ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.20, No.10, October 2009, pp.2907−2914
doi: 10.3724/SP.J.1001.2009.03552
© by *Institute of Software, the Chinese Academy of Sciences*. All rights reserved.
E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

可证明安全的多接收者公钥加密方案设计与分析*

庞辽军[1,2+], 李慧贤[3], 焦李成[2], 王育民[1]

[1](西安电子科技大学 计算机网络与信息安全教育部重点实验室,陕西 西安 710071)

[2](西安电子科技大学 智能信息处理研究所,陕西 西安 710071)

[3](西北工业大学 计算机学院,陕西 西安 710072)

Design and Analysis of a Provable Secure Multi-Recipient Public Key Encryption Scheme

PANG Liao-Jun[1,2+], LI Hui-Xian[3], JIAO Li-Cheng[2], WANG Yu-Min[1]

[1](The Ministry of Education Key Laboratory of Computer Networks and Information Security, Xidian University, Xi'an 710071, China)

[2](Institute of Intelligent Information Processing, Xidian University, Xi'an 710071, China)

[3](Department of Computer Science and Engineering, Northwestern Polytechnical University, Xi'an 710072, China)

+ Corresponding author: E-mail: ljpang@mail.xidian.edu.cn, http://www.xidian.edu.cn

Pang LJ, Li HX, Jiao LC, Wang YM. Design and analysis of a provable secure multi-recipient public key encryption scheme. *Journal of Software*, 2009,20(10):2907−2914. http://www.jos.org.cn/1000-9825/3552.htm

Abstract: To improve the inefficiency of the existing key distribution protocols in the secure broadcasting, an ideal multi-recipient public key encryption scheme to achieve the secret broadcasting is proposed. Based on Shamir's threshold secret sharing scheme, a multi-recipient public key encryption scheme of the IND-CPA security is proposed on bilinear pairing on elliptic curve. And then, extension is made on the proposed scheme to construct a new multi-recipient public key encryption scheme with the IND-CCA2 security. Based on the Bilinear Decisional Diffie-Hellman assumption and the Gap Bilinear Diffie-Hellman assumption, their security claimed above is proved. At the same time, analyses are made on the correctness and performance of the scheme. Analyses show that the proposed scheme is a efficient and secure public-key encryption scheme, in which, a ciphertext encrypted by an encryption key can be decrypted by a number of decryption keys. This makes it play an important role in many applications. Especially in the secure broadcasting, it can be applied to securely broadcast sensitive information in an unsafe and open network situation.

Key words: secure broadcasting; secret sharing; elliptic curve; multi-recipient public key encryption

* Supported by the National Natural Science Foundation of China under Grant No.60803151 (国家自然科学基金); the Key Program of NSFC-Guangdong Union Foundation under Grant No.U0835004 (国家自然科学基金委员会-广东联合基金重点项目); the Shaanxi Provincial Natural Science Foundation of China under Grant No.2007F37 (陕西省自然科学基金); the National Science Foundation for Post-Doctoral Scientists of China under Grant No.20070410376 (中国博士后科学基金); the Open Foundation of the Key Laboratory of Network and Information Security in Xidian University, the Ministry of Education of China under Grant No.2008CNIS-07 (西安电子科技大学教育部计算机网络与信息安全重点实验室开放基金), the NPU "Aoxiang Star" Project of China in 2008 (西北工业大学2008"翱翔之星计划"); the 111 Project of China under Grant No.B08038 (高等学校学科创新引智计划); the NPU Foundation for Undamental Research of China under Grant No.NPU-FFR-JC200819 (西北工业大学基础研究基金)

Received 2008-11-28; Accepted 2008-12-30

© 中国科学院软件研究所 http://www.jos.org.cn

摘 要: 针对现有安全广播协议密钥分发效率较低的问题,提出了一种通过多接收者公钥加密实现安全广播的方法.以 Shamir 的门限秘密共享方案为设计基础,首先提出了一个基于椭圆曲线上双线性变换的具有抗不可区分选择明文攻击(IND-CPA)安全性的多接收者公钥加密方案,然后对所提方案进行安全扩展,在此基础上最终提出了一个具有抗不可区分自适应选择密文攻击(IND-CCA2)安全性的多接收者公钥加密方案.基于双线性判定 Diffie-Hellman 假设和双线性间隙 Diffie-Hellman 假设,对上述所声称的 IND-CPA 安全性和 IND-CCA2 安全性进行了证明.同时,对方案的正确性及性能等进行了分析和证明.分析发现,该方案是一个安全、有效的公钥加密方案.由一个加密密钥所加密的密文可以被多个解密密钥解密而得到其所对应的明文,这使得该方案具有非常重要的应用,尤其是可以用来实现安全广播,以便在不安全的、开放的网络环境中安全地广播敏感信息.

