《合肥工业大学学报(自然科学版)》- 2014-08-28	是否引证：否
9	适用于物联网应用的密码体制设计与分析	0.6%（77）
	郑朝慧(导师：李发根) -《电子科技大学硕士论文》- 2016-03-29	是否引证：否
10	安全高效的基于身份的广义签密方案	0.5%（68）
	周才学;周顽;胡日新;江永和; -《计算机应用研究》- 2011-09-15	是否引证：否
11	改进的无证书混合签密方案	0.5%（61）
	周才学; -《计算机应用研究》- 2012-09-11 1	是否引证：否
12	基于证书签密的IPv6网络跨域认证协议	0.4%（48）
	张龙军;夏昂;莫天庆;赵李懿; -《计算机应用研究》- 2012-10-15	是否引证：否

原文内容　红色文字表示存在文字复制现象的内容; 绿色文字表示其中标明了引用的内容

证明：
初始阶段：F 设接收者公钥
r
pk ap，F 运行“CLPKC 系统建立算法”，输入安全参数l，产生系统参数 Params 和主密钥s 。F 发送系统参数 Params、主密
钥s 和接收者公钥
r
pk 给攻击者 A 。
1
H 询问： F 保持列表
1
(,)
i i
L ID t,初始为空。 A 询问
1
H 预言机，若
1
L 中存在询问项则直接返回，否则，F 选择
*
S ,计算
i t P ，返回
i t P 并将 (,)
i i
ID t 增加到
1
L
中。
2
H 询问： F 保持一个列表 { , , , , }
i
L m I D P R h，初始为空，
1
L 提出对
(, , ,)
i i i
m I D P R 的询问，若列表
2
L 中存在询问项， F 将 h 的值返回给 A ；否则，F

随机选择
*
q h Z,令 (, ,)
i i i ID Q D , F 将 h 返回给 A ，并将 (, , ,)
i i i
m ID P R 添加到列表
2
L 。
完全私钥询问：F 保持列表 (, , , ,)
i i i i
L ID D x P c，初始化为空。攻击者 A 提
交用户的身份
i ID ，若 L 中存在对应的元素信息，则返回 (,)
i i D x ，获得 (,)
i i i
S x D ,
然后返回
i
S 给攻击者 A 。否则， F 首先运行“CLPKC 部分私钥生成算法”，输出
部分私钥
i D ，然后运行“CLPKC 秘钥生成算法”获得用户的秘密值
i x 和公钥
i
P ，
获得用户完整私钥
i
S 。
签密询问：攻击者 A提交消息 m 和一个接收者公钥
w pk 。如果
w pk 等于
r
pk
或者不合法，则返回错误符号“⊥”，否则执行正常的签密操作，即调用“签密算法”生成并返回密文信息 (V ,C ,W)。
解签密询问：攻击者 A 提交一个密文 (V ,C ,W)给 F ，要求得到
(V ,C ,W)解密后的结果， F 执行以下操作过程：
F 在
3
L 中查找元组 (, ,)
i r V pk 满足 , (,)
r
e P pk e P 。
① 如果元组(, ,)
i r
V pk 已经存在于
3
L 中，那么返回 ωi
值作为
3
H 的结果。
② 如果
3
L 不存在相应元组，则在

3
L 中插入新的条目，新条目以
(, ,)
i r
V pk 为询问内容，然后从
3
H 值域中选择 0 ,1
lm
i
作为返回值，其中“Δ”
为 (, ,)
i r
P Vpk 为 CDH 问题的解。
19
(2) C 首先计算
1
( )
ii
Q H ID、
2
(|| || ||)
i r
h h m ID pk R，然后检查以下等式是
否成立： (,)
h r
e V pk g R
① 如果不成立，则输出错误符号“⊥”；②如果成立则进一步检查以下等式
, (,)
i r i e V pk e V ：
I 若成立，但则输出消息/签名对
,
(, , ,,)
i i i r m U P V pk 和发送者的公钥
i P 。
II 若成立，且 ，C 失败并终止。
挑战阶段
攻击者 A 决定在什么时间终止“阶段 1”同时进入“挑战阶段”。A 产生两个长
度一样的明文
0
m 与
1
m 、发送者和接收者公私钥
*
S 和
r
pk 。输出密文，C 随机选
择比特 b (0,1),并计算
b
m 在发送者私钥
*
S 和被攻击者的接收者公钥
r

pk ，返回密文
* *
(, ,)
b b r
Signcrypt m S pk。F 随机选择
*
0,1
lm
C 和
*
1
G，令
*
V bP、
*
1
( )
i i
Q H ID、
2
*
(|||| |)
ii
h h m x P R、
*
*
*
1
i r h W P
x s Q
，添加设定
* *
3
(, ,)
r
H V pk 为
* * * * *
(|| || || ||)
b
C m ID P W U,F 返回
* * * *
(C , V , R)给 A 。
猜测阶段A 输出比特
'
b ， F 忽略这个输出。
F 从
3
L 中提取一个随机的条目 (, ,)
i r V pk 或 (, , , ,,)
i i i r
m U P V pk 。
3

L 中包含
3
H q 项条目，随机选择的条目满足 (,) (,)
r
e bP pk e P 的概率为
3
1
H
q
，CDH 问题得以解决。
4.3.3 不可伪造性
定理 4.2 在随机预言模型下，假设 q-SDH 问题困难，则提出 CLPKC→TPKC 异构签密方案在适应选择消息攻击下是存在性不可伪造的，即 EUF-CLPKC -TPKC-HSC-CMA 安全的。
证明:我们构造一个算法B 利用 A解决 q-SDH 问题，保证攻击者 A能够以一定的优势攻破改方案。假设B是 q-SDH 问题的挑战者，对随机预言机
1
H 、
2
H 、
3
H 进行询问， B 的目标是根据身份
*
ID 和消息
*
M ，得到有效的签名，从而解决q-SDH 问题。
20
假设在群
1
G 上，获得 q 1元组
2
(, , , ,)
q
P aP a P a p，当作 q-SDH 问题的输入，
目标是让B 得到对
1
(c , P)
a c
,其中
*
1
,
q
a， c ， q Z P G。
首先 ， 获得生成元
`
1
P G, 依照下列步骤计算对 '
,
1
( )
i i y P

a y
, 其中
*
1 2 1 1
, '
q p
y y y Z p G
， ， 。
随机选择
*
1 2 1
,
q p
y y y Z
， ， 有展开式
1
*
0 1 1
1
( ) ( ), , ..., ,
q i q p i
f x x y c c c Z
,若
*
0 1 1
, ..., ,
q p
c c c Z
则有
1
0
( )
q i i i
f x c x
, 设
1
'
0
( ) ( )
q i i i
P c a P f a P
, 系统公钥
' '
1
1
( )
q i i i
Pub c a P aP
,a 是主密钥。B 展开
2
0
( )

( )
( )
q i i i i f x f x c x
x y
,
有
II
A ,可以计算对
'
1
(,)
i i y P
a y
。
B 设
' ' '
g e (P , P),
' '
pub
P aP， a 为系统密钥，对 B 保密，系统参数
'
1 2 1 2
(, , , , , , , ,)
pub Params G G e q P P g H H,
H
q 为
1
H 询问的最大次数。
1
H 询问：保持一个列表
1
{ }
i i L ID Q，初始为空，设
i
ID 是对
1
H 的第 i 次询
问，若
i
ID 在
1
L 列表中，返回对应
i
Q 值。否则，执行下列步骤：如果
*
i ID ID，
B 选择
* *
p
Q Z，且
*
1 2

