doi:10.3969/j.issn.1000-436x.2014.z2.014

针对服务器安全的指定验证者可搜索公钥加密

邵志毅[1]，杨波[1]，吴振强[1]，张明武[2]
（1. 陕西师范大学 计算机科学学院，陕西 西安 710062；2. 湖北工业大学 计算机学院，湖北 武汉 430068）

摘 要：在指定验证者的可搜索公钥加密(dPEKS)中，提出 IND-KGA-SERVER 安全模型，形式化描述针对服务器的安全。基于 IND-KGA 安全的 dPEKS、数字证书授权中心 CA、以及强不可伪造和不可否认的签名，在攻击者是服务器的情况下构造出抗 KG(keyword guessing)攻击的 dPEKS 方案。方案是从 IND-KGA 安全到 IND-KGA-SERVER 安全的编译器。

关键词：可搜索加密；关键字猜测攻击；指定验证者；IND-KGA 安全
中图分类号：TP309 **文献标识码**：A **文章编号**：1000-436X(2014)Z2-0106-06

Searchable public key encryption with designated verifier secure against the server

SHAO Zhi-yi[1], YANG Bo[1], WU Zhen-qiang[1], ZHANG Ming-wu[2]
(1. School of Computer Science, Shaanxi Normal University, Xi'an 710062, China;
2. College of Computer Science and Engineering, Hubei University of Technology, Wuhan 430068, China)

Abstract: In designated verifier searchable public key encryption (dPEKS) schemes, the IND-KGA-SERVER security was proposed to formalize the security against the server. Based on the IND-KGA secure dPEKS, the CA (certificate authority), and the strongly unforgeable and undeniable signature, the solution was proposed to show how to construct dPEKS schemes which are secure against KG (keyword guessing) attacks when the attacker is the server. The solution is a bootstrap from IND-KGA secure to IND-KGA-SERVER secure.

Key words: searchable encryption; keyword guessing attacks; designated verifier; IND-KGA security

1 引言

带关键字搜索的公钥加密(PEKS, public key encryption with keyword search)由 Boneh 等首次提出[1]，也称为可搜索公钥加密。该类方案中，邮件发送者通过邮件服务器给接收者发送邮件。邮件内容可使用普通公钥方案加密。为了服务器能代替接收者对邮件搜索以便找出包含某关键字的邮件，且防止服务器得知关键字，发送者用可搜索公钥加密对邮件关键字加密。服务器则使用接收者提供的关键字陷门代其完成搜索。

PEKS 的基本安全要求是，攻击者在可获得任何关键字陷门的情况下，仍然无法区分哪个 PEKS 密文和哪个关键字相关。所谓相关，是指由同一关键字生成。这是从语义安全角度的描述，被称为 IND-CKA (indistinguishability against the chosen keyword attack)安全，由 Boneh 等提出[1]。

然而，PEKS 要求在服务器和接收者之间存在安全信道。为取消该依赖，Baek 等[2]提出 dPEKS (designated tester PEKS)，也称为指定验证者的可搜索公钥加密。在 dPEKS 中，仅拥有相应秘密钥的服务器才能进行测试，从而判断 dPEKS 密文和给

收稿日期：2014-06-23
基金项目：国家自然科学基金资助项目 (61272436,61272404,61173190,61402275); 广东省自然科学基金资助项目 (10351806001000000)
Foundation Items: The National Natural Science Foundation of China (61272436,61272404,61173190,61402275); The Natural Science Foundation of Guangdong Province (10351806001000000)

定关键字陷门的相关性。但该安全无法阻止攻击者通过猜测得知关键字。

最近，Byun 等[3]证明了 dPEKS 方案中攻击者可通过离线关键字猜测攻击(KG attack, offline keyword guessing attack)猜出陷门对应的关键字。原因是关键字常取自较小空间，因此熵较小。攻击者遍历关键字空间，通过测试哪个关键字能和陷门满足某一特定关系，便可猜出陷门对应的关键字。Byun 等证明了敌手在该攻击中的成功概率不可忽略，这激发了研究者寻找解决 KG 攻击的方法。其中，Rhee 等[4, 5]引入陷门不可区分性(trapdoor indistinguishability)并证明其是抵抗 KG 攻击的充分条件。然而，Rhee 等的方案[5]在随机寓言机模型下运行，且在他们的安全模型中攻击者无法进行测试询问，这限制了攻击者的能力。

