前向安全的基于身份加密方案

杨浩淼，孙世新，李洪伟

(电子科技大学计算机科学与工程学院 成都 610054)

【摘要】构建了一个非交互式密钥更新、基于身份的加密方案，解决私钥的泄漏问题。非交互式特性通过前向安全实现；给出了非交互式密钥更新的基于身份加密方案的定义及安全性定义；基于已有的二叉树加密构造了基于身份的二叉树加密方案及非交互式密钥更新的基于身份加密方案；分析了方案的安全性和效率。

关 键 词 前向安全; 基于身份加密; 密钥泄漏; 密钥非交互式更新
中图分类号 TP309.2 文献标识码 A

Forward-Secure Identity-Based Encryption Scheme

YANG Hao-miao，SUN Shi-xin，LI Hong-wei

(School of Computer Science and Engineering, University of Electronic Science and Technology of China Chengdu 610054)

Abstract To deal with the threat of key exposure, an identity-based encryption scheme with non-interactive key update is proposed. The non-interactive property is obtained by forward-security (a typical key evolving paradigm). First the definition and security definition of Identity-Based Encryption with Non-Interactive Key Update scheme (IBE-NIKU) are given. Then identity-based binary tree encryption scheme is constructed. As a result, a concrete IBE-NIKU is given. The security and efficiency of these schemes are also analyzed.

Key words forward-security; identity-based encryption; key exposure; non-interactive key update

在传统的公钥加密中，公钥是与身份无关的随机字符串，需要公钥证书来绑定公钥和身份信息。文献[1]引入了基于身份的加密(Identity-Based Encryption，IBE)。在IBE中公钥是任意的字符串，如用户的名字、Email地址、手机号码等。公钥可直接从身份信息中提取，公钥目录不必要，因此可简化证书管理。适合于IBE的一个典型应用是移动电话网络系统，用户只需要通过他们的手机号码就能简单方便地相互通信：发送方以接收方手机号码作为公钥加密信息，接收方以存储在手机中的私钥解密。

秘密密钥(或私钥)的泄漏是密码系统中最致命的攻击，表明会失去所有的安全保障。随着便携式移动设备(如智能卡、移动电话)的广泛使用，其威胁日益严重。对攻击者来说，与解决密钥系统的数学难题相比，获得移动设备并取得其密钥容易得多，因此，构建一个实用的公钥加密方案必须解决私钥的泄漏问题。

在传统的PKI中，通过证书的吊销机制来减轻私钥的泄漏带来的危害。在IBE中，密钥吊销(或更新)问题在实践中同样不可避免。文献[2]提出了通用的针对IBE的密钥吊销方案。该方案要求在用户和可信的第三方——私钥生成器(Private Key Generator，PKG)之间交互式通信，失去了IBE的主要优势。除此之外，自1984年来的许多基于身份的密码系统都没能有效地解决密钥吊销问题。设计基于身份的非交互式密钥吊销和更新方案是IBE中一个具有挑战性的问题。

本文设计了具有密钥非交互式更新的IBE方案，通过前向安全来实现基于身份的非交互式密钥更新；给出了非交互式密钥更新的IBE方案的定义及安全性定义；基于已有的二叉树加密，构造了基于身份的二叉树加密方案；在此基础上，给出了非交互式密钥更新的IBE方案的一个具体的构造。

1 模型和定义

IBE-NIKU方案基于密钥进化技术，通过前向安全达到基于身份的非交互式密钥更新。

密钥进化技术使密钥泄漏带来的危害最小化，前向安全[3]、密钥绝缘[4]、入侵弹性[5]等都属于这类技术。在密钥进化中，系统的生命周期被分成N个时间段，记为$0,1,\cdots,N-1$，秘密密钥随时间进化；消息

收稿日期：2006 – 01 – 15
作者简介：杨浩淼(1974 –)，男，博士生，主要从事信息安全和密码算法等方面的研究.