{ , ,..., }
h q
Q Q Q Q , 将
*
Q 返回，并将 ( )
i i
ID Q 添加到表
1
L 中；
否则，从
1 2
{ , ,..., }
h q Q Q Q 中选择一个值，返回给 A 并将 ( )
i i
ID Q 添加到表
1
L 中。
2
H 询问： B 保持一个列表 { , , , , }
i
L m ID P R h，初始为空， A 提出对
(, , ,)
i i i
m I D P R的询问，若列表
2
L 中存在询问项， B 将 h 的值返回给 A ；否则， B
随机选择
*
-
q
h Z,令
2
(|| ||)
i i i h h m ID P R, B 将 h 输出给 A ，然后把 (, , ,)
i i i
m ID P R 添加到列表
2
L 。
3
H 询问：F 保持列表
3
(,, ,)
i r i i
L V pk T ,初始为空，A 询问
3
H 预言机。若存
在相应项，则直接返回结果i
；否则随机选择 0 ,1
lm
i
，返回i
给攻击者 A ，
并且将 (, , ,)

i r i
V pk 存入列表。如果
3
L 中已经存在 (, , ,)
i r i
V pk 并且有等式
(,) (,)
i r i i e V pk e P T成立，则用
i
T 来代替“Δ”。其中符号“Δ”表示 CDH 问题的一个解。
部分私钥询问：
I A 对
i ID 进行询问， B 维持列表 { , , }
i i i
E ID Q D，初始化为
空。对于身份
i
ID ， B 可以从列表
1
L 中得到元组 ( )
i i
ID Q ，如果
*
i
ID ID， B 结
21
束并返回“失败”。否则，计算
1
i i D
a Q
，返回
i D 给 A ，并将 (, ,)
i i i
ID Q D 添加到表E 。
私钥询问：当 A对
i
ID 进行询问时，如果
*
i
ID ID， B 结束并返回“失败”。
反之，L存在(, , ,)
i i i ID x P t 项、表 E 存在 (, ,)
i i i ID Q D 项，B 将 (,)
i i
x D 返回 A ；若不
存在，B 对
i ID 进行部分密钥询问和公钥询问获得 (,)
i i x D ，并将 (,)
i i
x D 返回给 A 。
公钥替换询问：当 A询问
'

(,)
i i ID P 时，若 L 中存在 (, , ,)
i i i ID x P t 项，B 将
i
P 改为
'
i
P ， t 0。并将 (, , ,)
i i i
ID x P t 添加到 L 表中。否则， B 作公钥询问获得
(, , ,)
i i i
ID x P t ，然后设置
'
i i
P P，假设 B 能够获得替换公钥
'
i
P 对应的秘密值
'
i
x ，
添加(, , ,)
i i i ID x P t 到表 (, ,)
i i i
C R V。
签名询问：若
I A 作 , , ,
i i i
m ID P R 签名询问， B 查表
1
L 和 L 获得 ,
i i
ID Q 和
, , ,
i i i
ID x P t .若
*
i
ID ID， B 终止并返回“失败”。否则，执行下列过程：若 t 1，
B 随机选择
*
i p r Z, 计算
ri i
R g， 然后查表
2
L 得到
i
h ， 计算
'
1
i i i i i i i i i r h r h V D P

x x a Q
,则签名为 (, ,)
i i i
C R V , B 返回给 A 。若 t 0, B
从 A获得
'
i
x 值。选取
*
i q r Z,计算
ri i
R g , 计算 '
1
i i i i i i i i i r h r h V D P
x x a Q
,则签
名为 (, ,)
i i i
C R V, B 返回给 A 。
最后使用分叉技术
[28]
：假设
*
ID 是 A 攻击的目标，
*
ID 的公钥是
*
i
P ，则 A 对
消息m 伪造签名为 (C , R , V)。通过重放技术，
I
A 可以获得另一个有效签名
' '
(C , R , V),且有。 和
'
满足下列等式：
' ' ' '
* * * *
'
* '
' ' 1 ( )
'
' ( ) ' * * ' ' ' '
'
' * * ' ' ' '
(,) (,) (,) (,)
(,) (, ( )) (( ) ,)
(( ) ( ),) (( ) ,)
g h g h h h ID ID ID ID h h ID pub e V P e V P e V P e V P g e V V P g e V V x P Q P e h h P P
e V V x a Q P e h h P P
这样 ， B 能够成功计算
' * * ' '

( ) ( ) ( )
i
V V x a Q h ， h有 P
' ' * ' 1
*
1
( ) ( )
i P V V x h h
a Q
成立 。 对于
*
1 2
{ , ,..., }
qh
Q Q Q Q， 输出一个对
*
*
1
(,)
i Q P
a Q
22
如果 A能够攻破本文方案，就可以获得 q-SDH 困难问题的一个解，从而出现矛盾。
4.3.4 效率分析
在表 1 中，列出了本文方案与文献[29]所需的运算量。其中，p 代表对运算。
分析表 1 可知，我们所提出的方案有更高的效率。
表 1 该文方案与其他方案所需的运算量
方案签密解签密系统参数
文献[29] 0p 2p 不相同
本方案 0p 1p 相同
4.4 本章小结
本章提出基于双线性对的从 CLPKC 到 TPKC 的异构签密方案，这个方案是基于随机预言机模型下设计的。该方案在进行签密操作的时候不需要对运算，而进行解签密操作的时候只需要一个对运算，使方案的效率有了一定的提高。
23
5 匿名 IDPKC→TPKC 异构签密方案
5.1 匿名 IDPKC→TPKC 异构签密方案定义和安全性模型
5.1.1 形式化定义
(1)IDPKC 系统建立算法。输入参数
1
1k ，输出主密钥
1
s 和系统参数
1
parmas 。
PKG 保密
1
s ，公开参数
1
parmas 。
(2)TPKC 系统建立算法。TPKC 系统中 CA（Certification authority）生成并
发布参数
2

parmas 。
(3)TPKC 密钥生成算法。该算法产生 TPKC 系统用户的私钥
2
sk 和公钥
2
pk 。
(4)IDPKC 密钥提取算法。IDPKC 系统中的用户使用这个算法获得自己的私钥。用户的公钥就是身份
1 1
pk ID，这种公钥不需要数字证书。
(5)签密算法。该算法输入系统参数
1
parmas 及
2
parmas ，发送者的私钥
1
sk 、
接收者的公钥
2
pk ，消息 m ，输出一个密文 。
(6)解签密算法。该算法输入系统参数
1
parmas 及
2
parmas ，发送者的公钥
1
pk 、
接收者的私钥
2
sk ，密文 ，输出消息 m 或者错误符号“⊥”(表示密文对于发送者和接收者是不是合法)。这些算法必须满足异构签密的一致性要求 ， 即如果
1 2
Signcrypt (sk , pk , m) ，那么
1 2
m Unsigncrypt (pk , sk ,)。
5.1.2 安全性模型
机密性游戏 5.1
初始阶段：
F 运行“IDPKC 系统建立算法”，获得参数
1
parmas 和主密钥
1
s 。 F 运行
“TPKC 秘钥生成算法”和“TPKC 系统建立算法”获得系统参数
2
parmas 和接收者的公钥
2
pk 、接收者私钥
2
sk ,发送参数
1
parmas 、

