ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.19, No.8, August 2008, pp.2159−2166
DOI: 10.3724/SP.J.1001.2008.02159

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

基于Weil对的多接收者公钥加密方案*

鲁 力+, 胡 磊

(中国科学院 研究生院 信息安全国家重点实验室,北京 100049)

Multi-Recipient Public Key Encryption Scheme Based on Weil Pairing

LU Li+, HU Lei

(State Key Laboratory of Information Security, Graduate University, The Chinese Academy of Sciences, Beijing 100049, China)

+ Corresponding author: E-mail: lulirui@gmail.com

Lu L, Hu L. Multi-Recipient public key encryption scheme based on Weil pairing. *Journal of Software*, 2008, 19(8):2159−2166. http://www.jos.org.cn/1000-9825/19/2159.htm

Abstract: This paper proposes a multiple-recipient public key encryption, called pairing-based multi-recipient encryption (PBMRE). The proposed scheme is constructed on Weil pairing on elliptic curves and the Shamir's secrets sharing scheme. As a result, a private key for decryption can be converted to multiple users' private keys by secrets sharing, and reconstructed by the bilinear property of Weil Pairing in decryptions. Through an analysis, it is shown that this scheme is efficient and can effectively defend against deciphers' collaborating. Based on the Gap-BDH (gap-bilinear Diffie-Hellman) assumption and the random oracle model, a strict security proof is presented stating that the scheme has the indistinguishability under adaptive chosen ciphertext attack,简称 (IND-CCA2).

Key words: multi-recipient public key encryption; secret sharing; Weil pairing; Gap-BDH (gap-bilinear Diffie-Hellman) assumption

摘 要: 提出了一种多接收者公钥加密方案,称为基于双线性映射的多接收者公钥加密(pairing-based multi-recipient encryption,简称 PBMRE).该方案使用椭圆曲线上的 Weil 对和 Shamir 的秘密分享方法来构造.利用秘密分享方法处理私钥,可以将一个解密私钥转换成多个用户私钥.利用 Weil 对的双线性,在解密时可以重新组合解密私钥.经过分析,给出的多接收者公钥加密方案效率高,并且能抵抗多个接收者的合谋攻击.基于间隙双线性 Diffie-Hellman 假设,证明了该体制具有抗自适应选择密文攻击的不可区分安全性(indistinguishability under adaptive chosen ciphertext attack,简称 IND-CCA2).

关键词: 多接收者公钥加密;秘密分享;Weil 对;间隙双线性 Diffie-Hellman 假设

中图法分类号: TP309 **文献标识码**: A

Internet 的发展促进了对广播传输服务的需求,例如,在付费电视应用中,提供服务的公司希望只有授权用户才能享受服务,而用户也希望他们收到的服务内容不会暴露给未获授权的用户.因此,产生了对安全广播传输的需求.对于安全广播,大多数密码体制的实现方法如下:

* Supported by the National Natural Science Foundation of China under Grant Nos.60373041, 60573053 (国家自然科学基金)
Received 2006-11-09; Accepted 2007-03-19

假设有 n 个接收者,记为 1,...,n,每个接收者的公、私钥对记为(pk_i,sk_i).对于发送给接收者 i 的明文 M_i,发送者用 i 的公钥 pk_i 加密为 C_i.在进行了 n 次加密后,发送者将密文 $C=C_1,...,C_n$ 广播.接收者 i 收到密文 C 后,将子密文 C_i 提取出来,并使用私钥 sk_i 解密获得明文 M_i.这样的公钥加密被称为多接收者公钥加密体制[1−3].

对于广播加密,可以使用上面所述的多接收者加密体制来构造.即对明文 M,使用每个接收者的公钥 pk_i,i=1,...,n,分别加密 n 次,并将(C_1,...,C_n)作为密文广播[2,3].但是,该体制对于每个明文 M 至少需要 n 次加密运算,效率很低.

在本文中,我们基于椭圆曲线上的 Weil 对构造了一种多接收者公钥加密方案,称为基于 Weil 对的多接收者公钥加密(pairing-based multi-recipient encryption,简称 PBMRE).该方案的主要思想是将单个解密钥拆分到多个私钥集合中,每个私钥集合对应一个解密者.我们使用 Shamir 的秘密分享方案来分拆解密钥,以使不同的解密者获得不同的解密钥.