M在时间段i加密的密文记为(i,C)；所有的密码计算都由设备自身完成。

在前向安全模型中秘密密钥存储于单个设备，在每个时间周期开端由设备自身来更新。攻击者在周期t获得密钥，在$t'\geq t$的所有周期都能签名或者解密；但在$t'<t$的任何周期，系统仍然是安全的。如果发生了密钥泄漏则后果比较严重，这是因为所有的秘密信息都存储在单个设备中。而在密钥绝缘和入侵弹性模型中，一部分秘密密钥信息需要存储在服务器(或帮助设备)上，服务器阶段性地与用户交互以更新密钥。

目前，大部分密钥进化方案的安全性都是基于双线性(Bilinear Diffie-Hellman，BDH)问题，可容许的双线性映射是BDH问题的基础。假定G_1、G_2均为阶为q的循环群，$P,Q\in G_1$, $a,b\in Z_q^*$。双线性映射$\hat{e}$为：$G_1\times G_1\to G_2$如果满足下面的条件，则称为可容许的双线性映射：(1) 双线性，$\hat{e}(aP,bQ)=\hat{e}(P,Q)^{ab}$；(2) 非退化性，如果$P$是$G_1$的生成元，则$\hat{e}(P,P)$是$G_2$的生成元；(3) 可计算性，存在有效算法计算$\hat{e}(P,Q)$。

本文将用户id在时间周期i的公钥标记为$<id, i>$；对应的秘密密钥为$SK_{<id, i>}$；消息空间为 $\mathcal{M}$；密文空间为$\mathcal{C}$。令$C\in\mathcal{C}$，$M\in\mathcal{M}$。

定义 1(IBE-NIKU)　非交互式密钥更新的基于身份加密(Identity-Based Encryption with Non-Interactive Key Update，IBE-NIKU)方案包含下面的多项式时间算法(Setup, InitKey, Update, Encryption, Decryption)：

(1) Setup(1^k, N)= $<s, p>$，其中，k为安全参数；N为总的时间周期数；p为公开的系统参数；s为只有PKG知道的主密钥。

(2) InitKey(p, id)= $SK_{<id, 0>}$，$SK_{<id, 0>}$为用户id的初始化私钥。Setup和InitKey仅由PKG运行，且PKG通过认证的安全信道把初始化私钥发送到用户id。

(3) Update(i+1, $SK_{<id, i>}$)= $SK_{<id, i+1>}$，输入周期i的私钥，输出周期i+1的私钥。

(4) Encryption(p, $<id, i>$, M) = C，其中，$<id, i>$为接收方的公钥。

(5) Decryption(p, $SK_{<id, i>}$,$<id, i>$, C)=M，其中，$SK_{<id, i>}$是接收方的私钥。加密和解密必须满足一致性限制。

安全性定义 (1) 密钥生成Oracle：$KG(\cdot)$。攻击者提交$<id, i>$，该Oracle运行$SK_{<id,i>}\leftarrow$Update (i–1,$\cdots$, Update(1,$SK_{<id, 0>}\cdots$)，并返回$SK_{<id, i>}$给攻击者。(2) 左-右加密Oracle：$LR(\cdot,\cdot,\cdot,p,b)$。攻击者提交$<id, i>$和两条等长度消息$M_0$、$M_1$，该Oracle运行$C^*\leftarrow$Encryption ($p$, $<id, i>$, M_b)，并返回质询密文C^*给攻击者，$b\in_R\{0, 1\}$。

定义 2(fs-CPA)　对IBE-NIKU方案，定义攻击者A的成功概率为：

$$\mathrm{Succ}_{\mathrm{A,IBE\text{-}NIKU}}=\Pr[(p,s)\leftarrow\mathrm{Setup9}(1^k,N);b\in_R\{0,1\};$$
$$b'\leftarrow A^{KG(\cdot),LR(\cdot,\cdot,\cdot,p,b)}:b'=b]$$

式中　A发布$KG(<id, i>)$查询和$LR(<id, i>, M_0, M_1, p, b)$查询，$0\leq j<i<N$。如果对任何概率多项式时间(Probabilistic Polynomial Time, PPT)的攻击者A，$|\mathrm{Succ}_{\mathrm{A,IBE\text{-}NIKU}}-1/2|$是可忽略量，则IBE-NIKU是fs-CPA安全的。

2　基于身份的BTE方案

2.1 BTE方案的构建

IB-BTE用来构建IBE-NIKU，它是基于BTE[3]的，但对BTE有以下改进：(1) 融入了IBE的概念，这是构建IBE-NIKU的关键。(2) 引入了密码学Hash函数H_2，消除了消息$M\in G_2$的限制。(3) 加解密的计算量正比于i(结点位于二叉树的第i层)。

