西 安 邮 电 大 学

毕 业 设 计（译 文）

论文题目：企业数据库加密技术的研究与实现

学　　院：通信与信息工程学院

专　　业：信息对抗技术

班　　级：信息对抗 1201

学生姓名：罗冲

导师姓名：闵祥参　职称：讲师

可证明的安全 Timed-Release 公钥

8.1 可证明安全的 Timed-Release 公钥加密

Timed-Release 密码体制允许发送者对消息进行加密，因此，收件人只能在指定的时间读它。形式化安全 timed-release 的概念，公钥密码系统是指依靠第三方保证在指定日期解密，这一概念相当于基于身份的加密；这就解释了观察到的所有已知的结构实现 timed-release 使用基于身份的加密安全原理。然后给出几个可行性安全解密加密的结构：一个普遍的结构是基于任何身份的加密，第二个结构是在第一个的基础上进行的密码双线性映射。第一个就是和 Boneh-Franklin 一样高效的基于身份的加密方案，并且是可证明的安全在随机预言模型的验证；最后的方案不是认证的而是可证实的标准模型。

附加的关键字和短语：timed-release，认证加密，密钥绝缘加密

8.2 介绍

Timed-Release 加密的目的是“发送一条消息到未来”要做到这一点的方法之一是对消息进行加密，这样接收器就不能解密密文。这种形式有很多实际应用；举几个例子：包括防止不诚实现象的发生以及防止提前开放选票投票中的不公平交换现象的发生，因此产生了机密信息的发布，和延迟签名文档的验证，如电子彩票[Syverson 1998]和支票兑现的问题首次提出 timed-release 密码学(1993 年 5 月)，然后进行了讨论让我们假设 Alice 想发送消息给 Bob，Bob 无法打开它，直到一个特定的时间。之前的解决方案分为两种类别：

（1）时间同步谜题:Alice 加密消息，所以 Bob 需要不停地执行 non-parallelizable 解密算法算出解密所需的时间，如果 Alice 准确地预测出和鲍勃之间的计算资源和所需的时间，然后 Bob 回复消息。

（2）可信代理解密:Alice 加密消息，为了解密消息，Bob 需要发布一些秘密值，一个值得信赖的代理所需的日期，一旦代理发布信息，Bob 便可以解密消息。

第一种方法给消息接收器造成了相当大的计算开销，这样一来使它在真实场景下并不受欢迎。此外，还要知道解密的计算复杂度，同时给我们一个 Bob 可

能需要解密消息的时间下限，并不能保证明文将在特定日期可用。不过，这种方法广泛用于特定的应用程序(Boneh and Naor 2000；Belare and Goldwasser 1996；Syverson 1998； Garay and Pomerance 2002, 2003]。基于代理的方法，另一方面，缓解 Bob 执行不停地计算，集合解密精确的日期，不需要 Alice 对 Bob 的信息功能。这是要付出代价的，代理必须信任，他们必须在指定的时间是可用的。

在本文中，我们专注于计划使用这种“解密代理”。我们形式化安全 timed-release 加密方案和解密的概念它相当于加强 key-insulated 加密的概念[when there is no a priori bound on the number of time periods . 2002]；当没有先天的时间段的数量，反过来，这一概念是基于身份的加密，或 IBE[Bellare and Palacio 2002]。我们也给出几个 provably-secure 结构第一可行性安全 timed-release 公钥加密，包括一般建设在文献中，第一个有效的方案在标准模型证明地安全，也就是说，没有随机的密钥。

ACM 交易信息和系统安全、11 卷，2 号第八条。日期：2008 年 5 月，证明地安全 Timed-Release 公钥加密。

8.3 可证明安全的 Timed-Release 公钥加密

我们的研究结果也为几个出现在之前的方案文献:每个可以被看作是一个已知 key-insulated 改编的加密方案。例如，李维斯特 et al。[1996]建议代理可以用一个密钥加密消息请求将发表在指定的日期由代理或代理可以预计算对公钥/私钥，发布公钥和释放的私钥所需的天，这些符合 key-insulated 方案出现在文献中。Crescenzo et al 。[1999]的方案基本上取代出版物的出版的关键信息，要求接收方参与一个条件的传输协议与代理解密该消息。在陈 et al。[2002]，作者提出使用 Boneh 和富兰克林的 IBE 方案[Boneh and Franklin 2003]timed-release 加密:从本质上说，该计划取代了身份在 IBE 方案解密的时间。类似的提案出现在虽然一些上述提案包含非正式的安全证明，没有他们考虑和/或给一个正式的治疗的安全属性 timed-release 公钥加密(或 TR-PKE)。第一次正式的治疗方法 TR-PKE 安全被显示在 Cheon et al[2004]，然后加强在 et al。[2006]。独立 Cathalo et al .[2005]。