关键词: 安全广播;秘密共享;椭圆曲线;多接收者公钥加密

中图法分类号: TP309 **文献标识码**: A

广播通信具有很多优点:(1) 可以提高通信效率,实现点对多点通信;(2) 相对来说节约能量,适合如无线传感器网络(WSN)等能量敏感的网络;(3) 适合无反向信道的通信系统.因此,广播一直以来受到人们的重视,而如何实现安全广播已成为当前研究热点之一,也是在无线局域网(WLAN)、无线城域网(WMAN)、WSN 等多种形式的无线网络和有线网络中尚未妥善解决的主要问题之一.例如:在 WLAN 的安全解决方案 IEEE 802.11i[1]或国内的 WAPI 协议[2]中,广播/组播密钥都是由接入点(access point,简称 AP)使用其与各移动终端(STAtion,简称 STA)共享的单播会话密钥加密发送的,效率非常低.假设有 n 个 $STA_i(i=1,...,n)$,每个 STA_i 与 AP 都共享一个单播会话加密密钥,记为 $sk_i(i=1,...,n)$.AP 为了分发一个广播/组播密钥 Key,需要使用每一个密钥 sk_i 加密 Key,并将加密后的密文发送给相应的 STA_i.很显然,这种方案的效率和实时性随着 STA 数目的增加而降低,难以满足实际应用需求.

IEEE 802.11i 和 WAPI 的安全广播在性能上存在很大缺陷.如果能有一种加密方案,发送者只加密一次,而每个接收者都可以使用自己独有的解密私钥进行解密,得到同样的明文信息,就能有效地解决上述的安全广播问题.这样的加密方法通常称为具有多个接收者的公钥加密方案,它是由 Baudron 等人[3]和 Bellare 等人[4]提出来的.之后,文献[5]基于随机重用技术将 ElGamal 加密方案推广为具有多接收者的公钥方案.文献[6,7]也分别基于椭圆曲线上的双线性对构造了基于身份的具有多接收者的公钥加密方案.

本文尝试将秘密共享技术[8]的门限共享思想用于公钥加密方案设计之中,设计了一个具有 IND-CPA 安全性的多接收者公钥加密方案,并使用文献[9]中提出的方法对其安全加以扩展,最终实现一个具有 IND-CCA2 安全性的多接收者公钥加密方案.

1 相关技术

定义 1(**间隙双线性 Diffie-Hellman 问题**(**Gap-BDH problem**)[10]). 对于定义 1 给出的双线性变换,给定(P,aP,bP,cP),在双线性判定 Diffie-Hellman 谕示(BDDH(bilinear decision Diffie-Hellman) oracle)的帮助下,求解 $e(P,P)^{abc}$ 即为 Gap-BDH 问题.其中 BDDH 谕示定义为:输入(P,aP,bP,cP,κ),如果$\kappa=e(P,P)^{abc}$,则输出 1;否则输出 0.

定义 2(**求解 Gap-BDH 问题的优势**[11]). 若 A 为敌手,其求解 Gap-BDH 问题的优势定义为

$$Adv_A = Prob[A(P,aP,bP,cP) = e(P,P)^{abc}] \quad (1)$$

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,则称该问题是(t,q_0,ε)困难.

单向性(one-way)安全:不存在多项式时间的敌手能够由密文恢复相应的明文.明文检测攻击(plaintext checking attack,简称 PCA):敌手可获得对明文检测谕示(plaintext checking oracle)的访问权限.当明文检测谕示的输入为明密文对(C,M)时,如果 C 是 M 的密文,则输出 1;否则输出 0.

文献[9]还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(one-way under plaintext checking

© 中国科学院软件研究所 http://www.jos.org.cn

attack,简称 OW-PCA)”这一概念,即在明文检测谕示的帮助下,不存在多项式时间的敌手能够以不可忽略的概率从一个给定的密文中恢复出完整的明文,则称该公钥加密体制满足明文检测攻击下的单向性.

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'.

2 本文提出的多接收方加密方案

2.1 具有IND-CPA安全性的方案

假设系统中有一个消息发送方(即加密者)S 和 n 个消息接收方(即解密者)$R_1,R_2,\ldots,R_n$.

(i) 系统参数:设$(G_1,+)$和$(G_2,\cdot)$为两个阶均为 p 的循环群,其中 p 为素数;令 P 为 G_1 的生成元;$e:G_1\times G_1\to G_2$ 为 G_1 和 G_2 上的双线性变换.