Fang 等[6]对 Rhee 的安全模型进行改进，提出 IND-KGA(indistinguishability against keyword guessing attack)安全，该安全模型扩充了攻击者的能力。Fang 等还在标准模型中构造了 IND-KGA 安全的 dPEKS，保证了外部攻击者(非服务器和接收者)无法通过 KG 攻击[3]从关键字陷门中猜出关键字。

Fang 的方案具有很强的安全性。然而，不管是他们的或前人的方案[1~11]，都没有解决攻击者是服务器的安全问题。

Boneh 等以可搜索公钥加密中陷门的安全为出发点，提出了函数保密（function-privacy）的问题，使得可搜索加密中的陷门泄漏更少的信息[12,13]。但他们是从陷门自身构造的角度去减少信息泄漏，并未指出在攻击者拥有测试能力的情况下如何保证攻击者无法利用关键字猜测攻击的方式猜出关键字。

本文首次在 IND-KGA 安全的 dPEKS 方案中，提出针对服务器的安全模型，即 IND-KGA-SERVER 安全，这是抵抗 KG 攻击的必要组成。文章基于公钥基础设施中数字证书授权中心的存在性以及强不可伪造和不可否认签名的存在性，给出构造 IND-KGA-SERVER 安全 dPEKS 的方法。方案独立于具体的 dPEKS，是从 IND-KGA 安全[6]到 IND-KGA-SERVER 安全的编译器。

2　准备知识

2.1　数字证书授权中心

数字证书授权中心(CA, certificate authority)是公钥基础设施(PKI, public key infrastructure)中最重要的组成。其任务是为用户生成、公布、撤销、归档数字证书[14]。它被广泛用在诸如安全套接字层协议、安全电子交易、以及身份认证等协议中。其原因是 CA 具有分辨成员对象身份、确认对象密钥和身份信息之间关系的能力[15]。这也是本文使用 CA 的原因。

2.2　强不可伪造和不可否认的签名

数字签名包含 3 个概率多项式时间的算法 $(Gen, Sign, Verify)$，满足：

1) 给定安全参数 1^k，密钥生成算法 Gen 输出签名者的公私钥对 (pk, sk)；

2) 输入消息 m 和签名者的私钥 sk，算法 $Sign$ 输出 m 的签名 σ。本文用 $\sigma \leftarrow Sign(sk, m)$ 表示签名；

3) 输入签名者的公钥 pk 和签名 σ，若 σ 有效，则验证算法 $Verify$ 输出 1；否则，输出 0。本文用 $Verify(pk, \sigma)$ 表示签名的验证。

本文主要涉及签名的下述性质:

1) 强不可伪造性，若敌手对已签名的消息再次签名从计算上不可行，则签名强不可伪造[16~18]；

2) 不可否认性，若没有签名者的帮助签名无法被验证，且签名者无法否认自己的签名，则签名不可否认[19,20]。

同时拥有这 2 种性质的签名是存在的，细节请参考文献[20~22]。

3　IND-KGA-SERVER 安全模型

本节定义 IND-KGA-SERVER 安全来形式化 KG 攻击下 dPEKS 中恶意服务器的能力。模型通过实验(游戏)定义。该实验在攻击者 $\mathcal{A}$ 和假想的挑战者 $\mathcal{B}$ 之间进行[23]。$\mathcal{A}$ 的能力包括：提出陷门询问、生成 dPEKS 密文、测试给定陷门是否和 dPEKS 密文相关。陷门询问用来描述 $\mathcal{A}$ 可从非安全信道中获取任何陷门。任何实体都可使用接收者的公钥生成 dPEKS 密文，$\mathcal{A}$ 同样可以。服务器可使用自己的私钥测试陷门和 dPEKS 密文的相关性，$\mathcal{A}$ 同样可以。然而，实验允许攻击者对被挑战的关键字进行询问，因为现实场景中的攻击者能够在多项式时间内遍历整个关键字空间。IND-KGA-SERVER 安全的方案能够保证即使挑战关键字被询问，攻击者仍然无法从陷门猜出关键字。实验中，$\mathcal{B}$ 建立算法并扮演接收者的角色。$\mathcal{B}$ 和 $\mathcal{A}$ 交互，并判断 $\mathcal{A}$ 是否能从陷门中猜测出关键字。定义该实验为 IND-KGA-SERVER 实验，并用 $Exp_{\mathcal{A},\Pi}^{IND-KGA-SERVER}(\lambda)$