2
parmas 和接收者的公钥
2
pk 给F 。
挑战阶段
攻击者 A判断阶段 1 何时停止进入挑战阶段。产生两个长度相同
0
m 、
1
m 和发送者身份
1
ID 和接收者的公钥
2
pk 并将它们发送给 F 。F 运行“IDPKC 密钥提取
24
算法”获得发送者的私钥
1
sk ，然后随机选择一个比特 {0,1}并计算
*
1 2
Signcrypt (sk , pk , m)
。
猜测阶段A 输出一个比特 ，如果
'
，那么 A 赢得游戏。 A 的优势被定义为
'
Adv(A) Pr [ ] 1 / 2， |其中
'
Pr[ ]表示
'
的概率。
定义 5.1 如果在 t 时间内没有任何多项式有界攻击者，经过
u
q 次解签密询
问至少的优势赢得游戏 5.1，那么称这个 IDPKC→TPKC 异构签密方案是
(, ,)
u
t q-IND-CLPKC-TPKC-HSC-CCA2 安全的。
不可伪造性游戏 5.2
初始阶段：C运行“IDPKC 系统建立算法”，获得参数
1
parmas 。C 运行“TPKC
密钥生成算法”和“TPKC 系统建立算法”获得系统参数
2
parmas 和接收者公钥/私钥
2 2
(pk , sk),发送参数
1
parmas 、
2
parmas 和
2 2

(pk , sk)给 F 。
攻击阶段：F 执行以下询问：
(1)密钥提取询问: F 选择身份
1
ID ，C 运行“IDPKC 密钥提取算法”并将
1
ID
对应的私钥发送给F 。
(2)签密询问: F 提交发送者的身份
1
ID 和消息 m 给 C 。C 首先运行“IDPKC 密钥提取算法”以获得发送者的私钥
1
sk ，然后运行 “ 签密算法 ” 返回密文
1 2
Signcrypt (sk , pk , m)给F 。
伪造阶段：F 产生发送者的身份
1
ID 和新的密文 *。当满足以下两个条件时候，F 赢得这个游戏。
① *对于
1
ID 和
2
pk 是合法的密文，即 *
1 2
Unsigncrypt (ID , sk ,)不会返回错误符号“⊥”。
② 没有询问过涉及 m* 、
1
ID 和
2
pk 的签密询问。
③ 在攻击阶段没有询问过
1
ID 的私钥。
定义 5.2 如果没有任何多项式有界的敌手在t时间内，在经过
k
q 次密钥提取
询问和
s
q 次签密询问以后，以至少的优势赢得游戏 5.2，那么 IDPKC→TPKC
异构签密方案是 EUF-HSC-CMA 安全的。
匿名性游戏 5.3
初始阶段： F 运行了“TPKC 密钥生成算法”生成两个公钥和私钥，分别为
25
2,0 2,0
(pk , sk)和
2,1 2,1
(pk , sk)。我们把它作为密文的接收者，并将公钥和发送给 A 。
F 运行“IDPKC 密钥提取算法”生成两个公钥和私钥，分别为
1,0 1,0
(pk , sk)和
1,1 1,1
(pk , sk)。我们把它作为密文的发送者，并将私钥

1,0
sk 和
1,1
sk 发送给 A 。
挑战阶段：A决定在什么时间终止“阶段 1”并进入“挑战阶段”。 A输出消息
m
以及发送者的私钥
1,0
sk 和
1,1
sk 。 F 选择 c { 0 , 1c } , ' { , 0 , 并1 } 计算
, ' ,
(, ,)
U c r c
S i g n c r y p t m S , p获 k得
*
给 A作为挑战密文。
猜测阶段：A随机选择
d , d ' {0,1}
，如果(d , d ') (c , c')
，则 A赢得游戏 4.3.1
定义 A赢得游戏的优势为：
Adv (A) | Pr[(d , d ') (c , c')] 1/ 4 |
定义5.3: 如果不存在任何多项式有界攻击者以不可忽略的优势赢得游戏5.3,
则称 IDPKC→TPKC 异构签密方案在适应性选择攻击下具有密文匿名性
[30]
。
5.2 匿名 IDPKC→TPKC 异构签密方案详细描述
(1) TPKC 系统建立算法
设
T1
G 为由
2
P 生成的循环加法群，阶为
2
q ，
T2
G 为具有相同阶的循环乘法群，
1 1 2
' :
T T T
e G G G为一个双线性映射。
2
l 表示
T1
G 元素。其中
2m
l 是签密消息的长度，
2
*
2 2
，

q
a b Z。发布系统参数
1 2 2 2 22 2
{ , , , , ', , ,}
T T
Params G G q P e la b。
(2) TPKC 密钥提取算法
TPKC 系统中的用户随机选择 *
2 p
x Z，计算自己的私钥
2 2
sk x和公钥
2 2 2
pk x P。
(3) IDPKC 系统建立算法
设
1
G 由
1
P 生成循环加法群，阶为
1
q (
1
q 为
1
k
比特素数)，
2
G 为具有相同阶
1
q 循环乘法群，
1 1 2
e :G G G为一个双线性对映射。定义三个安全的 Hash函数
[31]
1
**
1
:{0,1}
q
H Z
、
1
*
2 2
:{0,1}
q
H G Z
、
1
3
H :{0,1}* {0,1}l m，其中
1m

l 是签密消息的长度，
1
l 是
1
G 元素长度。PKG 随机选择一个主密钥
1
*
1
q
s Z
，计算
pub1 1
P s P，
设
1 1
g e(P , P)，PKG 公开系统参数
1 1 2 1 1 1 1 2 3
{ , , , , , , , , , , , }
pub m
Params G G q l P P l g H H H。
(4) IDPKC 密钥提取算法
IDPKC 系统中用户提交身份
U
ID 给 PKG ， PKG 计算改用户的私钥
1 1
1 1 1
1
( )
sk P
H ID s
。
(5) 签密算法
假设发送者 Alice 属于 IDPKC 系统作为发送者，他的公钥为身份
1
ID ，私钥
26
为 1 1
1 1 1
1
( )
sk P
H ID s
；接收者 Bob 属于 TPKC 系统作为接收者，其公钥为
2 2 2
pk x P，私钥为
2 2
sk x。当 Alice 希望通过签密的方式发送消息 m 给 Bob 时，
他执行以下过程：
① 随机选择 * *
1 2
1 2
, ,

q q
r Z r Z
，计算
1
x gr
，
2 2
V r P。
② 计算
2
h H (m, x)和
1 1
W (r h) sk。
③ 计算
2 2
T r pk和
3 2 1
C H (V , pk , T) (m || ID || W || h)，则消息 m 的签密密文 (C , V)
。
(6)解签密算法：
① 计算 (C , V)
，
1 3 2
(m || ID || W || h) C H (V , pk , T')
。
② 检查等式
1 1 1
(, ( )) h pub
x e W H ID P P g 是否成立。如果成立，那么接受该
密文并返回消息m
；否则返回错误符号“⊥”。
5.3 匿名 IDPKC→TPKC 异构签密方案安全型和效率分析
5.3.1 正确性
(1)正确解密：当 Bob 收到密文 (C , V)
时候，可以正确的解密。
`
1 1 3 2
1 1 2 2 3 2 2
1 1
3 2
3 2 2 2 2 3 2 22 2
1 1
(|| || || ||) (, ,)
(|| || ||) ( ) (, ,)
(|| || ||) ( ) (, ,)
(|| |
|| , ,
|| , ,
| ||||)
m ID pk W h C H V pk T m ID pk pk pk H V pk x m ID pk pk H V pk W h H x m I V r V W h H V r x P P D kh r
pW
(2) 正确验证：当 Bob 收到解密密文 (C , V)