首先,发送者 S 随机选取一个正整数 m(m 为后面所用多项式次数),并在 Z_q^* 中随机选择 $m+n$ 个不同的元素,构成向量 $\vec{S}=\{v_1,\ldots,v_m\}$ 和整数 $v_{m+j}(j=1,2,\ldots,n)$.接着,S 随机选取自己的加密主密钥 $S_S\in Z_q^*$,并计算 $Q_S=S_SP\in G_1$.随后,S 随机选择两个元素 $Q_1,Q_2\in G_1$ 以及一个 m 次多项式 $f(x)\in Z_p[x]$满足 $f(0)=S_S$,并计算如下信息:

$$\overrightarrow{S^*}=f(\vec{S})P=\{f(v_1)P,\ldots,f(v_m)P\}=\{S_1^*,\ldots,S_m^*\} \tag{2}$$

$$V_j=f(v_{m+j})(Q_1+Q_2)(j=1,2,\ldots,n) \tag{3}$$

其中,$(p,G_1,G_2,e,P,Q_S,Q_1,Q_2,\vec{S},v_{m+1},\ldots,v_{m+n},\overrightarrow{S^*})$ 为系统公共参数,S_S 为消息发送者 S 的加密主密钥,V_j 为接收者 R_j 的解密私钥$(j=1,2,\ldots,n)$.

(ii) 加密过程:为了加密 $M\in G_2$,S 随机选择整数 $r\in Z_p^*$,并计算密文如下:

$$C=(P^*,Q_1^*,U,\overrightarrow{S^*})=(rP,rQ_1,e(Q_S,Q_2)^rM,r\overrightarrow{S^*}) \tag{4}$$

(iii) 解密过程:任意接收者 $R_j(j=1,2,\ldots,n)$可以解密 C 以获取信息 m.R_j 首先构造 $\Gamma=\vec{S}\cup\{v_{m+j}\}=\{v_1,\ldots,v_m,v_{m+j}\}$,并对每个 $v_k\in\Gamma$算出$\sigma_{k,\Gamma}(0)$.最后,R_j 计算 M 如下:

$$M=\frac{e(Q_1^*,Q_S)U}{e\left(Q_1+Q_2,\sum_{i=1}^{m}\sigma_{v_i,\Gamma}(0)S_i^{**}\right)e(\sigma_{v_{m+j},\Gamma}(0)V_j,P^*)} \tag{5}$$

在公式(5)中,令$\{S_1^{**},\ldots,S_m^{**}\}=\overrightarrow{S^*}$,以方便清晰描述.

2.2 具有IND-CCA2安全性的方案

为了描述方便,不妨称第 2.1 节和第 2.2 节中的方案分别为方案 2.1 和方案 2.2.与方案 2.1 相似,方案 2.2 也包括系统参数、加密和解密 3 部分,具体描述如下:

(i) 系统参数:增加两个公开的单向 Hash 函数 $h_1:G_2\to\{0,1\}^{l_1}$ 和 $h_2:\{0,1\}^*\to\{0,1\}^{l_2}$.

(ii) 加密过程:为了加密 $M\in G_2$,S 随机选取 $W\in G_2$ 和 $r\in Z_p^*$,并计算密文 C 如下:

$$C=(P^*,Q_1^*,U,c,I,\overrightarrow{S^*})=(rP,rQ_1,e(Q_S,Q_2)^rW,M\oplus h_1(W),h_2(W,M,P^*,Q_1^*,U,c),r\overrightarrow{S^*}) \tag{6}$$

(iii) 解密过程:任意接收者 $R_j(j=1,2,\ldots,n)$可以解密 C 以获取信息 m.首先,构造 $\Gamma=\vec{S}\cup\{v_{m+j}\}=\{v_1,\ldots,v_m,v_{m+j}\}$,并对每个 $v_k\in\Gamma$计算$\sigma_{k,\Gamma}(0)$.然后计算:

$$W'=\frac{e(Q_1^*,Q_S)U}{e\left(Q_1+Q_2,\sum_{i=1}^{m}\sigma_{v_i,\Gamma}(0)S_i^{**}\right)e(\sigma_{v_{m+j},\Gamma}(0)V_j,P^*)} \tag{7}$$

$$M'=c\oplus h_1(W') \tag{8}$$

同样,在公式(7)中,令$\{S_1^{**},\ldots,S_m^{**}\}=\overrightarrow{S^*}$,以方便清晰描述.

© 中国科学院软件研究所 http://www.jos.org.cn

最后,判断 $h_2(W',M',P^*,Q_1^*,U,c)\overset{?}{=}I$ 是否成立.如果成立,接受 M'为合法明文,否则拒绝 M'.

3 分析和讨论

3.1 正确性分析

方案 2.2 是基于方案 2.1 构造的,我们仅需讨论方案 2.1 的正确性,其正确性可以通过下面的定理来说明.

定理 1. 接收者解密得到的消息 M 与发送者所加密的消息 M 是相等的.