表示。其中 λ 是安全参数，Π 是所构 dPEKS 方案。实验运行如下。

1) 初始化。$\mathcal{B}$ 运行算法 $GlobalSetup(\lambda)$ 生成全局参数 $\mathcal{GP}$，运行 $KeyGen_{\text{receiver}}(\mathcal{GP})$ 生成接收者密钥对 $(pk_{\text{receiver}}, sk_{\text{receiver}})$，并公布公钥 pk_{receiver} 和全局参数 $\mathcal{GP}$。$\mathcal{A}$ 运行算法 $KeyGen_{\text{server}}(\mathcal{GP})$ 生成服务器密钥对 $(pk_{\text{server}}, sk_{\text{server}})$，并公布 pk_{server}。

2) 第一阶段。

陷门询问。$\mathcal{A}$ 自适应地从关键字空间 $\mathcal{KS}$ 选取关键字 $w \in \mathcal{KS}$，并发起陷门询问 T_w。$\mathcal{B}$ 运行陷门生成算法，$T_w = Trapdoor(\mathcal{GP}, pk_{\text{server}}, sk_{\text{receiver}}, w)$，并用 T_w 对 $\mathcal{A}$ 的询问作以应答。

dPEKS 密文生成。$\mathcal{A}$ 猜测一个关键字 $k' \in \mathcal{KS}$，并运行 dEKS 算法生成相应的 dPEKS 密文 c'，即 $c' = dPEKS(pk_{\text{receiver}}, w')$。

相关性测试。$\mathcal{A}$ 运行算法 $dTest(c', sk_{\text{server}}, T_w)$ 测试生成的 dPEKS 密文和被询问陷门的相关性(如果相关，算法输出 1，$\mathcal{A}$ 成功猜出陷门对应的关键字)。

3) 挑战阶段。某时刻，$\mathcal{A}$ 完成第一阶段的询问，并输出一对关键字 (w_0, w_1)。$\mathcal{A}$ 希望这对关键字被挑战。但允许 w_0 和 w_1 在第一阶段被询问，因为关键字空间可以被攻击者在多项式时间内遍历。$\mathcal{A}$ 发送 (w_0, w_1) 给 $\mathcal{B}$。$\mathcal{B}$ 随机选择 $b \in \{0,1\}$ 并发送 T_{w_b} 给 $\mathcal{A}$。

4) 第二阶段。$\mathcal{A}$ 继续像第一阶段那样询问。

5) 相关性测测。$\mathcal{A}$ 输出猜测 b'。若 $b' = b$，则 $\mathcal{A}$ 赢得游戏并输出 1；否则，输出 0。

定义攻击者 $\mathcal{A}$ 在实验 $Exp_{\mathcal{A},\Pi}^{IND-KGA-SERVER}(\lambda)$ 中优势为 $Adv_{\mathcal{A}}^{IND-KGA-SERVER}(\lambda) = |\Pr[b' = b] - 1/2|$。

定义 1 IND-KGA-SERVER 安全。dPEKS 方案 Π 是 IND-KGA-SERVER 安全的，如果对于任意多项式时间的攻击者 $\mathcal{A}$（服务器），优势 $Adv_{\mathcal{A}}^{IND-KGA-SERVER}(\lambda)$ 是可忽略的。

断言 1 抵抗 KG 攻击的 dPEKS 方案应同时满足 IND-KGA 安全和 IND-KGA-SERVER 安全。

证明 假设接收者自身不是攻击者，这是合理的，因接收者是被动接收邮件，他希望邮件不被第三者看到。然而恶意的服务器拥有各种动机去偷看邮件内容，比如出于经济利益。文献[6]定义的 IND-KGA 安全模型中，攻击者 $\mathcal{A}$ 只能描述外部攻击者的能力，这样的攻击者既不包括服务器也不包括接收者。在 IND-KGA-SERVER 安全中，攻击者描述的是服务器的能力，因此 IND-KGA-SERVER 安全是对 IND-KGA 安全的必要补充。能够抵抗 KG 攻击的 dPEKS 方案必须同时满足 IND-KGA 安全和 IND-KGA-SERVER 安全。而且 IND-KGA-SERVER 安全甚至更重要，因为服务器和接收者、发送者直接交互，针对服务器的安全将直接影响邮件的安全。