基于双线性 Diffie-Hellman 问题的困难性,我们在标准模型[4]下证明了 PBMRE 具有抗选择明文攻击的语义安全性(indistinguishability under chosen plaintext attack,简称 IND-CPA).并且,基于间隙双线性 Diffie-Hellman (gap-bilinear Diffie-Hellman,简称 Gap-BDH)困难假设,我们在随机谕示(random oracle)模型下证明了 PBMRE 的扩展方案具有抗自适应选择密文攻击的语义安全性(indistinguishability under adaptive chosen ciphertext attack,简称 IND-CCA2).经过分析,我们的体制还能抵抗解密者的合谋攻击:即使所有的解密者合谋,他们也不能恢复完整的解密私钥.

本文第 1 节介绍相关工作.第 2 节为背景知识.第 3 节详细描述 PBMRE 的构造.第 4 节讨论方案的效率和抗合谋攻击的安全性.第 5 节给出 PBMRE 的严格安全性证明.第 6 节总结全文.

1 相关工作

多接收者公钥加密的概念最初是由 Bellare 和 Baudron 等人[1,5]提出来的.他们的结论表明,在单接收者情况下,公钥加密方案的安全性可以推广到多接收者情况.因此,语义安全的多接收者公钥加密方案可以简单地用单接收者情况下语义安全的加密方案来构造.其主要思想为:使用 n 个不同的公钥对同一明文加密 n 次得到广播密文,接收者再使用自己的私钥解密该广播密文.显然,对于一条广播消息,该方案需要加密 n 次,不适用于大规模的消息广播.后来,Kurosawa[3]提出了一种称为随机性重用的技术来提高基于 ElGamal[6]的多接收者公钥加密方案的效率.Bellare 等人[2]改进了 Kurosawa 的结果,并提出了一般化的测试方法以判定一个单接收者方案是否可以使用随机性重用技术来构造高效的多接收者方案.但是,他们的方法只是以提高多次重复加密的效率为目的,未能实现单一加密公钥对应多个解密私钥的功能,因此,加密效率的提高很有限.

从 2001 年第一个实用的基于身份的公钥加密体制[7]提出以后,出现了一些基于身份的多接收者公钥加密方案,如 Chen[8]和 Smart[9]等人的方案.但是,这些工作都没有给出适当的形式化安全性模型及安全性证明.Mu[10]和 Baek[11]分别在 2003 年和 2005 年给出了两个具有形式化安全性证明的基于身份多接收者公钥加密体制,但 Mu 的方案正确性存在问题.目前看来,正确且有形式化安全性证明的方案仅有 Beak 的方案[11].

本文的主要贡献在于,与 Baek 的基于身份的多接收者公钥加密方案相比,给出了一个一般的(不以基于身份公钥加密方案为基础)多接收者公钥加密方案,实现了一个加密公钥对应多个解密私钥的功能,并且给出了严格的形式化安全模型和安全证明.与一般的多接收者公钥加密方案相比,本文的方案对广播消息仅需要 1 次公钥加密,但可以使用多个不同的解密钥解密,效率获得了极大的提高.

2 背景知识

下面介绍在构造和分析 PBMRE 方案中所用到的数学工具和困难性假设.

定义 1. 双线性 Diffie-Hellman 判定假设(BDDH(bilinear determination Diffie-Hellman assumption)假设).设 G_1 和 G_2 分别是加法和乘法群,其阶均为素数 p.设 p 为 G_1 的生成元.假设 $e:G_1\times G_1\to G_2$ 为双线性映射,即对所有的 $Q,R\in G_1$ 和 $a,b\in Z_p$ 满足 $e(aQ,bR)=e(Q,R)^{ab}$,并且 $e(P,P)\neq 1$[7].假定挑战者随机选择 $a,b,c,z\in Z_p$,如果不存在多项

式时间算法能以不可忽略的概率区分四元组$(aP,bP,cP,e(P,P)^{abc})$和$(aP,bP,cP,e(P,P)^{z})$,则 BDDH 假设对(G_1,G_2,e)成立.

定义 2. 间隙双线性 Diffie-Hellman 问题(Gap-BDH problem)[11].设 G_1,G_2 和 e 如定义 1 中所示.给定(P,aP,bP,cP),在双线性 Diffie-Hellman 判定谕示(BDDH oracle)的帮助下,求解 $e(P,P)^{abc}$ 即为 Gap-BDH 问题.其中,BDDH 谕示如下:输入$(P,aP,bP,cP,\mathcal{K})$,如果 $\mathcal{K}=e(P,P)^{abc}$,则 BDDH 谕示输出 1,否则输出 0.