时候，可以通过等式
1 1 1
e(V , H (ID) P Pub) g h
1
1 1 1
1 1 1 1 1
1 1 1 1 1
1 1 1
1 1 1 1 1 1 1
1 1 1
1 1 1 1 1 1
1 1 1
1 1 1
(, ( ))
(( ) , ( ))
1
(( ) , ( ))
( )
1
(( ) , ( ))
( )
1
(( ) , (( )))
( )
(( ) ,)
h h pub h pub h h hr e V H ID P Pub g e r h sk H ID P P g e r h P H ID P P g H ID s e r h P H ID P s P g H ID s e r h P H ID s P g H ID s
e r h P P g g
27
5.3.2 机密性
定理 5.1 在随机预言模型下，如果存在一个攻击者 A能够以的优势攻破
IDPKC→TPKC 异构签密方案，那么存在一个算法F 能以
3 2
H H t
q q q
的优势解 CDH 问题。
证明：
初始阶段：C运行“IDPKC 系统建立算法”，输入安全参数
1
l ，产生系统参数
1
Parmas 和主密钥
1
s ，设
pub1 1
P s P。C 运行“TPKC 系统建立算法”和“ TPKC 秘钥生成算法”获得参数
2
Parmas 和接收者公钥私钥对
2 2
(sk , pk)， C 发送
1
Parmas 和

2
Parmas 、 挑战者身份
i
ID 和接收者公钥
2
pk 对发送给 A
。
阶段 1：C模拟游戏 1 中 A的挑战者。
1
H 维护
1
L 、
2
L 和
3
L 三张列表，分别用于跟踪 A对预言机
1
H 、
2
H 、
3
H 的询问。
2
H 询问：当 A 询问
2
(,)
i i
H m x 时，首先检查列表
2
L 是否已经存在这个询问的条目，如果存在，那么返回相同的回答；否则C 从
*
q1
Z 中随机选取
2,i
h 作为回答，
最后，将元组
2,
(, ,)
i i i
m x h 存入列表
2
L 中。
3
H 询问： C 保持列表
3 2
(, ,,)
i i i
L V pk T ,初始为空， A 询问
3
H 预言机， C 首先检查
3
L 中是否存在元组

2
, ,
i i V pk T 。若存在相应项，则直接返回结果i
；否则随
机选择 0 ,1
lm
i
，返回i
给攻击者 A，并且将
2
(, ,,)
i i
V pk 存入列表。如果
3
L
中已经存在
2
(, ,,)
i i
V pk 并且有等式
2 2
(,)(,)
i i e V pk e P T成立，则用
i
T 来代替“Δ”。其中符号“Δ”表示 CDH 问题的一个解。
签密询问：攻击者 A提交消息m 和一个接收者公钥
w pk 。如果
w
pk 等于
2
pk 或者不合法，则返回错误符号“⊥”，否则执行正常的签密操作，即调用“签密算法”
生成并返回密文信息 (V ,C)。
解签密询问：攻击者 A提交密文 (V ,C)给C ，要求得到解密后的结果，F
执行以下操作过程：
(1) C 在
3
L 中查找元组
2
(, ,)
i
V pk 满足
1 2 1
e pk , pk e (pk,)或者 。
如果元组
2
(, ,)
i
V pk 已经存在于
3
L 中，那么返回i
值作为
3

H 的结果；②如果
3
L 不存在相应元组，则在
3
L 中插入新的条目，新条目以
2
(, ,)
i
V pk 为询问内容，
然后从
3
H 值域中选择 0 ,1
lm
i
作为返回值，其中“Δ”为
2 2
(, ,)
i
P V pk为 CDH 问题的解。

指　标
疑似剽窃文字表述

1. 初始阶段：F 设接收者公钥
   r
   pk ap，F 运行“CLPKC 系统建立算法”，输入安全参数l，产生系统参数 Params 和主密钥s 。F 发送系统参数 Params、主密
   钥s 和接收者公钥
   r
   pk 给攻击者 A 。
2. 否则， F 首先运行“CLPKC 部分私钥生成算法”，输出
   部分私钥
   i D ，然后运行“CLPKC 秘钥生成算法”获得用户的秘密值
   i
3. 不可伪造性
   定理 4.2 在随机预言模型下，假设 q-SDH 问题困难，则提出 CLPKC→TPKC
   异构签密方案在适应选择消息攻击下是存在性不可伪造的，即 EUF-CLPKC
   -TPKC-HSC-CMA 安全的。
4. 设
   i
   ID 是对
   1
   H 的第 i 次询
   问，若
   i
   ID 在
   1
   L 列表中，返回对应
   i
   Q 值。否则，执行下列步骤：如果
   *

i

5. 中选择一个值，返回给 A 并将 ( )
i i
ID Q 添加到表
1
L 中。

6. IDPKC→TPKC 异构签密方案
5.1 匿名 IDPKC→TPKC 异构签密方案定义

7. TPKC 密钥生成算法。该算法产生 TPKC 系统用户的私钥
2
sk 和公钥
2
pk

8. 定义 5.2 如果没有任何多项式有界的敌手在t时间内，在经过
k
q 次密钥提取
询问和
s
q 次签密询问以后，以至少的优势赢得游戏 5.2，那么 IDPKC→TPKC
异构签密方案是

9. 发送给 A 。
挑战阶段：A决定在什么时间终止“阶段 1”并进入“挑战阶段”。 A输出消息

10. 系统建立算法
设
T1
G 为由
2
P 生成的循环加法群，阶为
2
q ，
T2
G 为具有相同阶的循环乘法群，
1 1 2
' :
T T T
e G G G为一个双线性映射。
2
l 表示
T1
G 元素。

11. TPKC 密钥提取算法
TPKC 系统中的用户随机选择 *
2 p
x Z，计算自己的私钥
2

12. IDPKC 密钥提取算法
IDPKC 系统中用户提交身份
U
ID 给 PKG ， PKG 计算改用户的私钥
1 1

1 1 1
1
(
13. Bob 属于 TPKC 系统作为接收者，其公钥为
2 2 2
pk x P，私钥为
2 2
sk x。当 Alice 希望通过签密的方式发送消息 m 给 Bob 时，
他执行
14. 证明：
初始阶段：C运行“IDPKC 系统建立算法”，输入安全参数
1
l ，产生系统参数
1
Parmas 和主密钥
1
s

4. 李臣意_计算机科学与技术_硕士_第4部分

总字数：6572

相似文献列表　文字复制比：24.1%(1581)　疑似剽窃观点：(0)