4 方案构造

Jeong 等[24]证明在攻击者是服务器的情况下无法构造抗 KG 攻击的 dPEKS，后续方案[4~6]都未解决该问题。然而，服务器直接和发送者及接收者交互。抗 KG 攻击的 dPEKS 不但不能放弃针对服务器的安全，而且应更重视该安全。下文首先分析已有方案无法抵抗服务器 KG 攻击的原因，并给出解决方案。

4.1 原因分析

IND-KGA 安全的 dPEKS 中，服务器仍然成功进行 KG 攻击的原因是服务器同时拥有生成 dPEKS 密文和运行 dTest 测试算法的能力。具体如下。

1) 服务器获得陷门 T_w 并试图猜测相应关键字 w。

2) 服务器随机选择 $w' \in \mathcal{KS}$，并计算 dPEKS 密文 $c_{w'}$。

3) 服务器运行 $dTest(c_{w'}, T_w, sk_s)$ 算法。若输出为 1，服务器成功猜出关键字 w。否则，返回 2)继续运行，直到成功为止。

任何可在多项式时间内遍历关键字空间的攻击者，都可成功利用上述方法猜出陷门对应的关键字。

4.2 解决方法

本文解决方法是，若 dPEKS 密文 c 由服务器生成，则不再允许服务器运行 dTest 算法，这是合理的。若 dPEKS 密文是由服务器生成，则服务器拥有消息内容，所以无需使用陷门。因此，问题转为在密文由服务器生成时，怎样阻止服务器运行测试算法 dTest。为此，本文引入 CA 以及强不可伪造和不可否认的签名。发送者将自己 ID 和相应签名附加在密文上，签名的不可否认性可阻止服务器伪装成外部攻击者以便运行 dTest 算法。接收者和 CA 交互，得到服务器真实 ID，并生成相应签名。接收者将该签名和服务器真实 ID 作为陷门的一部分发送给 dTest 算法。签名算法的强不可伪造性阻止了服务器对发送者发送给 dTest 算法的 ID 信息进行修改，以便提供给 dTest 算法虚假的 ID 从而运行算法。

因此方案的安全基于 CA 的权威性以及签名算

法的不可伪造和不可否认性。

4.3 dPEKS 简述

本文方案独立于具体的 dPEKS，因此下文首先从概括性角度对 IND-KGA 安全的 dPEKS 方案做以描述。该类方案是存在的，请参考文献[5,6]。

1) Global Setup(λ)：给定安全参数 λ，算法生成全局参数 $\mathcal{GP}$。

2) KeyGen$_{\text{server}}$($\mathcal{GP}$)：输入全局参数 $\mathcal{GP}$，算法输出服务器密钥对($pk_{\text{server}}, sk_{\text{server}}$)。

3) KeyGen$_{\text{receiver}}$($\mathcal{GP}$)：输入全局参数 $\mathcal{GP}$，算法输出接收者密钥对($pk_{\text{receiver}}, sk_{\text{receiver}}$)。

4) dPEKS($pk_{\text{receiver}}, pk_{\text{server}}, w$)：以接收者和服务器的公钥、关键字 w 为输入，任何实体都可运行算法进而获得关键字的 dPEKS 密文 c。

5) Trapdoor(sk_{receiver}, w)：以接收者秘密钥和关键字为输入，接收者运行算法获得关键字陷门 T_w。

6) dTest($c, sk_{\text{server}}, T_w$)：以 dPEKS 密文、服务器私钥、关键字陷门为输入，服务器运行算法以判断给定 dPEKS 密文和关键字陷门的相关性。若相关，算法输出 1；否则，输出 0。

4.4 本文方案

方案建立在 IND-KGA 安全的 dPEKS 基础上，但独立于其具体算法。方案如下运行：

1) Global Setup(λ)：给定安全参数 λ，算法生成全局参数 $\mathcal{GP}$。

2) KeyGen$_{\text{server}}$($\mathcal{GP}$)：输入全局参数 $\mathcal{GP}$，算法输出服务器密钥对($pk_{\text{server}}, sk_{\text{server}}$)。

3) KeyGen$_{\text{receiver}}$($\mathcal{GP}$)：输入全局参数 $\mathcal{GP}$，算法输出接收者密钥对($pk_{\text{receiver}}, sk_{\text{receiver}}$)。

4) KeyGen$_{\text{sender}}$($\mathcal{GP}$)：输入全局参数 $\mathcal{GP}$，算法输出发送者密钥对($pk_{\text{sender}}, sk_{\text{sender}}$)。