假定读者熟悉BTE方案，每个用户都有自己的二叉树。$<id, w>$为标记二叉树的结点，根结点为$<id, \varepsilon>$，id表示用户的身份，ε 代表空字符串。假定二叉树的高度为l，如果深度小于l的结点为$<id, w>$，则它的左孩子为$<id, w_0>$，右孩子为$<id, w_1>$。w的i-bit前缀为$w|_i$，即$w|_i=w_1, w_2,\cdots, w_i$。令$|w|$表示$w$的比特长度，$<id, w>$的秘密密钥为$SK_{<id, w>}\in G_1$，“翻译点”$R_{<id, w>}\in G_1$。翻译点仅用来解密操作，不需要秘密保存。

定义 3(IB-BTE)　基于身份的二叉树加密(Identity-Based Binary Tree Bncryption，IB-BTE)方案是多项式时间算法的五元组(Gen, Init, Der, Enc, Dec)。

(1) Gen(1^k,N)=$<params, s>$，$params$=$<G_1, G_2, q, \hat{e}, H, H_2, n, P, R>$。

运行BDH参数生成器$IG(1^k)$，输出阶为素数q的群G_1、G_2和可容许的双线性映射$\hat{e}$；随机选择生成元$P\in_R G_1$，随机选择$s\in_R Z_q$，并设置$R=sP$；选择密码学Hash函数H: $\{0,1\}^*\to G_1^*$，H_2: $G_2\to\{0,1\}^n$。安全分析视H, H_2为随机Oracle。消息空间$M=\{0,1\}^n$，密文空间$C=G_1^*\times\{0,1\}^n$。系统参数$params=<G_1, G_2, \hat{e}, n, P; R, H, H_2>$，主密钥为$s$。

(2) Init(s, id) = $SK_{<id, \varepsilon>}$ 给定字符串$id\in\{0,1\}^*$，该算法输出初始化密钥：$SK_{<id, \varepsilon>}=sH(id\|\varepsilon)=sH(id)$。

(3) Der($params$, $<id, w>$, $SK_{<id, w>}$) = $<SK_{<id, w_0>}$,

$SK_{<id, w_1>}$, $R_{<id, w_0>}$, $R_{<id, w_1>}$。

随机选择$\rho_{<id, w_0>}$, $\rho_{<id, w_1>} \in_R Z_q$，设置$R_{<id, w_0>} = \rho_{<id, w_0>}P$，$R_{<id, w_1>} = \rho_{<id, w_1>}P$，计算$SK_{<id, w_0>} = SK_{<id, w>} + \rho_{<id, w_0>}H(id \| w_0)$，$SK_{<id, w_1>} = SK_{<id, w>} + \rho_{<id, w_1>}, H(id \| w_1)$。

(4) Enc(*params*, <*id*, *w*>, *M*) = *C*

随机选择$\gamma \in_R Z_q$，输出$C=(\gamma P, \gamma H(id\|w|_1), \gamma H(id\|w|_2), \cdots, \gamma H(id\|w), M \oplus H_2(d)), d=\hat{e}(R, H(id))^{\gamma}$。

(5) Dec(*params*, <*id*, *w*>, $SK_{<id, w>}$, *C*) = *M*

令$C=(U_0, U_1, \cdots, U_{|w|}, v)$，计算$M=v \oplus H_2(d)$，其中，$d=\dfrac{\hat{e}(U_0, SK_{\langle id,w\rangle})}{\prod_{i=1}^{|w|}\hat{e}(U_i, R_{\langle id,w|_i\rangle})}$。

2.2 安全性分析

本文需验证加密和解密满足一致性限制，即加密时，有：

$$d = \hat{e}(R, H(id))^{\gamma} = \hat{e}(P, H(id))^{\gamma s}$$

解密时，有：

$$U_0 = \gamma P, U_i = \gamma H(w|_i)$$

因此对$i \geq 1$，有：

$$d = \frac{\hat{e}(U_0, SK_{\langle id,w\rangle})}{\prod_{i=1}^{|w|}\hat{e}(U_i, R_{\langle id,w|_i\rangle})} = \frac{\hat{e}(\gamma P, sH(id) + \sum_{i=1}^{|w|}\rho_{\langle id,w|_i\rangle}H(id\|w|_i))}{\prod_{i=1}^{|w|}\hat{e}(\gamma H(id\|w|_i), \rho_{\langle id,w|_i\rangle}P)} = \frac{\hat{e}(P, H(id))^{\gamma s}\prod_{i=1}^{|w|}\hat{e}(P, H(id\|w|_i))^{\gamma\rho_{\langle id,w|_i\rangle}}}{\prod_{i=1}^{|w|}\hat{e}(H(id\|w|_i), P)^{\gamma\rho_{\langle id,w|_i\rangle}}} = \hat{e}(P, H(id))^{\gamma s}$$