介绍另一个概念 timed-release 安全和认为这不是暗示 key-insulated 加密；然而，这似乎是一个副作用的论模型中，用必须提交到一个特定的解密代理在选择他的公钥。身份验证用于 Timed-Release 加密。

许多的应用 timed-release 上面需要某种形式的身份验证。例如，如果没有验证密封的投标拍卖，投标人可以伪造投标，拍卖或权利失败通过提交不合理的

高报价。在本文中，我们考虑这些应用程序所需安全属性和发展正式的安全条件 Timed-Release 公钥认证加密(TR-PKAE)计划。

开发 TR-PKAE 方案会作曲未经过身份验证的 TR-PKE 与签名方案或计划(non-timed-release)PKAE 方案。尽管这样的建筑是可能的，我们注意到，这篇作文的细节不是微不足道的，从一个例子[2001]和多迪和卡茨[2005]说明天真的结构可以失败提供预期的安全属性。另外，我们注意到计划都可能面临一个相对于基于方案的性能损失在一个原始的。因此，除了介绍一个通用的建筑，我们介绍起他们安全建设 TR-PKAE 方案本质上以前的建筑没有进行身份验证的 TR-PKE 一样有效计划(Chen et al. 2002； Marco Casassa Mont and Sadler 2003； Blake and Chan 2005].

ACM 交易信息和系统安全、11 卷，2 号第八条，日期:2008 年 5 月。

8.4 定义

在本节中，我们将在本文使用审查安全定义，。在此外，我们引入新的定义，即 timed-release 公众密钥加密(TR-PKE)和验证 TR-PKE(TR-PKAE)。

基于身份加密。我们正式定义一个 IBE 方案 IBES 的元组四个随机算法:

（1）SetupIBE(1k)给定的输入 1 k(安全参数)，产生公众参数 π IBE，包括哈希函数、消息和密文空间等等。此外，主秘密 δ IBE 生成保密由中央权威。

（2）ExtractIBE(π IBE δ IBE，我)，鉴于公共参数 π IBE δ IBE 主人的秘密和身份 I∈{ 0，1 }*，输出一个秘钥 I(和 π IBE 一起)I 是对应的公钥身份。

（3）EncryptIBE(π IBE，米)计算加密的密文 c 表示认同 I 的消息 mwith π IBE 公共参数。

（4）DecryptIBE(π IBE， skI ，bc)输出相对应的明文 tobc 就是解密成功否则会显示特殊符号“失败”。

为了一致性，我们要求 π IBE， skI ，EncryptIBE(π IBE，I，m)) =m， for all valid (I，skI)，m，for all valid (I，skI)，(π IBE，δ IBE)， and m. (π IBE，δ IBE)，and m. m，for all valid (I， skI)，(π IBE，δ IBE)， and m. We use the IND-ID-CCA notion of security for and IBE scheme [Boneh 我们使用 IND-ID-CCA 安全的概念和 IBE 方案[Boneh 和 Franklin2003]。简单地说，在这种情况下，敌人可以自适应地问密钥对应任意的身份，也可能要求解密的密文使用任何身份。最终的对手提出了一种“挑战身份”和一份“挑战明文”，考虑到其中一个明文的加密挑战

下的身份。敌人可能会继续要求密钥和解密，除了它其他人不能参加查询密钥的身份或挑战解密密文的挑战，作为挑战者的身份的如果能猜出这暗文便对手赢得挑战的胜利加密的挑者证明该方案是安全的，如果没有多项式时间那么对手赢得挑战的优势目测大概大于 1/2。公钥加密。PKE 包含公钥加密系统由三种算法构成:

（1）KeyGenPKE 输入 1 k，输出公共/私有密钥对(pk，sk)。的还包括公钥加密/解密所需的公共参数。

（2）EncryptPKE，pk 和消息 m 的输入，输出密文 c。

（3）DecryptPKE，ciphertextbc 和私钥 sk 的输入，输出一些消息失败的象征。

为了保持一致性，要求 DecryptPKE(sk，EncryptPKE(pk，m))= m 所有有效的(pk，sk)和 m。

ACM 交易信息和系统安全、11 卷，2 号第八条。日期:2008 年 5 月。证明地安全 Timed-Release 公钥加密。

8.5 可证明安全的 Timed-Release 公钥加密

我们利用 PKE IND-CCA2 安全对自适应的对手所述 Bellare et al。[1998]。简而言之，“挑战者”号生成一个公共/私人密钥对和给敌人的公钥。敌人允许查询使用私钥解密的密文。一步的挑战，挑战的对手产生一对明文并给出加密的两人之一。对手获胜，如果考虑到能够查询任何消息，但挑战密文的解密，它能猜出这两个明文加密的挑战的一步。