若 A 为敌手,其求解 Gap-BDH 问题的优势定义为

$$Adv_A^{Gap\text{-}BDH}=\Pr[A^{O_{BDDH}}(P,aP,bP,cP)=e(P,P)^{abc}].$$

设 A 在时间 t 内询问 BDDH 谕示最多 q_0 次,若 A 求解 Gap-BDH 问题的优势不小于ε,则称 A 为 Gap-BDH 问题的(t,q_0,ε)解法.如果 Gap-BDH 问题不存在(t,q_0,ε)解法,则称该问题为(t,q_0,ε)困难的.

除了椭圆曲线点群上的 Weil 对以外,我们构造 PBMRE 的另一个工具是 Shamir 的秘密分享体制[12].秘密分享是将主秘密分成若干碎片,并将这些碎片分布到多个参与者手中,而这些参与者可以使用他们所掌握的碎片恢复主秘密.为便于叙述,我们引入如下记号:

设Γ为有限乘法群 Z_p^* 的子集,其中 p 为素数.设拉格朗日插值多项式$\Delta_{i,\Gamma}(i\in\Gamma)$为

$$\Delta_{i,\Gamma}(x)=\prod_{j\in\Gamma,j\neq i}\frac{x-j}{i-j}.$$

设$|\Gamma|=m$,则 $m-1$ 次多项式 $q(x)\in Z_p[x]$可以描述为

$$q(x)=\sum_{i\in\Gamma}q(i)\Delta_{i,\Gamma}(x).$$

显然,$q(0)=\sum_{i\in\Gamma}q(i)\Delta_{i,\Gamma}(0)$.在 PBMRE 体制中,我们用 $q(0)$表示主秘密.

3 方案描述

我们首先给出一种具有抗选择明文攻击安全性(IND-CPA)的方案 PBMRE-CPA,然后,使用文献[13]中的方法将其扩展为具有抗自适应选择密文攻击安全性(IND-CCA2)的方案 PBMRE-CCA.

3.1 PBMRE-CPA

该方案由 3 种算法组成,分别是密钥生成(key generation)、加密(encryption)和解密(decryption).

Key Generation:选择两个阶均为素数 p 的群 G_1 和 G_2(其中,G_1 为加法群,G_2 为乘法群),使得存在双线性映射 $e:G_1\times G_1\to G_2$,且 G_1 中 Diffie-Hellman 计算问题困难[7].设 P 是 G_1 的生成元.随机选择两个元素 $Q,R\in G_1$.

假设 E 为消息加密者(即发送者),存在 d 个解密者(即接收者),记为 $D_1,D_2,\ldots,D_d$.设 a 和 b 为两个正整数.在 Z_p 中随机选择 $a+bd$ 个不同的元素,记为 $t_{0,1},\ldots,t_{0,a},t_{1,1},\ldots,t_{1,b},\ldots,t_{d,1},\ldots,t_{d,b}$.并设

$$EC=\{t_{0,1},\ldots,t_{0,a}\},\ DC_j=\{t_{j,1},\ldots,t_{j,b}\}.$$

随机选择 $s\in Z_p$ 作为主秘密.设 $m=a+b$,随机选择 $m-1$ 次多项式 $q(x)\in Z_p[x]$,其常数项为 s,即 $q(0)=s$.计算 $EK=\{q(t_{0,1})P,\ldots,q(t_{0,a})P\}$,$DK_j=\{q(t_{j,1})(R+Q),\ldots,q(t_{j,b})(R+Q)\}$.最后计算 $P_0=sP$ 并输出公共参数$(p,G_1,G_2,e,P,Q,R,P_0,EC)$.接收者 D_j 获得解密私钥 DK_j.

Encryption:随机选择 $r\in Z_p^*$ 并计算密文:

$$(U,V,W,X)=(rP,rQ,e(P_0,R)^r\cdot M,r\cdot EK).$$

其中,$r\cdot EK=\{rq(t_{0,1})P,\ldots,rq(t_{0,a})P\}$.

Decryption:每个接收者 D_j 知道$\Gamma=EC\cup DC_j$.因此,对每个 $i\in\Gamma$,D_j 可以计算出$\Delta_{i,\Gamma}(0)$.于是,D_j 计算明文:

$$M=\frac{e(V,P_0)\cdot W}{\prod_{i=1}^{a}e(R+Q,rq(t_{0,i})P)^{\Delta_{0,i,\Gamma}(0)}\cdot\prod_{k=1}^{b}e(q(t_{j,k})(R+Q),U)^{\Delta_{j,k,\Gamma}(0)}}.$$

通过 Weil 对的双线性和拉格朗日插值,容易验证上式等于

$$\frac{e(V,P_0)\cdot W}{e(R+Q,sP)^r}=\frac{e(Q,P_0)^r\cdot W}{e(R,P_0)^r\cdot e(Q,P_0)^r}=\frac{W}{e(R,P_0)^r}=\frac{e(R,P_0)^r\cdot M}{e(R,P_0)^r}=M.$$

3.2 PBMRE-CCA

该方案同样由 3 个算法组成:密钥生成(key generation)、加密(encryption)和解密(decryption).