所以解密能正确地恢复出消息*M*。

2.3 性能分析

(1) 存储要求：从根到结点<*id*, *w*>需存储密钥和翻译点共2|*w*|+2个G_1元素。

(2) 安全性：类似于BTE[3]的证明，IB-BTE方案也是*SN-CPA*安全的。

(3) 效率：在IB-BTE中，PKG运行的Setup算法时间复杂度为$O(\text{poly}(k))$，poly(*k*)表示*k*的多项式。PKG为每个用户运行Init算法，运行时间包括G_1中的1次乘法和调用1次Hash函数$H(\ )$。Der包括G_1中的4次乘法和2次$H(\ )$。位于*i*层结点的Enc算法包括G_1中的*i*+1次乘法，*i*次$H(\ )$，1次$\hat{e}(\cdot,\cdot)$，1次$H_2(\ )$，以及G_2中的1次异或和1次乘幂运算。*i*层结点的Dec算法包括*i*+1次$\hat{e}(\cdot,\cdot)$，1次$H_2(\ )$，以及G_2中的*i*次乘法，1次除法，和1次异或运算。

3 构建IBE-NIKU方案

3.1 IBE-NIKU方案的构建

在基于IB-BTE、IBE-NIKU方案中，为简单起见，假定全部时间周期数*N*是2的乘幂，$N = 2^l$，则IB-BTE是深度为*l*的完全二叉树。对用户*id*的IB-BTE树进行前序遍历，映射结点<*id*, *w*>到时间周期<*id*, *i*>，<*id*, *i*>为前序遍历的第*i*个结点。

IB-BTE树的前序遍历定义为：<*id*, 0> = <*id*, *ε*>。对$i > 0$，如果<*id*, *i*>所对应的<*id*, *w*>是非叶子结点($|w| < l$)，则<*id*, *i*+1> = <*id*, w_0>；如果该<*id*, *w*>是叶子结点($|w|=l$)，则<*id*, *i*+1> = <*id*, w_1'>，其中<*id*, w_0'>是<*id*, *i*>的最长前缀。

给定IB-BTE方案(Gen, Init, Der, Enc, Dec)，构建IBE-NIKU方案如下：

(1) 算法Setup(1^k, *N*)运行Gen(1^k, *N*)，得到*params*，输出*p* = *params*。

(2) 算法InitKey(*p*, *id*)运行Init(*p*, *id*)时，得到了$SK_{<id, \varepsilon>}$，输出$SK_{<id, 0>} = SK_{<id, \varepsilon>}$。

(3) 算法Update(*i*+1, $SK_{<id, i>}$)。私钥以堆栈的方式组织，$SK_{<id, i>}$在栈顶。当前密钥$SK_{<id, i>}$出栈，如果<*id*, *i*>所对应的<*id*, *w*>是叶子结点($|w| = l$)，则下一个出栈的就是$SK_{<id, i+1>}$。否则调用Der(*p*,<*id*, *w*>, $SK_{<id, w>}$)，先$SK_{<id, w_1>}$入栈，再$SK_{<id, w_0>}$入栈。则新栈顶是$SK_{<id, w_0>}$(<*id*, *i*+1> = <*id*, w_0>)。无论<*id*, *w*>是否叶子结点，最后Update算法都要删除$SK_{<id, w>}$，以保证前向安全。

(4) 算法Encryption(*p*,<*id*, *i*>, *M*)运行Enc(*p*, <*id*, *w*>, *M*)。

(5) 算法Decryption(*p*, $SK_{<id, i>}$,<*id*, *i*>, *C*)运行Dec(*p*, $SK_{<id, w>}$, <*id*, *w*>, *C*)。

3.2 安全性分析

类似于文献[3]中的证明方式，在随机Oracle模型中，假定底层的IB-BTE方案是SN-CPA安全，则可以证明IBE-NIKU方案是fs-CPA安全的。通过Fujisaki-Okamoto转换[6]，还能取得更严格的fs- CCA安全[7]。

3.3 性能分析和实现

(1) 效率 IBE-NIKU方案中的任何一个操作至多要求一个底层IB-BTE中的操作，因此IBE-NIKU具有与IB-BTE一样的复杂性。

(2) 实现 IBE-NIKU方案是基于MIRACL软件包(http://indigo.ie/~mscott/)。MIRACL软件包通过C或C++语言实现了密码学中所必须的大数运算和数论函数，并支持ECC，可针对不同的处理器(包括32 b