1	10736_070101_2011100043_LW LW - 《学术论文联合比对库》- 2015-04-10	9.6%（631） 是否引证：否
2	影子银行对货币政策传导机制影响研究 陈迪(导师：胡定核;高云峰) - 《西南大学硕士论文》- 2016-05-25	4.3%（285） 是否引证：否
3	麦冬主要活性成分对OATP1B1、OATP1B3转运功能的影响及其机制研究 陈琳(导师：夏春华) - 《南昌大学硕士论文》- 2016-05-01	4.2%（274） 是否引证：否
4	企业慈善行为的可持续性研究 孙杰(导师：赵庆波) - 《长春工业大学硕士论文》- 2011-04-01	4.0%（266） 是否引证：否
5	具有特殊性质的认证协议设计及应用研究 金春花(导师：许春香) - 《电子科技大学博士论文》- 2016-04-01	3.9%（254） 是否引证：否
6	马克思主义城乡一体化理论视域下的乡村旅游发展研究 张静(导师：冯继康) - 《曲阜师范大学硕士论文》- 2016-03-10	3.9%（254） 是否引证：否
7	外源NO对盐胁迫下番茄光合碳同化的影响 王松(导师：刘慧英) - 《石河子大学硕士论文》- 2016-06-01	3.9%（254） 是否引证：否
8	人际冷漠维度探索 徐菲(导师：周宁) - 《云南师范大学硕士论文》- 2016-04-06	3.9%（254） 是否引证：否
9	果洛州乡镇级公路雪灾风险探讨 刘钊(导师：侯光良) - 《青海师范大学硕士论文》- 2016-04-01	3.8%（250） 是否引证：否
10	BiOX(X=Cl、Br)纳米片复合薄膜的构筑及光催化性能研究 巩祥庚(导师：陆军) - 《北京化工大学硕士论文》- 2016-04-20	3.8%（250） 是否引证：否
11	全方位移动AGV智能控制技术研究 杨天旭(导师：楼佩煌) - 《南京航空航天大学硕士论文》- 2016-03-01	3.8%（250） 是否引证：否
12	粉虱寄生蜂体内卵子发育的自主调控研究	3.8%（247）

	张超然(导师：臧连生) -《吉林农业大学硕士论文》- 2016-05-01	是否引证：否
13	苗期低温对烟草BR信号通路关键基因表达及发育进程的影响	3.7%（243）
	肖立增(导师：戴秀梅) -《西南大学硕士论文》- 2016-04-20	是否引证：否
14	水稻核心种质糖分含量全基因组关联分析	3.6%（237）
	许久月(导师：王功伟) -《华中农业大学硕士论文》- 2016-06-01	是否引证：否
15	社会治理视阈下的生态文明建设研究	3.6%（237）
	张小群(导师：熊洁) -《西南大学硕士论文》- 2016-04-15	是否引证：否
16	温州市瓯海区农村公路建设现状及对策研究	3.1%（203）
	吴茫茫(导师：胡水秀;张丙宣) -《江西农业大学硕士论文》- 2016-05-01	是否引证：否
17	土地覆盖多尺度遥感分类研究	2.8%（184）
	高文杰(导师：王金亮) -《云南师范大学硕士论文》- 2016-06-01	是否引证：否
18	优酷并购土豆的协同效应分析	2.8%（184）
	汤兴华(导师：戴新民;陈俊) -《安徽工业大学硕士论文》- 2016-06-01	是否引证：否
19	Au催化剂界面现象对乙炔氢氯化反应催化作用机制研究	2.2%（145）
	印雪(导师：朱明远) -《石河子大学硕士论文》- 2016-06-01	是否引证：否
20	邻苯二甲酸二乙基已酯（DEHP）及代谢产物邻苯二酸—单-2-乙基已酯（MEHP）对幼鼠生精功能损害机制的研究	1.9%（127）
	李静(导师：马洪) -《遵义医学院硕士论文》- 2011-05-03	是否引证：否
21	刘海龙_计算机技术_硕士	1.9%（123）
	-《学术论文联合比对库》- 2015-04-14	是否引证：否
22	高效的可撤销无证书签名方案	1.7%（111）
	张玉磊;李臣意;周冬瑞;王彩芬; -《计算机工程》- 2015-07-15	是否引证：是
23	芳基吲哚衍生物以及吲哚基吡唑啉的合成研究及应用	1.3%（84）
	封小龙(导师：张应鹏) -《兰州理工大学硕士论文》- 2016-04-01	是否引证：否
24	花岗岩崩岗集水坡面土壤水分状况研究	1.3%（84）
	倪晨(导师：陈家宙) -《华中农业大学硕士论文》- 2016-06-01	是否引证：否
25	氮沉降对桑树冠层持水及氮磷截留的影响	1.2%（81）
	王月红(导师：谢德体) -《西南大学硕士论文》- 2016-04-10	是否引证：否
26	签密体制的设计与安全性分析	1.2%（79）
	钟笛(导师：李发根) -《电子科技大学硕士论文》- 2013-03-18	是否引证：否
27	双弧脉冲MIG焊方法及控制系统研究设计	1.2%（77）
	孙百才(导师：张立华;卢立晖) -《曲阜师范大学硕士论文》- 2016-03-24	是否引证：否
28	不同处理对牛板筋品质的影响及其休闲食品的研制	1.2%（77）
	霍俊侃(导师：吴晓光) -《吉林农业大学硕士论文》- 2016-05-01	是否引证：否
29	不同农产品质量安全规制体系研究	0.4%（29）
	杨建辉(导师：任建兰) -《山东师范大学博士论文》- 2016-04-05	是否引证：否

原文内容　红色文字表示存在文字复制现象的内容; 绿色文字表示其中标明了引用的内容

(2) C 首先计算
1 1
1 1 1
1
( )
sk P
H ID s
、
i2 2
V r P，然后检查以下等式是否成立：
1 1 1
(, ( )) h pub x e W H ID P P g I 如果不成立，则输出错误符号“⊥”；
II 如果成立则进一步检查以下等式;
2
, (,)
i i
e V pk e V 。
①若成立，但 ，则输出消息/签名对
,
(, , ,)
i i r m P V pk 和发送者的公钥
i
P 。
②若成立，且 ，C失败并终止。
挑战阶段
攻击者 A决定什么时候结束“阶段 1”并进入“挑战阶段”。 A生成两个相同长度的明文
0
m 与
1
m 、发送者私钥
*
S 和接收者公钥
r
pk 请求 F 返回挑战密文， C 随机选择比特 b (0,1),并计算
b
m 在发送者私钥
*
S 和被攻击者的接收者公钥
r
pk ，返回密文
* *
2
(, ,)
b b
Signcrypt m S pk。 F 随机选择
2
*
0,1
l m
C 和