5) dPEKS($pk_{\text{receiver}}, pk_{\text{server}}, w, ID_{\text{sender}}$):

①以接收者和服务器的公钥、关键字为输入，发送者运行算法生成关键字密文 c'。

②以发送者私钥和身份为输入，发送者运行签名算法生成签名 $\sigma_{\text{sender}} = sign(sk_{\text{sender}}, ID_{\text{sender}})$。此处用到签名的不可否认性。

③发送者运行该算法从而设置 dPEKS 密文为 $c = (c', ID_{\text{sender}}, \sigma_{\text{sender}})$。

6) Trapdoor(sk_{receiver}, w)。

①以接收者秘密钥和关键字为输入，接收者运行算法以获得关键字陷门 t_w。

②接收者和 CA 交互获得服务器身份 ID^{CA}_{server}。

③接收者以秘密钥和 ID^{CA}_{server} 为输入，运行签名算法生成签名 $\sigma^{\text{receiver}}_{ID^{CA}_{\text{server}}} = sign(sk_{\text{receiver}}, ID^{CA}_{\text{server}})$。此处用到签名算法的强不可为造性。

④接收者运行算法以设置关键字陷门为 $T_w = (t_w, ID^{CA}_{\text{server}}, \sigma^{\text{receiver}}_{ID^{CA}_{\text{server}}})$ 并发给服务器以便搜索。

7) dTest($c, sk_{\text{server}}, T_w$)。

①服务器运行算法从 dPEKS 密文 c 中提取出 c'、ID_{sender} 和 σ_{sender}，并检测 $ID_{\text{sender}} \stackrel{?}{=} ID^{CA}_{\text{server}}$。若相等，算法拒绝被运行并输出 0 (在算法拒绝被运行以及测试结果为不相关这 2 种情况下，算法都输出 0，攻击者因此无法区分这 2 种情况)。若等式不成立，算法如下运行。

②算法运行 $Verify(pk_{\text{sender}}, ID_{\text{sender}}, \sigma_{\text{sender}})$ 以验证发送者签名是否有效。若验证失败，算法拒绝被运行并输出 0。否则，算法如下运行。

③算法从陷门 T_w 中提取出 t_w、ID^{CA}_{server} 和 $\sigma^{\text{receiver}}_{ID^{CA}_{\text{server}}}$，并运行 $Verify(pk_{\text{receiver}}, ID^{CA}_{\text{server}}, \sigma^{\text{receiver}}_{ID^{CA}_{\text{server}}})$ 以验证 $\sigma^{\text{receiver}}_{ID_{\text{server}}}$ 的有效性。若验证失败，算法拒绝被运行并输出 0。否则，算法如下运行。

④以关键字密文 c'、陷门 t_w、以及服务器私钥 sk_{server} 为输入，算法检测密文 c' 与关键字陷门 t_w 的相关性。若相关，算法输出 1；否则输出 0。

定理 1　假设所依赖的 dPEKS 方案 Π^D 是 IND-KGA 安全的，则本文方案 Π^O 也是 IND-KGA 安全的。

证明　为证明定理，只需证明在与 Π^D 中进行对比时，攻击者 $\mathcal{A}$ 在 Π^O 中增加的视图无法被用来从陷门中猜测关键字。在 Π^O 中，$\mathcal{A}$ 增加的视图为 $View^{\Pi^O}_{\text{add}} = (ID_{\text{sender}}, \sigma_{\text{sender}}, ID^{CA}_{\text{server}}, \sigma^{\text{receiver}}_{ID^{CA}_{\text{server}}})$。在 Π^D 中，尽管未明确指出任何攻击者都可获得 ID_{sender} 和 ID^{CA}_{server}，但在 PKI 存在的情况下，这些信息很容易被获取。且在 Π^O 中，尽管 $\mathcal{A}$ 能获得 σ_{sender} 和 $\sigma^{\text{receiver}}_{ID^{CA}_{\text{server}}}$，签名算法的强不可伪造性保证 $\mathcal{A}$ 无法伪装成相应的发送者进而展开可能的攻击。即 $View^{\Pi^O}_{\text{add}}$ 对 $\mathcal{A}$ 猜测关键字没有帮助。因此在假设 Π^D 是 IND-KGA 安全的前提下，Π^O 也是 IND-KGA 安全的。