证明:

$$\frac{e(Q_1^*,Q_S)U}{e\left(Q_1+Q_2,\sum_{i=1}^{m}\sigma_{v_i,\Gamma}(0)S_i^{**}\right)e(\sigma_{v_{m+j},\Gamma}(0)V_j,P^*)}=\frac{e(Q_1^*,Q_S)U}{e\left(Q_1+Q_2,\sum_{i=1}^{m}\sigma_{v_i,\Gamma}(0)rf(v_i)P\right)e(\sigma_{v_{m+j},\Gamma}(0)f(v_{m+j})(Q_1+Q_2),P^*)}$$

$$\overset{(*)}{=}\frac{e(rQ_1,Q_S)e(Q_S,Q_2)^rM}{e\left(Q_1+Q_2,\sum_{i=1}^{m}rf(v_i)\sigma_{v_i,\Gamma}(0)P\right)e(f(v_{m+j})\sigma_{v_{m+j},\Gamma}(0)(Q_1+Q_2),rP))}$$

$$\overset{(*)}{=}\frac{e(Q_1,Q_S)^re(Q_2,Q_S)^rM}{e\left(Q_1+Q_2,P\left(\sum_{i=1}^{m}(f(v_i)\sigma_{v_i,\Gamma}(0))+f(v_{m+j})\sigma_{v_{m+j},\Gamma}(0)\right)\right)^r}$$

$$\overset{(+)}{=}\frac{e(Q_1,Q_S)^re(Q_2,Q_S)^rM}{e(Q_1+Q_2,PS_S)^r}\overset{(*)}{=}\frac{e(Q_1,Q_S)^re(Q_2,Q_S)^rM}{e(Q_1+Q_2,Q_S)^r}$$

$$\overset{(*)}{=}\frac{e(Q_1,Q_S)^re(Q_S,Q_2)^rM}{e(Q_1,Q_S)^re(Q_2,Q_S)^r}\equiv M.$$

其中,(*)标识椭圆曲线双向性变换;(+)标识 Lagrange 插值变换. □

3.2 安全性分析

定理 2. 如果存在攻击方案 2.1 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 $\varepsilon'=\frac{1}{2}\varepsilon$,运行时间为 $t'=O(t)$.

证明:首先,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,$Z_0=e(P,P)^{abc}$,$Z_1=e(P,P)^z$,$z$ 为从 Z_p^* 中随机选择的整数.设 B 区分(P,aP,bP,cP,Z_0)和(P,aP,bP,cP,Z_1)的优势为ε',其运行时间为 t'.算法 B 按如下方法生成方案 2.1 的一个实例.

Phase 1:B 令 $Q_S=aP$ 和 $Q_2=bP$,并分别随机选择 $r\in Z_p^*$ 和 m 次多项式 $f(x)\in Z_p[x]$.另外,B 随机选择 Z_p^* 的一个子集,记为 $\vec{S}=\{v_1,...,v_m\}$,然后计算 $Q_1=rP$ 并输出系统公共参数 $(p,Q_1,Q_2,P,Q_S,e,G_1,G_2,\vec{S})$ 给 A.

Challenge Phase:A 选择两个等长明文 M_0 和 M_1 并发送给 B.B 收到后生成目标密文 C^+如下:

- 随机选择 $u,v\in\{0,1\}$;
- 返回 $C^+=(cP,bcP,Z_vM_u,\{f(v_i)cP\mid v_i\in\{v_1,...,v_m\}\})$.

对于 Z_v,如果 v=0,因为 $Z_vM_u=e(P,P)^{abc}M_u=e(aP,bP)^cM_u$,由加密过程可知,$C^+$是 M_u 的合法密文.如果 v=1,则 $Z_vM_u=e(P,P)^zM_u$.由 z 的随机性可知,A 不能得到关于 u 的任何信息.

Guess:收到 A 的猜测 u'后,如果 $u'=u$,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}).

下面,我们来分析 B 的优势.

如果 v=1,A 不能得到关于 u 的任何信息.因此有 $Prob[u'=u\mid v=1]=Prob[u'\neq u\mid v=1]=\frac{1}{2}$,并且 B 猜测正确

© 中国科学院软件研究所 http://www.jos.org.cn

的 BDDH 组的成功概率是 $Prob[B\ success \mid v=1]=\frac{1}{2}$.

如果 v=0,B 返回 M_u 的合法密文.由定理中所述的条件,A 攻击方案 2.1 的优势为ε.因此 $Prob[u'=u \mid v=0]=\frac{1}{2}+\varepsilon$,$B$ 猜测正确的 BDDH 组的成功概率为 $Prob[B\ success \mid v=0]=\frac{1}{2}+\varepsilon$.