*
T1
G、 *
1
q1
r Z ,
令
*
2
V bP、
*
1
( )
i i
Q H ID、 *
2
(,)
i
h H m x、 *
1 1
*
1
1
( )
i W r h P
Q s
， 添加设定
* *
3
(, ,)
r
H V pk 为
* * * *
(|| || ||)
b
C m ID h W,F 返回
* * *
(C ,V)给 A 。
猜测阶段A 选择一个比特
'
，F 忽略这个输出。
F 从
3
L 中提取一个随机的条目 (, ,)
i r
V pk 。
3
L 中包含
3
H
q 项条目，随机选择的条目满足
1 2 1

e (pk , pk) e (pk,)的概率为
3
1
H
q
，并且 CDH 问题得以解决。
5.3.3 不可伪造性
定理 5.2 在随机预言模型中，若存在一个敌手 F 能够在 t 时间内，以
2
10(1)( ) / 2
k s s
q q qH的优势解决游戏 5.2，则存在一个算法 C ，能够在
1 2
' 2
( )
120686 ( )
(1 1/ 2)(1 / 2)
s p H H m k k t O q t t q q O n t
n
时间内解决 n-SBDH 问题。
证明：
为了签密一个消息m
，生成的元组
1 2
(, h,)
对应着三阶段诚实验证者零知识认证协议
[31]
。
1
x
是证明者的承诺，
2
h H (m, x)
是根据消息m
和
1
计算得
29
到的 Hash 中，
2
W
是根据
1
、h和私钥
1
sk 的回答。
下面显示C可以给F 提供一个完美的模拟并通过与F
的交互来解决 n-SDH
问题。C输入
2
1 1 1
(, , ,...)

n
P P P，目的在与找到一个对
1
1
(, P)
。
初始阶段：C随机选择
1
，… ，
1
，
1
，
*
n p
Z
。与文献
[14]
相同，C 使用的输入
2
1 1 1
(, , ,...)
n
P P P计算一个生成元
1 1
Q G
和
1 1
，
pub
Q Q G
以至于它知
道 n 1对
1
1
(,)
i i i
V Q
， i {1,..., n 1}
为了获得这样的元素，C 展开多项式:
1 1
10
( ) ( )
n n j i j ij
f z z c z
生成元
1
Q 和元素
pub
Q 可以分别通过
1
1 1 1

0
( ) ( )
n j j j
Q c P f P
和
1 1 1
1
( ) ( )
n j pub j j
Q c P f Q 得到。同时(,)
i i
V
可以通过
2
0
( )
( )
n j i j j i f z f z d z
z
并计算
2
1 1 1
0
( )
( ) ( )
n j i j i j i f
V d P f P P
1
1
i
Q 得到。PKG 的公钥设为
pub Q ，相应的私钥为C 将系统参数[包括
1
Q 、
pub1
Q Q
和
1 1
g e (Q , Q)
]发送给 F 。同时 C 运行
“IDPKC 系统建立算法”产生系统参数
1
Parmas ，设
pub1 1
P s P。 C 运行“TPKC 系统建立算法”和“ TPKC 密钥生成算法”获得参数
2
Parmas 和接收者公私钥对
2 2
(pk , sk)， C 发送
1
Parmas 和
2

Parmas 挑战者身份
i
ID 和接收者公私钥
2 2
(pk , sk)
对发送给F
。
攻击阶段：C模拟游戏 5.2 中 F 的挑战者。C 维护
1
L 、
2
L 、
3
L 三张列表，
分别用于跟踪F 对预言机
1
H 、
2
H 、
3
H 的询问。这里假设每次
1
H 询问是不同的，
目标身份
1
ID 在某个时候被询问过
1
H 和身份
1
ID 在被使用到其它询问之前已经询问过
1
H 预言机。
2
H 询问：当 A 询问
2
(,)
i i
H m x 时，首先检查列表
2
L 是否已经存在这个询问的条目，如果存在，那么返回相同的回答；否则C 从
*
q1
Z 中随机选取
2,i
h 作为回答，
最后，将元组
2,
(, ,)
i i i
m x h 存入列表
2
L 中。

3
H 询问：当 F 询问 m 时，初始化为空，C 首先检查列表
3
L 是否已经存在元组
2
(, ,)
i i V pk T ，如果存在，那么直接返回结果i
；否则，随机选择C 从 {0,1}
m l
i
30
并返回i
给攻击者F ，并将
2
(, , ,)
i i
V pk
存入
3
L 中。
密钥提取询问：当F 询问
i ID 的私钥时，如果
i1
ID ID
，那么C 失败并停止；
否则C知道
1
( )
i i
H ID
，并返回
1
1
i i
W Q
给F 。
签密询问：
m 提交发送者的身份
i ID 和消息 m 给 C 。如果
i1
ID ID
，那么C 知
道发送者的私钥
i i
S V
，可以按照正常的签密步骤来询问。如果
i1
ID ID
，那么C 执行下列的步骤：
① 随机选择
1
*

,
q
h Z
② 计算
2 2
pk sk和
i2 2
V r P
③ 计算 '
B i
T x V
④
1 3 2
(|| || ||) (, , ')
i
m ID W h C H V pk T
⑤ 计算
2 i
T r V
⑥ 计算
3 2 1
C H (V , pk , T) (m || ID || W || h)
⑦ 返回密文 (C , V)
给F 。
伪造阶段：接下来，将发送者身份 F 和消息m
接合在一起，变成一个推广的伪造消息
1
(ID , m)，其目的在游戏 5.2 中隐藏其基于身份的特征。
由分叉引理
[32]
可得，如果 F 上述交互中是一个有效的伪造者，那么可以构造一个算法
'
F 。
'
F 可以输出同样承诺 x 的两个签名，即
1
((I D , m), h ,W)和
1
((ID , m) , h ', W ')，这里 h h'。
最后为了解决 n-SDH 问题，这里构造如下算法。
① C通过运行 F '得到两个不同的签名
1
((ID , m), h, W)和
1
((ID , m) , h ', W ')。
② C计算
* ' 1 '
D (h h) (W W)
1 1
1 ( )
A A f
Q P

。
③ C 使用长除法将多项式 f 写为
1
( ) ( ) ( )
A
f z z z
，这里 ，
2
0
( )
n i i i
z z
和
*
1 q1
Z
。
( )
A f z
z
可以写为
1
( )
( )
A A f z z
z z
2
1
0
n i i i A z
z
。这样C就可以计算
2
*
1 1
0
1
1 1
[( )]
n i i i A
P D P
。
③ C输出
1
1
(,)
A A
P
作为 n-SDH 问题的解。
根据分叉引理，如果F 能够在t
时间内，以
2