Key Generation:选择两个哈希函数 $H_1:G_2\to\{0,1\}^{l_1}$ 和 $H_2:\{0,1\}^*\to\{0,1\}^{l_2}$,其余与 CPA 方案相同.输出公共参数$(p,G_1,G_2,e,P,Q,R,P_0,EC,H_1,H_2)$.

Encryption:分别从 G_2 和 Z_p^* 中随机选择 $S\in G_2$ 和 $r\in Z_p^*$.计算密文 $C=(U,V,W_1,W_2,\sigma,X)$如下:

$$(rP,rQ,e(P_0,R)^r\cdot S,M\oplus H_1(S),H_2(S,M,U,V,W_1,W_2),r\cdot EK).$$

Decryption:对解密者 D_j,由$\Gamma=EC\cup DC_j$,D_j对每个 $i\in\Gamma$计算$\Delta_{i,\Gamma}(0)$.将密文分拆为(U,V,W_1,W_2,σ,X)的形式后,D_j计算:

$$S'=\frac{e(V,P_0)\cdot W_1}{\prod_{i=1}^{a}e(R+Q,rq(t_{0,i})P)^{\Delta_{0,i,\Gamma}(0)}\cdot\prod_{k=1}^{b}e(q(t_{j,k})(R+Q),U)^{\Delta_{j,k,\Gamma}(0)}},$$

$$M'=W_2\oplus H_1(S'),$$

$$\sigma'=H_2(S',M',U,V,W_1,W_2).$$

验证$\sigma'=\sigma$是否成立,如果成立,则接收 M'为合法明文;否则拒绝该密文.

4 讨 论

在本节中,我们讨论抵抗解密者合谋攻击的安全性和算法效率.

4.1 合谋攻击

如上一节中所述,$m-1$ 次多项式 $q(x)\in Z_p[x]$用来在 $a+bd$ 个碎片中隐藏主秘密 s.由门限秘密分享的性质,$a+bd$ 个碎片中任取 m 个可以恢复主秘密 s,但少于 m 个就得不到 s 的任何信息.显然,由于 $b<m$,任何一个解密者 D_j 都不能恢复主秘密 s.另外,若 $bd<m$,则即使所有的解密者合谋也不能恢复主秘密 s.

由 $bd<m$ 和 $a+b=m$,我们可以得到 $a>b(d-1)$.如果 $b=1$,则 $a=b=m-1$ 为加密者保留的主秘密碎片的最小数目.当然,我们可以选择任意满足 $b>1$ 和 $a>b(d-1)$的参数(a,b,d),但是这样会降低通信和计算效率.

4.2 计算效率

加密一个明文 M,PBMRE 需要 1 次 Weil 对的计算(如果预先计算 $e(P_0,R)$则加密时无须计算 Weil 对)、$a+2$ 次椭圆曲线点群 G_1 上的倍点运算(计算 $rP,rQ,rq(t_{0,1})P,\ldots,rq(t_{0,a})P$)和 1 次乘法群 G_2 上的指数运算(计算 $e(P_0,R)^r$).

在解密时,PBMRE 看似需要 $m=a+b$ 次 Weil 对的计算,但是,我们可以将解密过程写成如下形式(这里仅以 PBMRE-CPA 为例,在 PBMRE-CCA 中类似的变化也成立):

$$M=\frac{e(V,P_0)\cdot W}{e\left(R+Q,\sum_{i=1}^{a}\Delta_{0,i,\Gamma}(0)\cdot rq(t_{0,i})P\right)\cdot e\left(\sum_{k=1}^{b}\Delta_{j,k,\Gamma}(0)\cdot q(t_{j,k})(R+Q),U\right)}.$$

解密过程修改后,我们只需要 3 次 Weil 对的运算、$a+b$ 次点乘运算(计算 $\Delta_{0,i,\Gamma}(0)\cdot rq(t_{0,i})P$,$1\le i\le a$ 和 $\Delta_{j,k,\Gamma}(0)\cdot q(t_{j,k})\cdot(R+Q)$,$1\le k\le b$)和 3 次 G_2 中的运算(2 次乘法和 1 次除法).