我们注意，给定一个安全的 IBES，我们可以很容易地获得一个安全的 PKE。为目的，每个用户简单地运行 ib SetupIBE ExtractIBE，使用一个任意的身份，获得它的公钥和私钥(即 IBES 的密钥)。我连同身份 IBES 的公共参数作为用户的公钥，而主密钥作为私人关键。一个简单的论据表明，如果 IBES IND-ID-CCA 安全那么相应的 PKE IND-CCA2 安全。然而，由于在实际应用我们期望一个更有效地使用 PKE 结构，本文使用单独的 IBE 和 PKE 方案。

数字签名和标签。除了上面的原语，我们会的也使用签名方案。我们首先开始审查标准的签名。签名方案 DS 由三种算法:

（1）SigGen，输入 1k，输出签署/验证密钥对(SK，VK)。VK 也包括公共信息空间等参数等等。

（2）Sig，在输入 SK 和消息，输出签名 σ。在输入消息 m - v，签名 σ 和 VK，输出正确或假。

（3）Ver，当输入信息 m - v,签名信息 σ 和 VK，输出或真或假。

为了一致性，要求每一个有效的结对(SK、VK)和消息 m，VerVK(m，SigSK(m))= true。我们将使用 unforgeability 强的概念在自适应选择明文攻击(SUF-CMA)。简单地说，“挑战者”号生成(SK、VK)，并给出了 VK 的对手。敌人给出了签名 σ 1 σ 2。σ q，自适应地选择消息 m1、m2。，mq 和输出一对(m，σ)。对手获胜，如果(m，σ)是一个有效的消息签名对和不等于任何一对(mi，σ i)。

标准签名旁边，我们还将使用一次性的签名定义类似地，除了在 SUF-CMA 对手是允许的只有一个查询。任何公钥签名 SUF-CMA 安全也是一个安全的一次性签名。然而，相反的，显然不是如此一次性签名通常更有效。

我们还可以添加公共标签 IBE 和 PKE 加密/ decryptionmechanisms，这注定 nonmalleable 的密文(Shoup 博士 2004 年)在保持安全。实际上，密文代另外需要输入一个标签，变成密文的一部分。解密时，不仅解密密钥，也适用于公众的标签。

ACM 交易信息和系统安全、11 卷,2 号第八条。日期:2008 年 5 月。

8.6 自然的方式修改标签

1 Timed-Release 公钥加密(TR-PKE)

在本节中,我们形式化的功能和安全要求 timed-release 公钥加密系统。这些要求为了捕捉隐性安全需求没有在之前解决工作 [May 1993； Rivest et al. 1996；Chen et al. 2002；Marco Casassa Mont 工作(1993 年 5 月，Rivest et al . 1996；Chenet al . 2002； Sadler2003， Blake 和 2005]；特别是他们不解决身份验证需求，我们加入 2.3 节。非正式地，我们可以认为任何主要在 TR-PKE 系统填充三个角色的一个或多个。的 timed-release 代理或提(timed-release 公共服务器)出版 timed-release 公钥和释放“令牌”，允许解密消息加密的定期为当前时间。接收方发布一个公钥，允许别人这样只有他可以加密消息用一个密钥来解密，他保持私有，和适当的 timed-release 令牌。发送方使用接收方的公钥和提公钥加密消息，稍后可以解密的时候选择。

1.1 功能需求

公钥加密系统 Ŵ 五元组随机算法：

（1）Setup，给定的输入 1 k(安全参数)，产生公共参数 π g，包括哈希函数、消息和密文空间等等。

（2）TRSetup，产生一对(δ， π tr) δ 是主人的密钥和 π tr 相应 timed-release 公共参数。此设置由主密钥保密，所有其他参数都是公开的。我们表示结合公共参数 π g 和 π tr π 。

（3）注册机，鉴于 π g 公共参数，输出一对密钥和公开 key (sk，pk)。tg(π，δ T)计算相对应的令牌 tknT 时间 T 使用(δ π)。这个功能是由公开版 tknT 在时间 T。

（4）TG(π，δT)计算相对应的令牌 tknT 使用(δπ)的时间 T。这个功能是由正式版 tknT 提供的。

（5）加密(π，pk，m，T)计算 timed-release 密文 c 表示使用公钥加密的消息 m pk、公共参数 π 和时间编码 T。

（6）解密(π，sk，tknT)输出相对应的明文 tobc 表示解密成功或“失败”。

为了一致性，我们要求解密(π、sk、加密(π，pk，m T)，TG(π，δT))= m，为所有有效(pk，sk)，(δπ)，T，m。不像功能需求中指定的那样，我们明确地分离功能 TRSetup 和注册机，允许用户生成独立的密钥任何 timed-release 服务器。这允许发送方选择哪些服务器信任在加密。

ACM 交易信息和系统安全、11 卷，2 号第八条。日期：2008 年 5 月。