10(1)( ) / 2
k s s
q q qH的优势
31
解决游戏 3.2.1，那么 C 能够在
1 2
' 2
( )
120686 ( )
(1 1/ 2)(1 / 2)
s p H H m k k t O q t t q q O n t
n
时间内解决 n-SBDHP 问题。
5.3.4 效率分析
在表 1 中，列出了该文方案与文章[33]中所需要的***运算量，其中***
p
表示对运
算，
e
表示幂运算。
表 1 本文方案与其他方案所需要的运算量
5.4 本章小结
本章所提出的 IDPKC→TPKC 异构签密方案不仅保证在安全通信过程中信
息的机密性和不可伪造性；其次，与文献[20]相比效率有了一定的提高；最后，
方案中 IDPKC 和 TPKC 密码环境中使用了不同的系统参数，从而更加有效的模拟了实际的应用场景；同时方案实现了通信过程中的匿名性。
方案签密解签密系统参数匿名性
文献[20] 0p+1e 2p+1e 相同不满足
本文方案 0p+1e 1p+1e 不相同满足
32
6 总结与展望
6.1 总结
密码学是信息安全的核心。大部分发送方或者接收方都是在相同的密码环境进行通信(即同构密码环境)
[34]
。在现实生活中，不同的应用场景，所采用的密码环境是不一样的，如果要在采用不同密码环境的系统之间进行安全通信，就需要
支持异构通信的签密体制。本文针对以上问题，在下面 3 个方面做了初步研究:
(1) 高效的 TPKC→IDPKC 的异构签密方案:在已有 Sun 等人方案的基础上提
出一种高效的异构签密方案，适应于 TPKC 和 IDPKC 两种不同的密码环境，进行安全通信。
(2) 基于双线性对 CLPKC→TPKC 的异构签密方案：该方案的优点是在进行
签密操作的时候不需要对运算，而进行解签密操作的时候只需要一个对运算，效率有了较大的提高；其次，该方案具有“密钥隐私”
[35]
的特性，即解密时候，不需要知道发送者 Alice 的公钥，这样，隐藏了发送者的身份信息，实现了发送者身份的匿名。
(3) 匿名 IDPKC→TPKC 异构签密方案：以上所提出的两种方案，虽然在效
率上有了一定的提高，同时安全性有了很大的改进，相对于以前的方案，但是仍然存在一定的不足，不同密码环境所采用的参数是一样的，不能更好的模拟现实的应用场景。因此，提出了一个匿名的异构签密方案，不仅在 IDPKC 和 TPKC
密码环境中采用了不同的系统参数，更好的模拟现实的应用场景；而且该方案实现了密文的匿名性，并且满足签密过程中的内部安全性
[36]
，从而保护了发送方和接收方的隐私；同时在效率上有了很大的提高。
6.2 展望

(1) 本文所提出的异构签密方案，不仅在效率有了一定的提高，而且，在安
全性方面有了很大的改进，更重要的是在不同密码体制之间所采用的参数都是相同的，满足不同实际应用场景的需求。
(2)随着 5G 异构网络、大数据的推广，异构密码环境将逐渐普遍。未来工作
可能设计标准模型
[37]
下安全的异构签密，或者设计处具有特殊性质的异构签密，
门限异构签密
[38]
、代理异构签密体制
[39]
、盲异构签密体制
[40]
、环异构签密体制
[41]
等。还可以将异构签密应用于异构网络中，如云计算
[42]
和物联网
[43]
等领域。
33

7 参考文献

[1]Wei G, Shao J, Xiang Y, et al. Obtain confidentiality or authenticity in big data by id-based generalized signcryption[J]. information sciences, 2014, 318(C):111-122.
[2]Tong D, Liu X, Guo T, et al. Analysis and practice of cloud computing Information Security[J]. telecommunications science, 2013.
[3]张雪菲. 异构协作网络的无线定位研究[D]. 北京邮电大学, 2015.
[4]Fu X, Li X, Liu W. IDPKC-to-TPKC construction of multi-receiver signcryption[C]// international conference on intelligent NETWORKING and collaborative systems. IEEE computer society, 2013:335-339.
[5] Lu X, Wen Q, Li W, et al. A fuzzy identity-based signcryption scheme from lattices[J]. ksii transactions on internet & information systems, 2014, 8(11):4203-4225.
[6] 马冰. 基于 PKI 体系和 IBC 认证技术跨云认证研究[D]. 沈阳理工大学， 2015.
[7]Rathfelder C, Becker S, Krogmann K, et al. Workload-aware system monitoring using performance predictions applied to a large-scale e-mail system[C]// joint working IEEE conference on Software Architecture and European conference on Software Srchitecture. IEEE computer society, 2012:31-40.
[8]Kim I T, Hwang S O. An efficient identity-based broadcast signcryption scheme for wireless sensor networks[C]// international symposium on wireless and pervasive computing. IEEE xplore, 2011:1-6.
[9] 刘景伟，张俐欢， 孙蓉. 异构系统下的双向签密方案[J]. 电子与信息学， 2016,38(11):2948-2953.
[10] Xin L, Lei W. Fully anonymous multi-service subscription system without random oracles[J]. journal of computer applications, 2013, 33(2):417-422.
[11] Dan B, Boyen X. Efficient selective-id secure identity-based encryption without random oracles[M]// Advances in Cryptology - EUROCRYPT 2004. Springer Berlin Heidelberg, 2004:223-238.
[12]Dan B, Boyen X. Short signatures without random oracles[M]// Advances in Cryptology EUROCRYPT 2004. Springer Berlin Heidelberg, 2004:56-73.
34
[13] Al-Riyami S S, Paterson K G. Certificateless public key cryptography[M]//

Advances in Cryptology - ASIACRYPT 2003. Springer Berlin Heidelberg, 2003:452-473.
[14] Baek J, Safavi-Naini R, Susilo W. Certificateless public key encryption without pairing[C]//international conference on information security. springer-verlag, 2005:134-148.
[15] Sun Y, Zhang F, Baek J. Strongly secure certificateless public key encryption without pairing[C]// international conference on cryptology and network security. springer-verlag, 2007:194-208.
[16] Liu Z, Hu Y, Zhang X, et al. Certificateless signcryption scheme in the standard model[J]. information sciences, 2010, 180(3):452-464.
[17] Sun Y X, Li H. Efficient signcryption between TPKI and IDPKC and its multi-receiver construction[J]. Science China Information Sciences, 2010, 53(3): 557-566.
[18] Huang Q, Wong D S, Yang G. Heterogeneous signcryption with key privacy[J]. computer journal, 2011, 54(4):525-536.
[19] Fu X, Li X, Liu W. IDPKC-to-TPKC Construction of multi-receiver signcryption[C]// international conference on intelligent NETWORKING and Collaborative Systems. IEEE Computer Society, 2013:335-339.
[20] Li F, Zhang H, Takagi T. Efficient signcryption for heterogeneous systems[J]. IEEE systems journal, 2013, 7(3):420-429.
[21] 曹珍富. 密码学的新发展[J]. 四川大学学报:工程科学版， 2015， 47(1):1-12.
[22] Liu J, Zhang L, Rong S. Mutual Signcryption schemes under heterogeneous systems[J]. journal of electronics & information technology, 2016.
[23] Shor P W. Polynomial-Time Algorithms for prime factorization and discrete logarithms on a quantum computer[J]. SIAM Journal on Computing, 1997, 26(5):1484-1509.
[24] Zhang J, Gao S, Chen H, et al. A novel id-based anonymous signcryption scheme[C]// Advances in data and web management, Joint International Conferences, WAIM 2009, Suzhou, China, April 2-4, 2009, Proceedings. DBLP, 2009:604-610.
[25]Baek J, Steinfeld R, Zheng Y. Formal proofs for the security of signcryption[C]// international workshop on practice and theory in public key
35
cryptosystems: Public Key Cryptography. Springer-Verlag, 2007:80-98.
[26] 李臣意， 张玉磊， 张永洁，等. 高效的 TPKC→IDPKC 的异构签密方案[J]. 计算机工程与应用，2016.
[27]Boneh D, Franklin M K. Identity-based encryption from the weil pairing[C]// international cryptology conference on Advances in cryptology. Springer-Verlag, 2001:213-229.
[28]Pointcheval D, Stern J. Security Arguments for Digital Signatures and Blind Signatures[J]. Journal of Cryptology, 2000, 13(3):361-396.
[29] 张玉磊， 张灵刚， 张永洁，等. 匿名 CLPKC-TPKI 异构签密方案[J]. 电子学报，, 2016, 44(10):2432-2439.
[30] Seo J H, Kobayashi T, Ohkubo M, et al. Anonymous hierarchical identity-based encryption with constant size ciphertexts[C]// public Key cryptography - PKC 2009, international conference on practice and theory in public key cryptography, irvine, ca, usa, march 18-20, 2009. Proceedings. DBLP, 2009:215-234.
[31]王晓峰, 王尚平, 张璟,等. 零知识证明的前向安全不可否认数字签名方案[J]. 计算机工程, 2007, 33(8):27-29.
[32] Barreto P S L M, Libert B, Mccullagh N, et al. Efficient and Provably-Secure Identity-Based Signatures and Signcryption from Bilinear Maps[J]. Lecture Notes in Computer Science, 2005, 3788:515--532.
[33] Li F G, Shirase M, Takagi T. Efficient multi-pkg id-based signcryption for ad hoc networks[M]// information security and cryptology. Springer-Verlag,