5 安全性证明

本节给出 PBMRE-CPA 和 PBMRE-CCA 的安全性证明.首先,在标准模型下,我们在双线性 Diffie-Hellman 假设(BDDH)下证明 PBMRE-CPA 具有 IND-CPA 安全性;然后,在随机谕示模型下,基于间隙 Diffie-Hellman 假设,

我们证明 PBMRE-CCA 具有 IND-CCA2 安全性.

定理 1. 如果存在攻击 PBMRE-CPA 的 IND-CPA 多项式时间敌手 A,其优势为 ε,运行时间为 t,则以 A 为子程序可以构造求解 BDDH 问题的算法,其优势为 $\frac{1}{2}\varepsilon$,运行时间为 $t'=O(t)$.

证明:我们以 A 为基础来构造求解 BDDH 问题的算法 B.

设 BDDH 问题的实例$(P,G_1,G_2,e,aP,bP,cP,Z_0,Z_1)$,其中,$Z_0=e(P,P)^{abc}$,$Z_1=e(P,P)^z$,$z$ 为 Z_p^* 中随机选择的元素.记算法 B 区分(P,aP,bP,cP,Z_0)和(P,aP,bP,cP,Z_1)的优势为 ε'.设 B 的运行时间为 t'.B 按照如下方法生成一个 CPA 方案实例.

B 选择合适的参数 α,β,d 和 m,满足 $\beta<m$,$\beta d<m$ 和 $\alpha+\beta=m$.这里,d 表示解密者个数.

Phase 1: B 设 $P_0=aP$ 和 $R=bP$.随机选择 $\gamma\in Z_p^*$ 和 $m-1$ 次多项式 $q(x)\in Z_p[x]$.另外,B 随机选择 Z_p^* 的一个子集,记为 EC,使得$|EC|=\alpha$.然后,B 计算 $Q=\gamma P$ 并输出系统公共参数$(p,Q,R,P,P_0,e,G_1,G_2,EC)$给 A.

Challenge Phase: A 选择两个等长明文 M_0 和 M_1 并发送给 B.B 收到后按如下过程生成目标密文 C^*:

- 随机选择 $u,v\in\{0,1\}$;
- 返回 $C^*=(cP,\beta cP,Z_v\cdot M_u,\{q(i)\cdot cP|i\in EC\})$.

对于 Z_v,如果 $v=0$,因为 $Z_v\cdot M_b=e(P,P)^{abc}\cdot M_b=e(aP,bP)^c\cdot M_b=e(P_0,R)^r\cdot M_u$,则 C^* 是 M_u 的合法密文.如果 $v=1$,则 $Z_v\cdot M_u=e(P,P)^z\cdot M_u$.由于 z 的随机性,A 不能得到关于 u 的任何信息.

Guess:收到 A 的猜测 u'后,如果 $u'=u$,则 B 输出(P,aP,bP,cP,Z_v)作为正确的 BDDH 组;否则输出(P,aP,bP,cP,Z_{1-v}).

我们分析 B 的优势.

如果 $v=1$,则 A 不能得到关于 u 的任何信息.因此, $\Pr[u'=u\mid v=1]=\Pr[u'\neq u\mid v=1]=\frac{1}{2}$, 并且 B 猜测正确的 BDDH 组的成功概率是 $\Pr[B\ Success\mid v=1]=\frac{1}{2}$.

如果 $v=0$,B 返回 M_u 的合法密文.由定理中所述的条件,A 攻击 CPA 方案的优势为 ε.

因此, $\Pr[u'=u\mid v=0]=\frac{1}{2}+\varepsilon$, B 猜测正确的 BDDH 组的成功概率为 $\Pr[B\ Success\mid v=0]=\frac{1}{2}+\varepsilon$.

综上,B 区分 BDDH 组的优势为

$$\begin{aligned}\Pr[B\ Success]-\frac{1}{2}&=\Pr[B\ Success\wedge v=0]+\Pr[B\ Success\wedge v=1]-\frac{1}{2}\\&=\frac{1}{2}\cdot\Pr[B\ Success\mid v=0]+\frac{1}{2}\cdot\Pr[B\ Success\mid v=1]-\frac{1}{2}\\&=\frac{1}{2}\cdot\left(\frac{1}{2}+\varepsilon\right)+\frac{1}{2}\cdot\frac{1}{2}-\frac{1}{2}=\frac{1}{2}\varepsilon.\end{aligned}$$