因此,B 区分 BDDH 组的优势为

$$\begin{aligned}Prob[B\ success]-\frac{1}{2}&=Prob[v=0 \text{ and } B\ success]+Prob[v=1 \text{ and } B\ success]-\frac{1}{2}\\&=\frac{1}{2}Prob[B\ success \mid v=0]+\frac{1}{2}Prob[B\ success \mid v=1]-\frac{1}{2}\\&=\frac{1}{2}(\frac{1}{2}+\varepsilon)+\frac{1}{2}\times\frac{1}{2}-\frac{1}{2}=\frac{1}{2}\varepsilon.\end{aligned}$$ □

定理 3. 假设存在多项式时间 t 内攻击方案 2.2 的 IND-CCA2 敌手 A,其优势为ε.设 A 对随机谕示 h_1 和 h_2 最多分别实施 q_{h_1} 和 q_{h_2} 次查询,对解密谕示最多实施 q_d 次查询,那么,以 A 为子程序可以构造算法 B 求解 Gap-BDH 问题,其优势为 $\varepsilon' \geq \frac{1}{q_{h_2}}\left(\varepsilon-\frac{q_d}{2^{l^1}}\right)\left(1-\frac{q_{h_1}}{2^{l_1}}-\frac{q_{h_2}}{2^{l_2}}\right)$,运行时间为 $t'=O(t)$.其中,l_1 和 l_2 分别代表单向 Hash 函数 h_1 和 h_2 的输出长度.

证明:首先,我们证明方案 2.1 在 Gap-BDH 假设下是 OW-PCA 单向安全的.这里用反证法进行证明.假设敌手可以攻破方案 2.1 的 OW-PCA 单向安全性,这时,该敌手就可以根据所得到的系统公共参数 $(p,G_1,G_2,e,P,Q_S,Q_1,Q_2,\bar{S},v_{m+1},...,v_{m+n},\overline{S^*})$ 以及给定密文 $(P^*,Q_1^*,U,\overline{S^*})$ 和为该密文找到的某个明文 M',通过明文检测谕示检测分析 $(P,P^*,Q_S,Q_2,U/M')$ 是否为 BDDH 组.如果以该敌手为子程序,就可以构造算法来求解 Gap-BDH 问题.因此,我们可以得到这样的结论:如果假设 Gap-BDH 问题是困难问题,那么,方案 2.1 在 Gap-BDH 假设下是 OW-PCA 单向安全的.

下面我们证明方案 2.2 是 IND-CCA2 安全的.我们以上述定理 2 中所给出的敌手 A 为子程序构造方案 2.1 的 OW-PCA 敌手 B.

假设敌手 B 得到方案 2.1 的系统公共参数 $(p,G_1,G_2,e,P,Q_S,Q_1,Q_2,\bar{S},v_{m+1},...,v_{m+n},\overline{S^*})$ 和目标密文 $C^+=(P^{*+},Q_1^{*+},U^+,\overline{S^{*+}})=(r^+P,r^+Q_1,e(Q_S,Q_2)^{r^+}M^+,r^+\overline{S^*})$.记敌手 B 攻击方案 2.1 的成功概率为ε'(即找到 C 所对应明文的概率).B 模拟 A 的目标系统,并与 A 一起进行如下的 IND-CCA2 攻击过程.

Phase 1:B 给 A 公共参数 $(p,G_1,G_2,e,P,Q_S,Q_1,Q_2,\bar{S},v_{m+1},...,v_{m+n},\overline{S^*},h_1,h_2)$.这里,$h_1$ 和 h_2 是由 B 控制的随机谕示,其控制方法如下:

对于 h_1:B 初始时为其构造一个数据项格式,如$(W,h_1(W))$的空表格.为了方便起见,记 $H_1=h_1(W)$.当 B 收到 A 的查询 $W_j(1\leq j\leq q_{h_1})$ 后,判断 h_1 的表项中是否已存在数据项(W_j,H_1).如果是,返回 H_1;否则,用明文检测谕示检测目标密文 C^+是否是 W_j 的密文.如果是,则返回 W_j 并终止 A 的攻击过程(这时,B 已经找到目标密文 C^+所对应的明文,即 B 攻击成功);否则,随机选取一个 $H_{1,j}\in\{0,1\}^{l_1}$,将$(W_j,H_{1,j})$加入 h_1 的表项中,同时返回 $H_{1,j}$.