定理 2　假设 IND-KGA 安全的 dPEKS 的存在性、CA 的存在性、强不可伪造和不可否认签名的存在性，本文的方案是 IND-KGA-SERVER 安全的。

证明 4.1 节分析了 IND-KGA 安全的 dPEKS 在 KG 敌手是服务器的情况下不安全的原因是服务器同时拥有生成 dPEKS 密文和运行 dTest 测试算法的能力。定理 1 证明了本文的构造是 IND-KGA 安全的，因此只需要证明，如果 dPEKS 密文由服务器自己生成，则服务器无法再运行 dTest 算法测试密文和陷门的相关性。在 dTest 算法中，算法需检测密文生成者是否是服务器，所以问题转化为证明服务器无法伪装成外部发送者。在 dTest 算法检测密文生成者（即发送者）ID 时，服务器仍然能够提供虚假 ID 进行欺骗。然而，签名算法的不可否认性保证了服务器无法否认自己对该 ID 的签名。而且，如果服务器使用虚假的 ID 和窃取到的真实的签名作为输入，则签名无法通过验证。为保证 dTest 算法能够从接收者获得服务器的真实身份，接收者直接和 CA 交互。CA 的权威性保证了接收者得到的 ID 信息是真实的。但恶意服务器能够更改接收者发送给 dTest 算法的消息，并且将更改后的消息作为输入提供给 dTest 算法。然而，dTest 算法在验证接收者签名时，签名算法的强不可伪造性保证了 dTest 算法从接收者得到的信息是可靠的。即服务器无法通过伪装进而运行 dTest 算法测试密文和陷门的相关性。因此，CA 的权威性、签名算法的强不可伪造性和不可否认性保证了本文所提出的方案是 IND-KGA-SERVER 安全的。

5 结束语

本文定义了 IND-KGA 安全的 dPEKS 方案中针对服务器的 IND-KGA-SERVER 安全，是抵抗 KG 攻击的必要组成；分析了传统的 IND-KGA 安全的 dPEKS 方案在攻击者是服务器的情况下不安全的原因；给出了解决方法和方案。方案基于 IND-KGA 安全的 dPEKS，但是又独立于其具体构造，可被看作从 IND-KGA 安全的 dPEKS 到 IND-KGA-SERVER 安全的 dPEKS 的编译器。

参考文献：

[1] BONEH D, CRESCENZO G D, OSTROVSKY R, PERSIANO G. Public key encryption with keyword search[A]. EUROCYPT[C]. 2004. 506-522.

[2] BAEK J, SAFAVI-NAINI R, SUSILO W. Public key encryption with keyword search revisited[A]. ACIS[C]. 2006. 1249-1259.

[3] BYUN J W, RHEE H S, PARK H A, LEE D H. Off-line keyword guessing attacks on recent keyword search schemes over encrypted data[A]. SDM[C]. 2006. 75-83.

[4] RHEE H S, SUSILO W, KIM H J. Secure searchable public key encryption scheme against keyword guessing attacks[J]. IEICE Electronics Express, 2009, 6(5): 237-243.

[5] RHEE H S, PARK J H, SUSILO W, LEE D H. Trapdoor security in a searchable public-key encryption scheme with a designated tester[J]. Journal of System and Software, 2010, 83(5): 763-771.

[6] FANG L, SUSILO W, GE C, WANG J. Public key encryption with keyword search secure against keyword guessing attacks without random oracle[J]. Information Sciences, 2013, 238: 221-241.

[7] LI J, WANG Q, WANG C, *et al*. Fuzzy keyword search over encrypted data in cloud computing[A]. INFOCOM[C]. 2010. 1-5.

[8] WANG C, CAO N, LI J, *et al*. Secure ranked keyword search over encrypted cloud data[A]. ICDCS[C]. 2010. 253-262.

[9] CAO N, WANG C, LI M, *et al*. Privacy-preserving multi-keyword ranked search over encrypted cloud data[J]. IEEE Transactions on Parallel and Distributed Systems, 2014, 25(1): 222-233.

[10] WANG C, CAO N, REN K, *et al*. Enabling secure and efficient ranked keyword search over outsourced cloud data[J]. IEEE Transactions on Parallel and Distributed Systems , 2012, 23(8): 1467-1479.

[11] LI M, YU S, CAO N, *et al*. Authorized private keyword search over encrypted data in cloud computing[A]. ICDCS[C]. 2011. 383-392.