显然,当 A 攻击过程结束时,B 马上给出计算结果,所以 $t'=O(t)$. □

定理 2. 假设存在多项式时间 t 内攻击 PBMRE-CCA 的 IND-CCA2 敌手 A,其优势为 ε.设 A 对随机谕示 H_1 和 H_2 最多分别作 q_{H_1} 和 q_{H_2} 次查询,并且对解密谕示最多作 q_d 次查询,则以 A 为子程序可以构造算法 B 求解间隙 Diffie-Hellman 问题(Gap-BDH),其优势为 ε',运行时间为 t'.若 l_1 和 l_2 分别代表哈希函数 H_1 和 H_2 的输出长度.那么 $t'=O(t)$, $\varepsilon'\geq\frac{1}{q_{H_2}}\left(\varepsilon-\frac{q_d}{2^{l_1}}\right)\left(1-\frac{q_{H_1}}{2^{l_1}}-\frac{q_{H_2}}{2^{l_2}}\right)$.

证明:在文献[13]中,对公钥加密体制的安全性定义了明文检测攻击下的单向性(oneway-ness under plaintext checking attack,简称 OW-PCA)这一概念.简单来说,一个公钥加密体制称为(t',q_0,ε')安全是指对任何攻击时间为 t'的敌手 B',向明文检测谕示(plaintext checking oracle,简称 PC)最多作 q_0 次查询后,B'找到给定密文所对应的明文的优势不大于 ε'.PC 谕示的输入为明密文对(C,M),如果 C 是 M 的密文,则输出 1,否则输出 0.

在 Gap-BDH 问题困难性假设下,易知 CPA 方案是 OW-PCA 安全.敌手得到公共输入参数中的(P,R,P_0)和给定密文$(U,V,W,r\cdot EK)$后,如果能找到某个明文 M',则通过 PC 谕示检测$(P,U,R,P_0,W/M')$是否为 BDH 组.如果是,则该敌手就攻破了 CPA 方案的单向安全性.以该敌手为子程序,我们可以构造算法来求解 Gap-BDH 问题.

假设一个 IND-CCA2 敌手 A 在多项式时间 t 内攻击 CCA 方案的优势为ε,对 H_1,H_2 和解密谕示最多分别作 q_{H_1},q_{H_2} 和 q_d 次查询.我们以 A 为子程序来构造 CPA 方案的 OW-PCA 敌手 B.

假设 B 得到 CPA 方案的公共参数$(p,Q,P,R,P_0,G_1,G_2,e,EC)$和目标密文 $C^*=(U^*,V^*,W^*,X^*)=(r^*P,r^*Q,e(P_0,R)^{r^*}\cdot S^*,r^*\cdot EK)$.$B$ 模拟 A 的目标系统,与 A 进行如下 IND-CCA2 攻击过程.

Phase 1: B 模拟 IND-CCA2 攻击的公共参数$(p,Q,P,R,P_0,G_1,G_2,e,EC,H_1,H_2)$,并提供给 A.这里,H_1 和 H_2 是由 B 控制的随机谕示,其控制方法如下:

H_1:初始,B 置表 H_1^{list} 为空,表中的数据项格式为(S,K),其中 $K=H_1(S)$.

B 收到 A 的查询 S_j $(1\le j\le q_{H_1})$ 以后:

- 如果(S_j,K_j)已经存在于 H_1 表中,则返回 K_j;
- 否则,用 PC 谕示检测目标密文 $C^*=(U^*,V^*,W^*,X^*)$是否为 S_j 的密文
  - 如果是,则返回 S_j 并终止 A 的攻击过程(B 已经找到目标密文 C^*所对应的明文.B 的攻击成功);
  - 否则,
    - 随机选择 $K_j\in\{0,1\}^{l_1}$;
    - 将(S_j,K_j)放入 H_1^{list} 中,并返回 K_j.

H_2:初始,B 置表 H_2^{list} 为空,表中的数据项格式为(S,M,U,V,W_1,W_2).

B 收到 A 的查询$(S_j,M_j,U_j,V_j,W_{j_1},W_{j_2})(1\le j\le q_{H2})$ 以后:

- 如果 $((S_j,M_j,U_j,V_j,W_{j_1},W_{j_2}),\sigma_j)$ 在表 H_2^{list} 中,则返回σ_j;
- 否则,用 PC 谕示检测目标密文 C^*是否为 S_j 的密文:
  - 如果是,则返回 S_j 并终止 A 的攻击过程(B 已经找到目标密文 C^*所对应的明文);
  - 否则,
    - 随机选择 $\sigma_j\in\{0,1\}^{l_2}$;
    - 将 $((S_j,M_j,U_j,V_j,W_{j_1},W_{j_2}),\sigma_j)$ 放入 H_2^{list} 中并返回σ_j.