2009:289-304.
[34] 左黎明， 陈仁群， 郭红丽. 可证安全的基于身份的签密方案[J]. 计算机应用，2015, 35(3):712-716.
[35] 何巍，习军. 基于双线性对的前向安全无证书签名技术研究[J]. 计算机应用与软件， 2013，30(4):323-325.
[36] Xiong H, Li F, Qin Z. Certificateless threshold signature secure in the standard model[J]. Information Sciences, 2013, 237(13):73-81.
[37]Yan J, Wang L, Wang L, et al. Efficient lattice-based signcryption in standard model[J]. mathematical problems in engineering, 2013, 2013(11):1-18.
[38] Xiu Hua L U, Wen Q Y, Wang L C. A lattice-based heterogeneous signcryption[J].
36
journal of university of electronic science & technology of china, 2016.
[39] Xiu-Hua L U, Wen Q Y, Wang L C. A lattice-based heterogeneous signcryption[J]. journal of university of electronic science & technology of china, 2016.
[40] Ullah R, Nizamuddin, Umar A I, et al. Blind signcryption scheme based on elliptic curves[C]// conference on information assurance and cyber security. 2014:51-54.
[41]Hagras E A A A, Aly H H, Elsaied D. An efficient key management scheme based on elliptic curve signcryption for heterogeneous wireless sensor networks [M]// An efficient key management scheme based on elliptic curve signcryption for heterogeneous wireless sensor networks. UCST. 2013:1-9.
[42] 冯登国， 张敏， 张妍，等. 云计算安全研究[J]. 软件学报,2011， 22(1):71-83.
[43]周宣武， 付燕,金志刚，等. 基于椭圆曲线签密的物联网安全通信方案[J]. 微电子学与计算机， 2014(11):23-26.
[44]Li C K, Yang G, Wong D S, et al. An efficient signcryption scheme with key privacy and its extension to ring signcryption[J]. journal of computer security, 2010, 18(3):451-473.

37

攻读硕士学位期间发表的论文

1.发表的学术论文

[1] 张玉磊，李臣意，王彩芬，等. 无证书聚合签名方案的安全性分析和改进[J]. 电子与信息学报， 2015， 37(8):1994-1999.

[2] ***张玉磊， 李臣意，周冬瑞，等. 高效的可撤销无证书签名方案[J]. 计算机工程，2015， 41(7):157-162.***

[3] 张玉磊，王欢， 李臣意，等. 可证安全的紧致无证书聚合签密方案[J]. 电子与信息学报，2015， 37(12):2838-2844.

[4] 张玉磊， 周冬瑞， 李臣意，等. 高效的无证书广义指定验证者聚合签名方案[J]. 通信学报，2015， 36(2):48-55.

[5] 李臣意 ，张玉磊 ，张永洁，王彩芬.《高效的 TPKC→IDPKC 的异构签密方案.计算机工程与应用，2017.11(已经录用)

2.参与项目

[1] 参与甘肃省高等学校科研项目“医疗云电子健康档案 HER 平台签密方案研究”(2015B-220)。

[2] 参与甘肃省高等学校科研项目“车联网系统中身份认证与隐私保护的关键问题研究”(2013A-014)。

[3] 参与甘肃省杰出青年基金项目***“基于网络信任体系的电子政务数据安全交换平台的研究与实现”***(145RJDA325)。

[4] 参与兰州市科技计划基金项目“面向信息化公共服务平台的跨域身份认证系统的研究与实现”(2013-4-22)。

38

致谢

转眼间，三年的研究生生活就要结束了，而入学仿佛是昨天的事情，初来乍到时的场景犹历历在目。回忆起这三年的点点滴滴，感慨不已，欣慰之余而又感到庆幸无比。值得欣慰的是，我这三年的时间学到了许多受益无穷的东西；庆幸的是我来到了一个很好的环境，遇到了很多良师益友，给我了很多的指引和帮助，

使我能够顺利地完成学业，在此谨向他们表示中心的感谢首先感谢导师张玉磊副教授，论文定题到写作定稿，倾注了张老师大量的心血。在我攻读硕士研究生期间，深深受益于张老师的关心、爱护和敦敦教诲教导。

他作为老师，指点迷津，让人如沐春风；作为长辈，关怀备至，让人感念至深。

能师从张老师，我为自己感到庆幸。再次谨向张老师表示我最诚挚的敬意和感谢。

感谢王彩芬教授、杨小东副教授、牛淑芬副教授、曹素珍副教授和李亚红师姐等给我的指导、关心和帮助。

感谢我的同窗好友李亚楠、高国娟、邓云霞、康步荣等，感谢他们对我学习和工作中的帮助。感谢各位师弟师妹们，创造了欢乐、和谐的学习环境，促进我们彼此间的交流，使我受益匪浅，在此致以诚挚的谢意。

感谢我的父母，感谢我的兄弟姐妹，我知道如果没有他们的支持就没有我的今天，我也知道我永远无法完全回报他们的爱，所以我希望顺利完成学业，争取更大的成功，给他们一点欣慰。

作者李臣意

2017 年月日

指　标

疑似剽窃文字表述

1. ②若成立，且 ，C失败并终止。
   挑战阶段
   攻击者 A决定什么时候结束“阶段 1”并进入“挑战阶段”。
2. 询问过
   1
   H 和身份
   1
   ID 在被使用到其它询问之前已经询问过
   1
   H 预言机。
3. 致谢
   转眼间，三年的研究生生活就要结束了，而入学仿佛是昨天的事情，初来乍到时的场景犹历历在目。回忆起这三年的点点滴滴，感慨不已，欣慰之余而又感到庆幸无比。值得欣慰的是，我这三年的时间学到了许多受益无穷的东西；庆幸的是我来到了一个很好的环境，遇到了很多良师益友，给我了很多的指引和帮助，
   使我能够顺利地完成学业，在此谨向他们表示中心的感谢首先感谢导师张玉磊副教授，
4. 感谢我的父母，感谢我的兄弟姐妹，我知道如果没有他们的支持就没有我的今天，我也知道我永远无法完全回报他们的爱，所以我希望顺利完成学业，争取更大的成功，给他们一点欣慰。
   作者李臣意
   2017 年月日