的ARM)进行优化。

4 结 束 语

本文通过前向安全来实现基于身份的非交互式密钥更新，方案简单，只需用户自身来更新密钥，适合于对安全性要求不高的环境。还可通过入侵弹性实现基于身份的非交互式密钥更新，该方案提供更强的安全性，但需要引入与网络无连接的、计算资源和存储资源受到限制的私有设备来帮助更新密钥，需要进一步的研究。

参 考 文 献

[1] SHAMIR A. Identity-based cryptosystems and signature schemes[C]//Proc. of Crypto'84, LNCS 196. Berlin: Springer-Verlag, 1985: 47-53.

[2] BONEH D, FRANKLIN M. Identity-based encryption from the Weil pairing[C]//Proc. of Crypto'01, LNCS 2139. Berlin: Springer-Verlag, 2001: 213-229.

[3] CANNETI R, HALEVI S, KATZ J. A forward secure public key encryption scheme[C]//Proc. of Eurocrypt'03, LNCS 2656.Berlin: Springer-Verlag, 2003: 255-271.

[4] DODIS Y, KATZ J, XU S. Key-insulated public key cryptosystems[C]//Proc. of Eurocrypt'02, LNCS 2332. Berlin: Springer-Verlag, 2002: 65-82.

[5] DODIS Y, FRANKLIN M, KATZ J. Intrusion-resilient public-key encryption[C]//Proc. of CT-RSA'03, LNCS 2612, Berlin: Springer-Verlag, 2003:19-32.

[6] FUJISAKI E, OKAMOTO T. Secure integration of asymmetric and symmetric encryption schemes[C]//Proc. of Crypto'99, LNCS 1666. Berlin: Springer-Verlag, 1999: 537-554.

[7] 毛文波. 现代密码学: 理论与实践[M]. 北京: 电子工业出版社, 2004.

编 辑 黄 莘

(上接第530页)

5 结 论

本文将粗糙集理论引入数据库的推理泄漏控制，可以提取出数据库中非敏感和敏感数据之间蕴含的确定性推理规则。根据这些规则和属性的重要程度，在保证数据库推理泄漏控制的前提下，实现发布给用户数据量修改的最小化。同现有方法相比，该方法计算量小，可扩展性强，在保证大规模数据库可用的同时，增加了数据库的安全性。

参 考 文 献

[1] MARKS D. Inference in MLS database system[J]. IEEE Trans Knowledge and Data Eng, 1996, 8(1): 46-55.

[2] DAWSON S, VIMERCATI S D C. Minimal data upgrading to prevent inference and association attacks[C]// In: Proceedings of the Eighteenth ACM SIGACT-SIGMOD-SIGART Symposium on Principles of Database Systems. Pennsylvania: ACM Press, 1999: 114-125.

[3] SHAFER G. Detecting inference attacks using association rules[J/OL]. http://www. glennshafer. com/courses/ downloads/ raman.pdf, 2004-04-18.

[4] CHANG L, MOSKOWITZ S. A study of inference problem in distributed database systems[C]//In: Proceedings of IFIP Data Security and Applications. Cambridge, UK: Cambridge Uni. Press, 2002: 229-243.

[5] 刘 清. Rough集及Rough推理[M]. 北京: 科学出版社, 2001.

[6] ULLMAN J D. Principle of database and knowledge-base system, Vols. I and II[M]. Rockville, MD: Computer Science Press, 1988,1989.

编 辑 漆 蓉

(上接第533页)

参 考 文 献

[1] DENNING D E. Secure information flow in computer systems[D]. W. Lafayette, Ind.: Purdue Univ., 1975.

[2] DENNING D E. A lattice model of secure information flow[J]. COMM ACM, 1976, 19(5): 236-243.

[3] DENNING D E, DENNING P J. Certification of program for secure information flow[J]. COMM ACM, 1977, 20(7): 504-513.

[4] 肖军模, 刘 军, 周海刚. 网络信息安全[M]. 北京: 机械工业出版社, 2006

[5] 肖军模. 对军用安全模型的扩展[J]. 电子科技大学学报, 2005, 34(2): 186-189.

[6] 江义华. JAVA完美经典[M]. 北京: 中国铁道出版社, 2004.

编 辑 黄 莘