对于 h_2,其处理与上述过程类似:B 初始时为其构造一个数据项格式,如 $((W,M,P^*,Q_1^*,U,c),H_2)$ 的空表格,其中,$H_2=h_2(W,M,P^*,Q_1^*,U,c)$.当 B 收到 A 的查询 $(W_j,M_j,P_j^*,Q_{1,j}^*,U_j,c_j)(1\leq j\leq q_{h_2})$ 后,如果 $((W_j,M_j,P_j^*,Q_{1,j}^*,U_j,c_j),H_{2,j})$ 已经存在于 h_2 的表项中,返回 $H_{2,j}$;否则,用明文检测谕示检测目标密文 C^+是否是 W_j 的密文.如果是,返回 W_j,并终止 A 的攻击过程(这时,B 已经找到目标密文所对应的明文,即 B 攻击成功);否则,随机选择一个 $H_{2,j}\in\{0,1\}^{l_2}$,然后将 $((W_j,M_j,P_j^*,Q_{1,j}^*,U_j,c_j),H_{2,j})$ 加入 h_2 的表项中,同时返回 $H_{2,j}$.

Phase 2:B 回答 A 的解密查询.当收到一个解密查询 $C_j=(P_j^*,Q_{1,j}^*,U_j,c_j,I_j,\overline{S_j^*})$ $(1\leq j\leq q_d)$时,判断 $((W_j,M_j,P_j^*,Q_{1,j}^*,U_j,c_j),I_j)$ 是否在 h_2 的表项中.如果不在,则拒绝该密文 C_j;否则,使用 h_1 谕示计算 $h_1(W_j)$并验证 $h_1(W_j)\oplus M_j=c_j$

© 中国科学院软件研究所 http://www.jos.org.cn

是否成立.如果不成立,则拒绝该密文 C_j;否则,使用明文检测谕示验证 $(P_j^*,Q_{1,j}^*,U_j,\overrightarrow{S_j^*})$ 是否为 W_j 所对应的密文.如果是,则返回 M_j;否则,拒绝该密文 C_j.

Phase 3:*B* 用方案 2.2 的目标密文 C^+构造方案 2.2 的合法密文 C^{++}.当 *B* 收到 *A* 发送的两个等长明文(M_0,M_1)后,随机选择一个 $b\in\{0,1\}$,一个 $H_1^+\in\{0,1\}^{l_1}$ 并置 $H_1^+=h_1(W^+)$,一个 $H_2^+\in\{0,1\}^{l_2}$ 并置 $H_2^+=h_2(S^*,M_b,P^{*+},Q_1^{*+},U^+,c^*)$.最后,令 $C^{++}=(P^{*+},Q_1^{*+},U^+,H_1^+\oplus M_b,I^+,\overrightarrow{S^*}^+)$.

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

Phase 5:当 *B* 收到 *A* 对 *b* 的猜测值 *b*′后,判断 *b*′=*b* 是否成立.如果成立,在 h_2 的表项中均匀地随机选择一个 *W* 并输出;否则,终止而不输出任何信息.

需要说明的是,在上面的攻击过程中,对解密谕示的模拟与真实环境下是近似相同的,但有一种情况除外.即如果敌手 *A* 不需要查询 h_2 就能正确猜测 h_2 输出,那么尽管 *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.这种情况发生的概率为 $\frac{1}{2^{l_2}}$.这里,不妨假设用事件 E_0 来表示在整个攻击过程中 *A* 不查询 h_2 而正确猜测其输出的事件.由于 *A* 最多实施 q_d 次解密询问,所以有 $Prob[E_0]\le\frac{q_d}{2^{l_2}}$.

下面分析在与 *A* 进行上述攻击过程之后,*B* 在什么情况下可以给出目标密文 C^*的正确解密.分如下 3 种情况:

(1) 当 *A* 以 W_j 在 h_1 表项中查询 $h_1(W_j)$时,*B* 发现 C^+是 W_j 对应的密文,其发生的概率为 $\frac{q_{h_1}}{2^{l_1}}$.该事件可以简单记为 E_1;

(2) 当 *A* 以 $(W_j,M_j,P_j^*,Q_{1,j}^*,U_j,c_j)$ 在 h_2 表项中查询 $h_2(W_j,M_j,P_j^*,Q_{1,j}^*,U_j,c_j)$ 时,*B* 发现 C^+是 W_j 对应的密文,这种情况发生的概率为 $\frac{q_{h_2}}{2^{l_2}}$.该事件可以简单记为 E_2;

(3) 当 *A* 的攻击过程结束时,如果 *A* 攻击成功,则 *B* 在 h_2 表项中均匀地随机选择一个 W_j 作为目标密文 C^+的明文(注意,这时事件 E_0 没有发生).该事件可以简单记为 E_3.