Phase 2: B 回答 A 的解密查询如下:

收到一个解密查询$C_j=(U_j,V_j,W_{j_1},W_{j_2},r_j\cdot EK,\sigma_j)(1\le j\le q_d)$以后:

- 如果 $((S_j,M_j,U_j,V_j,W_{j_1},W_{j_2}),\sigma_j)$ 存在于 H_2^{list} 中:
  - 使用 H_1 谕示计算 $H_1(S_j)$并验证 $H_1(S_j)\oplus M_j=W_{j_2}$ 是否成立;
    - 如果不成立,则拒绝该密文 C_j;
    - 如果成立,则使用 PC 谕示验证 $(U_j,V_j,W_{j_1},r_j\cdot EK)$ 是否为 S_j 所对应的密文:
      - 如果是,则返回 M_j;
      - 否则,拒绝该密文.
- 否则,拒绝该密文 C_j.

Phase 3: B 收到 A 发送的两个等长明文(M_0,M_1)以后,用 CPA 方案的目标密文 C^*构造 CCA 的合法密文 C^{**}:

- 随机选择 $b\in\{0,1\}$;
- 随机选择 $K^*\in\{0,1\}^{l_1}$,并置 $H_1(S^*)=K^*$;
- 随机选择 $\sigma^*\in\{0,1\}^{l_2}$,并置 $(S^*,M_b,U^*,V^*,W_{j_1}^*,W_{j_2}^*)=\sigma^*$;
- 返回 $C^{**}=(U^*,V^*,W_{j_1}^*,K^*\oplus M_b,\sigma^*,r^*\cdot EK)$.

Phase 4: B 回答 A 的询问过程与 Phase 1 和 Phase 2 相同.

Phase 5: 收到 A 对 b 的猜测 b'以后,如果 $b'=b$,则 B 在 H_2^{list} 中均匀随机选择一个 S 并输出;如果 $b'\neq b$,则 B 终止,不输出任何信息.

在上面的攻击过程中,B 对解密谕示的模拟与真实环境下近似相同.但有一种情况除外:如果敌手 A 不需要查询 H_2 就能正确猜测到 H_2 输出,那么,A 可以生成合法的密文,但解密谕示会拒绝 A 所提交的合法密文,这与真实环境下的解密谕示不同.该情况发生的概率为 $1/2^{l_2}$.我们记在整个攻击过程中,A 没有查询 H_2 而正确猜测 H_2 输出的事件为 $GuessH_2$.

在与 A 进行上述攻击过程以后,B 在下述情况下会给出目标密文 C^*的正确解密:

1. A 以 S_j 向 H_1 查询 $H_1(S_j)$时,B 发现 C^*是 S_j 对应的密文.该情况发生的概率为 $\frac{q_{H_1}}{2^{l_1}}$.
2. A 以 $(S_j,M_j,U_j,V_j,W_{j_1},W_{j_2})$ 向 H_2 查询 $H_2(S_j,M_j,U_j,V_j,W_{j_1},W_{j_2})$ 时,B 发现 C^* 是 S_j 对应的密文.该情况发生的概率为 $\frac{q_{H_2}}{2^{l_2}}$.
3. 在 A 的攻击过程结束时,如果 A 攻击成功,则 B 在 H_2^{list} 中均匀随机选择一个 S_j 作为目标密文 C^*的明文.这时,$GuessH_2$ 事件没有发生.

将上述 3 个事件分别记作 E_1,E_2 和 E_3,则

$$\begin{aligned}\Pr[B\ Success]&=\Pr[E_1]\Pr[B\ Success\mid E_1]+\Pr[E_2]\Pr[B\ Success\mid E_2]+\Pr[E_3]\Pr[B\ Success\mid E_3]\\&\geq(1-\Pr[E_1]-\Pr[E_2])\Pr[B\ Success\mid E_3]\\&\geq\frac{1}{q_{H_2}}\left(1-\frac{q_{H_1}}{2^{l_1}}-\frac{q_{H_2}}{2^{l_2}}\right)\left(\Pr[b'=b\mid\neg GuessH_2]-\frac{1}{2}\right)\\&\geq\frac{1}{q_{H_2}}\left(1-\frac{q_{H_1}}{2^{l_1}}-\frac{q_{H_2}}{2^{l_2}}\right)\left(\Pr[b'=b]-\Pr[GuessH_2]-\frac{1}{2}\right).\end{aligned}$$