[12] BONEH D, RAGHUNATHAN A, SEGEV G. Function-private identity-based encryption: Hiding the function in functional encryption[A]. CRYPTO[C]. Springer Berlin Heidelberg, 2013. 461-478.

[13] BONEH D, RAGHUNATHAN A, SEGEV G. Function-private subspace-membership encryption and its applications[A]. ASIACRYPT[C]. Springer Berlin Heidelberg, 2013. 255-275.

[14] LI J, WANG Q, WANG C, *et al*. Fuzzy keyword search over encrypted data in cloud computing[A]. INFOCOM[C]. 2010. 1-5.

[15] WANG C, CAO N, LI J, *et al*. Secure ranked keyword search over encrypted cloud data[A]. ICDCS[C]. 2010. 253-262.

[16] CAO N, WANG C, LI M, *et al*. Privacy-preserving multi-keyword ranked search over encrypted cloud data[J]. IEEE Transactions on Parallel and Distributed Systems, 2014, 25(1): 222-233.

[17] WANG C, CAO N, REN K, *et al*. Enabling secure and efficient ranked keyword search over outsourced cloud data[J]. IEEE Transactions on Parallel and Distributed Systems , 2012, 23(8): 1467-1479.

[18] LI M, YU S, CAO N, *et al*. Authorized private keyword search over encrypted data in cloud computing[A]. ICDCS[C]. 2011. 383-392.

[19] BONEH D, RAGHUNATHAN A, SEGEV G. Function-private identity-based encryption: hiding the function in functional encryption[A]. CRYPTO[C]. Springer Berlin Heidelberg, 2013. 461-478.

[20] BONEH D, RAGHUNATHAN A, SEGEV G. Function-private sub-

space-membership encryption and its applications[A]. ASIACRYPT[C]. Springer Berlin Heidelberg, 2013. 255-275.

[21] HAIDAR A N, ABDALLAH A E. Formal modeling of PKI based authentication[J]. Electronic Notes in Theoretical Computer Science, 2009, 235: 55-70.

[22] GOLLMANN D, MEIER J, SABELFELD A. Computer Security[M]. Springer, Germany, 2006.

[23] AN J, DODIS Y, RABIN T. On the security of joint signature and encryption[A]. Eurocrypt[C]. 2002. 83-107.

[24] BONEH D, SHEN E, WATERS B. Strongly unforgeable signatures based on computational Diffie-Hellman[A]. PKC[C]. 2006. 229-240.

[25] SHAO Z, GAO Y. Practical verifiably encrypted signatures without random oracles[EB/OL]. http://dx.doi.org/10.1016/j.ins.2014.03.092.

[26] CHAUM D, ANTWERPEN H V. Undeniable signatures[A]. CRYPTO[C]. 1989. 212-216.

[27] KUROSAWA K, NOJIMA R. Relation between verifiable random functions and convertible undeniable signatures, and new constructions[J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2014, 97(1): 215-224.

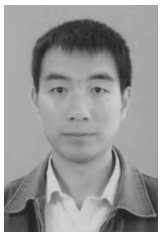
[28] SCHULDT J C N, MATSUURA K. An efficient convertible undeniable signature scheme with delegatable verification[A]. ISPEC[C]. 2010. 276-293.

[29] HUANG Q, WONG D S, SUSILO W. The construction of ambiguous optimistic fair exchange from designated confirmer signature without random oracles[J]. Information Sciences, 2013, 228: 222-238.

[30] KATA J, LINDELL Y. Introduction to Modern Cryptography: Principles and Protocols[M]. CRC Press, Boca Raton, 2007.

[31] JEONG I R, KWON J O, HONG D, LEE D H. Constructing PEKS schemes secure against keyword guessing attacks is possible[J]. Computer Communications, 2009, 32(2):394-396.

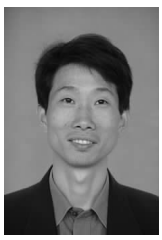
作者简介：



邵志毅（1983-），男，陕西西安人，陕西师范大学博士生，主要研究方向为信息安全。

杨波（1963-），男，陕西渭南人，陕西师范大学教授、博士生导师，主要研究方向为密码学与信息安全。

吴振强（1968-），男，陕西商洛人，陕西师范大学教授、博士生导师，主要研究方向为网络安全。



张明武（1972-），男，湖北仙桃人，湖北工业大学副教授，主要研究方向为信息安全。