这时,我们有

$$\begin{aligned}\varepsilon' &= Prob[B\ Success]\\ &= Prob[E_1]Prob[B\ Success\,|\,E_1]+Prob[E_2]Prob[B\ Success\,|\,E_2]+Prob[E_3]Prob[B\ Success\,|\,E_3]\\ &\ge (1-Prob[E_1]-Prob[E_2])Prob[B\ Success\,|\,E_3]\\ &\ge \frac{1}{q_{h_2}}\left(1-\frac{q_{h_1}}{2^{l_1}}-\frac{q_{h_2}}{2^{l_2}}\right)\left(Prob[b'=b\,|\,\neg E_0]-\frac{1}{2}\right)\\ &\ge \frac{1}{q_{h_2}}\left(\varepsilon-\frac{q_d}{2^{l_2}}\right)\left(1-\frac{q_{h_1}}{2^{l_1}}-\frac{q_{h_2}}{2^{l_2}}\right).\end{aligned}$$

□

3.3 抗联合攻击

本文方案能够防止接收者联合破译发送者私钥 S_S 的攻击.在方案 2.1 中,通过 *m* 次多项式在 *m*+*n* 个份额中隐藏(或共享)了发送者的私钥,其中,*m* 个份额是公开参数,另外 *n* 个为各接收者的私钥.由 Shamir 门限秘密共享的性质可知[12],任取 *m*+1 个份额可以恢复 S_S,但少于 *m*+1 个就得不到关于 S_S 的任何信息.然而,公开参数和各接收者私钥中包含的关于多项式 $f(x)$的函数值都是非直接结果,也都是使用等式(2)和等式(3)的计算结果.要根据这些结果求取真正的函数值将面临 G_1 上椭圆曲线离散对数的困难性.因此,看似接收者或若干接收者联合可以占有多达 *m*+1 个子信息,但由于它们不是真正的函数值,因此无法重构多项式 $f(x)$,故接收者或他们之间联合起来试图获取发送者的主密钥 S_S 都是计算上不可行的.

© 中国科学院软件研究所 http://www.jos.org.cn

3.4 性能分析

在方案 2.1 中加密一个明文 m,需要 1 次双线性变换计算、m+2 次椭圆曲线点群 G_1 上的倍点运算和 1 次乘法群 G_2 上的指数运算;在解密时只需要 3 次双线性变换运算、n+1 次点乘运算和 3 次 G_2 中的运算(两次乘法和一次除法)即可.另外,在系统参数建立阶段,m 可以为任意正整数.特别地,如果令 m=1,系统的性能会得到很大提高,因为所涉及的 Lagrange 多项式仅为 1 次,解密时,$\sigma_{k,I}(0)$计算仅为 2 次.但是这会导致子秘密之间存在一些线性的性质,一般应该避免这种情况的发生.由上述安全性分析可知,m 的值不会对安全造成影响.如果选取较大,会降低通信和计算效率;同样,为了提高方案的性能,可以适当选取较小的整数.

从上面的分析可以看出,方案 2.1 中比较复杂的运算主要是倍点和双线性运算.由于本文采用了椭圆曲线上双线性对,能够使得安全方案以较短的密钥和较小的计算实现同等的安全强度,因此,方案 2.1 在计算上还是非常有效的.而方案 2.2 比起方案 2.1 仅多了 4 次 Hash 运算和 2 次异或运算,其计算复杂度相比较是可以忽略的.因此,方案 2.2 也是非常有效的.

3.5 与现有方案对比

多接收者公钥加密的概念最初是由 Baudron 等人[3]和 Bellare 等人[4]提出来的,他们的方法都是基于将在单接收者情况下公钥加密体制(即通常意义上的公钥加密体制)的安全性推广到多接收者情况.这种方法的主要缺点是加密效率不高,而且对传输带宽要求较高,不适宜实际应用.因此,他们的方法没有得到应用和推广.之后,文献[5]基于随机重用技术将 ElGamal 加密方案推广为具有多接收者的公钥方案.这种方法很大程度上改进了前面方案中效率不高和带宽要求较高的缺点,但其效率相对于应用需求来说还是较低的.为了提高计算性能,文献[6]基于椭圆曲线上的双线性对提出了构造基于身份的具有多接收者的公钥加密方案的思想,但他们所提出的安全性受到质疑[7],无法证明和确保其安全性.当然,除此之外还存在一些其他的多接收者公钥加密方案,这些方案无外乎基于上述几个典型方案的思想或者在它们的基础上演变而来.就目前研究现状来说,效率和带宽已成为衡量一个多接收者公钥加密方案好坏的主要指标之一,会影响方案的应用和推广.本文提出的方案在效率上比现有方案有了很大提高,通过第 3.4 节的分析可知,本文方案所采用的 Lagrange 插值多项式的阶数是可以任意选取的,而不会影响系统安全性.为了提高性能,可以选取较低阶的多项式,甚至在一些等级较低的应用中,可以选取阶数为 1,极大地提高了计算性能.对于通信带宽,由于系统参数初始化过程可以离线(off-line)方式操作,而在加密过程和解密过程中,用户之间均无须交互信息,因而不再对通信带宽有所要求.通过这些分析可见,本文方案在计算性能和通信带宽方面都有了很大的改善.