由于在整个攻击过程中,A 最多进行 q_d 次解密询问,所以, $\Pr[GuessH_2]\leq\frac{q_d}{2^{l_2}}$. 因此,

$$\varepsilon'=\Pr[B\ Success]\geq\frac{1}{q_{H_2}}\left(\varepsilon-\frac{q_d}{2^{l_2}}\right)\left(1-\frac{q_{H_1}}{2^{l_1}}-\frac{q_{H_2}}{2^{l_2}}\right).$$

当 A 攻击过程结束时,B 马上给出计算结果,所以 $t'=O(t)$. □

6 结束语

为了实现安全广播中数据机密性的要求,本文给出了一种基于 Weil 对的可证安全的多接收者公钥加密方案(PBMRE).基于间隙双线性 Diffie-Hellman 假设,经过严格安全性证明,该方案具有抗自适应选择密文攻击语义安全性.效率分析表明,与以前的方案相比,该方案加、解密效率更高,并具有可证明安全性的特点,可用于高效的安全数据广播加密.

References:

[1] Bellare M, Boldyreva A, Micali S. Public-Key encryption in a multi-user setting: Security proofs and improvements. In: Preneel B, ed. Advances in Cryptology—EUROCRYPT 2000. Berlin: Springer-Verlag, 2000. 259−274.

[2] Bellare M, Boldyreva A, Staddon J. Multi-Recipient encryption schemes: Security notions and randomness re-use. In: Desmedt Y, ed. Proc. of the Public Key Cryptography—PKC 2003, the 6th Int'l Workshop on Theory and Practice in Public Key Cryptography. Berlin: Springer-Verlag, 2003. 85−99.

[3] Kurosawa K. Multi-Recipient public-key encryption with shortened ciphertext. In: Naccache D, ed. Proc. of the Public Key Cryptography—PKC 2002, the 5th Int'l Workshop on Practice and Theory in Public Key Cryptosystems. Berlin: Springer-Verlag, 2002. 48−63.

[4] Feng DG. Research on theory and approach of provable security. Journal of Software, 2005,16(10):1743−1756 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/16/1743.htm

[5] Baudron O, Pointcheval D, Stern J. Extended notions of security for multicast public key cryptosystems. In: Montanari U, ed. Proc. of the Automata, Languages and Programming, the 27th Int'l Colloquium. Berlin: Springer-Verlag, 2000. 499−511.

[6] ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Trans. on Information Theory, 1985,IT-31(4):469−472.

[7] Boneh D, Franklin M. Identity-Based encryption from the weil pairing. In: Kilian J, ed. Advances in Cryptology—CRYPTO 2001, the 21st Annual Int'l Cryptology Conf. Berlin: Springer-Verlag, 2001. 213−230.

[8] Chen L, Harrison K, Soldera D, Smart NP. Applications of multiple trust authorities in pairing based cryptosystems. In: Davida GI, ed. Proc. of the Infrastructure Security, Int'l Conf., InfraSec 2002. Berlin: Springer-Verlag, 2002. 260−275.

[9] Smart NP. Access control using pairing based cryptography. In: Joye M, ed. Proc. of the Topics in Cryptology—CT-RSA 2003, the Cryptographers' Track at the RSA Conf. 2003. Berlin: Springer-Verlag, 2003, 111−121.

[10] Mu Y, Susilo W, Lin YX. Identity-Based broadcasting. In: Johansson T, ed. Proc. of the Progress in Cryptology—INDOCRYPT 2003, 4th Int'l Conf. on Cryptology in India. Berlin: Springer-Verlag, 2003. 177−190.

[11] Baek J, Safavi-Naini R, Susilo W. Efficient multi-receiver identity-based encryption and its application to broadcast encryption. In: Vaudenay S, ed. Proc. of the Public Key Cryptography—PKC 2005, the 8th Int'l Workshop on Theory and Practice in Public Key Cryptography. Berlin: Springer-Verlag, 2005. 380−397.

[12] Shamir A. How to share a secret. ACM Communications, 1979,22(11):612−613.

[13] Okamoto T, Pointcheval D. REACT: Rapid enhanced-security asymmetric cryptosystem transform. In: Naccache D, ed. Proc. of the Topics in Cryptology—CT-RSA 2001, the Cryptographer's Track at RSA Conf. 2001. Berlin: Springer-Verlag, 2001. 159−174.

附中文参考文献:

[4] 冯登国.可证明安全性理论与方法研究.软件学报,2005,16(10):1743−1756. http://www.jos.org.cn/1000-9825/16/1743.htm

鲁力(1978－),男,贵州铜仁人,博士,讲师,主要研究领域为密码学,网络安全.

胡磊(1967－),男,博士,教授,博士生导师,主要研究领域为密码学.