4 结 论

以门限秘密共享方案为工具,我们提出了一个基于椭圆曲线上双线性变换的多接收者公钥加密方案,并证明其具有 IND-CPA 安全性.同时,对该方案进行安全扩展,给出一个具有 IND-CCA2 安全性的多接收者公钥加密方案.本文的方案具有非常重要的应用前景,可用于无线局域网、无线城域网、无线传感器网络等多种形式的无线网络和有线网络,以实现安全广播.

References:

[1] IEEE Standard. P802.11i Draft Supplement to Standard for Telecommunications and Information Exchange Between Systems—LAN/MAN Specific Requirements—Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Specification for Enhanced Security. Piscataway: IEEE Press, 2002.

[2] Chinese Standard. GB15629.11-2003/XG1-2006 of Telecommunications and Information Exchange Between Systems—LAN/MAN Specific Requirements—Part 11: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Specification for Enhanced Security. Beijing: Chinese Standard Press, 2006 (in Chinese).

© 中国科学院软件研究所 http://www.jos.org.cn

[3] Baudron O, Pointcheval D, Stern J. Extended notions of security for multicast public key cryptosystems. In: Widmayer P, Francisco T, *et al*., eds. Proc. of the Automata, Languages and Programming, the 29th Int'l Colloquium (ICALP 2000). LNCS 1853, Heidelberg: Springer-Verlag, 2000. 499−511.

[4] Bellare M, Boldyreva A, Micali S. Public-Key encryption in a multi-user setting: Security proofs and improvements. In: Naor M, ed. Proc. of the Advances in Cryptology (Eurocrypt 2000). LNCS 1807, Heidelberg: Springer-Verlag, 2000. 259−274.

[5] Kurosawa K. Multi-Recipient public-key encryption with shortened ciphertext. In: Naccache D, Paillier P, eds. Proc. of the 5th Int'l Workshop on Practice and Theory in Public Key Cryptography (PKC 2002). LNCS 2274, Heidelberg: Springer-Verlag, 2002. 48−63.

[6] Mu Y, Susilo W, Lin Y. Identity-Based broadcasting. In: Johansson T, Maitra S, eds. Proc. of the 4th Int'l Conf. on Cryptology in India (INDOCRYPT 2003). LNCS 2904, Heidelberg: Springer-Verlag, 2003. 177−190.

[7] 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 8th Int'l Workshop on Practice and Theory in Public Key Cryptography (PKC 2005). LNCS 3386, Heidelberg: Springer-Verlag, 2005. 380−397.

[8] Pang LJ, Liu Y, Wang YM. An efficient (*t*,*n*) threshold multi-secret sharing scheme. Acta Electronica Sinica, 2006,34(4):587−589 (in Chinese with English abstract).

[9] Okamoto T, Pointcheval D. REACT: Rapid enhanced-security asymmetric cryptosystem transform. In: Naccache D, ed. Proc. of the Cryptographer's Track at RSA Conference (CT-RSA 2001). LNCS 2020, Heidelberg: Springer-Verlag, 2001. 159−174.

[10] Okamoto T, Pointcheval D. The gap-problems: A new class of problems for the security of cryptographic schemes. In: Kim KJ, ed. Proc. of the 4th Int'l Workshop on Practice and Theory in Public Key Cryptography (PKC 2001). LNCS 1992, Heidelberg: Springer-Verlag, 2001. 104−118.

[11] Boneh D, Franklin M. Identity-Based encryption from the Weil pairing. In: Kilian J, ed. Proc. of the Advances in Cryptology (CRYPTO 2001). LNCS 2139, Heidelberg: Springer-Verlag, 2001. 213−229.

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

附中文参考文献:

[2] 中国标准 GB15629.11-2003/XG1-2006《信息技术 系统间远程通信和信息交换 局域网和城域网特定要求 第 11 部分:无线局域网媒体访问控制和物理层规范 第 1 号修改单》.北京:中国标准出版社,2006.

[8] 庞辽军,柳毅,王育民.一个高效的(*t*,*n*)门限多重秘密共享体制.电子学报,2006,34(4):587−589.

庞辽军(1978－),男,陕西渭南人,博士,副教授,CCF 会员,主要研究领域为密码学,安全协议设计与分析.

焦李成(1959－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为神经网络,机器学习,自然计算,图像感知和认知.

李慧贤(1977－),女,博士,副教授,主要研究领域为网络与信息安全.

王育民(1936－),男,教授,博士生导师,主要研究领域为信息论,密码,编码.

© 中国科学院软件研究所 http://www.jos.org.cn