可公开验证的 ElGamal/RSA 加密

伍前红　　王继林　　袁素春　　王育民
(西安电子科技大学 ISN 国家重点实验室 119 信箱　西安　710071)

摘　要：可公开验证加密允许任何实体验证加密的消息和先前承诺的秘密一样，但不会泄漏明文的任何信息。这在公平交换、防欺骗的秘密分享和安全多方计算中有重要应用。该文分别给出可公开验证的 ElGamal 加密和 RSA 加密方案。其中前者是 Stalder 方案的改进，改进后的方案是语义安全的而 Stalder 方案达不到语义安全性。同时将该方案推广到了多个接受者的情形，最后给出了高效的可公开验证 RSA 加密方案。

关键词：可公开验证加密 ，零知识证明, bit 承诺, RSA 体制, ElGamal 体制
中图分类号：TN918　　**文献标识码**：A　　**文章编号**：1009-5896(2005)04-0608-04

Publicly Verifiable Encryption for ElGamal/RSA Encryption

Wu Qian-hong　　Wang Ji-lin　　Yuan Su-chun　　Wang Yu-min
(*State Key Lab. of Integrated Service Networks, Xidian Univ., Xi'an* 710071, *China*)

Abstract　A publicly verifiable encryption scheme allows any entity to verify that a cipher-text hides the same message as committed before without revealing it. It is important to construct fair exchange scheme, publicly verifiable secret sharing and cheater-resistant secure multi-party computation. In this paper, publicly verifiable encryption schemes are presented for ElGamal/RSA cryptosystem. The ElGamal case is an improved version of Stadler publicly verifiable encryption scheme. The improved scheme is semantic secure while Stadler scheme is not. Also, the scheme is extended to the context of multi-recipient ElGamal encryption and an efficient publicly verifiable RSA scheme is proposed.

Key words　Publicly verifiable encryption (PVE), Zero-knowledge Proof of Knowledge (ZPK), Bits commitment, RSA cryptosystem, ElGamal cryptosystem

1　引言

可公开验证加密（PVE）的概念最先在设计可公开验证秘密分享协议中引入[1]，文献[2]给出了更一般的形式分别用于签名分享，可验证加密还可以用于可撤销匿名的电子支付[3,4]和秘密数据托管[5,6]等。可公开验证加密是一个三方协议，其中证明者 P 是普通公钥体制下的消息发送者，普通公钥体制下的消息接受者 B 可以提取秘密消息，验证者 V 可以是任何实体，能够验证 P 发送给 B 的秘密消息是否与先前承诺的消息具有关系 R，但 V 并不能提取秘密消息。三方的公共输入是一个公开的加密算法 E，对秘密消息 x 的一个公开承诺和一个关系 R。V 根据 $(x, m)\in R$ 是否成立来决定是否接受 P 的证明。协议需要保证 V 接受一个不合法的加密的概率是可忽略的，而且，除了密文隐藏的消息是有效的以外，V 不能获得进一步的任何信息。

本文分别给出可公开验证的 ElGamal 加密和 RSA 加密方案。其中前者是 Stalder 方案的改进：本文的方案是语义安全的而 Stalder 方案[1]达不到语义安全性。同时我们还给出了效率比可以从文献[2]导出的方案更高的可公开验证 RSA 加密方案。

2　安全定义与组成模块

2.1　可公开验证加密的安全性

首先给出可公开验证加密的安全模型与定义。

定义1 (安全的可公开验证加密)　设R是一个二分关系且$L_R=\{x|\exists w: x,w\in R\}$。对关系$R$的一个可公开验证加密方案是一个三方协议 ($P$; V; Recipient)。记$V_p(E, x, l)$表示V与P对输入(E, x, l)交互后的输出，其中l是一个安全参数。一个可公开验证加密是安全的如果满足下列条件：

完备性　如果P和V是诚实的，那么对于任意$(E;D)\in G(1^l)$和任意$x\in L_R$，$V_P(E, x, l)=\perp$的概率是可忽略的，其中1^l是输入的1元编码，$G(1^l)$ 表示一个关于安全参 数 l的 概率多项式

2003-12-25 收到，2004-06-15 改回
973 国家重大项目 (G1999035804)和国家自然科学基金 (60073052)资助课题

时间算法，⊥表示协议异常中止。

有效性　对所有多项式时间P'，所有多项式时间算法 Recover$(\cdot)$，所有的正多项式$p(\cdot)$，所有充分大的l，以及所有的$(E;D)\in G(1^l)$，有

$$\Pr[(x,\text{Recover}(D,\alpha)\notin R\text{且}\alpha\neq\perp\text{且}\alpha=V_{P'}(E,x,l))]<1/p(l)$$

零知识性　对任意V'，存在一个多项式时间模拟器$S_{V'}$以黑盒子的方式访问V'满足对任意的区分器$A(\cdot)$，所有的$p(\cdot)$，所有$x\in L_R$，和所有充分大的l，有

$$\Pr[A(E,x,\alpha_i)=I\ \text{且}\ (E,D)=G(1^l)\ \text{且}\ \alpha_0=S_{V'}(E,x,l)$$
$$\text{且}\alpha_1=V_P'(E,x,l)\ \text{且}\ i\in\{0,1\}]<1/2+1/p(l)$$

完备性保证诚实的证明者和验证者成功执行协议的概率为1；有效性保证如果$x\notin L_R$，证明者伪造证据被验证者接受的概率是可以忽略的；最后，零知识性保证验证者除了$x\in L_R$这一事实外不能获得更多的信息。PVE和ZPK的区别在于前者中某个接受者可以提取秘密消息，而零知识证明中没有谁能够提取类似的秘密。显然，只有在关系R具有单向性时PVE才有意义。如前面所述，证明密文中的秘密是否等于先前承诺的消息在应用中特别重要，本文要讨论的也是这种情形。

2.2　陷门承诺

设G是一个高阶循环群，$\langle g\rangle\subseteq\langle h\rangle\subseteq G$，其中$g$和$h$生成$G$的高阶子群，使得在$\langle g\rangle$和$\langle h\rangle$中计算离散对数是不可行的，特别有$\log_g h$未知。Alice拥有秘密$x$，可以向Bob如下承诺。Alice 随机选取整数$r$，向Bob发送$C=\text{commit}(x,r)=g^x h^r$作为对$x$的承诺。Alice不可能找到$x_1\neq x_2$满足$\text{commit}(x_1,r_1)=\text{commit}(x_2,r_2)$，除非知道$\log_g h$（计算绑定性）。即使他具有无限的计算能力，Bob 也不可能从C提取任何信息(无条件隐藏性)。这是一个陷门承诺，也就是说，如果Alice知道了陷门$\log_g h$则可以任意欺骗Bob，详细请参阅文献[7]。

2.3　ZPK$\{x|y_1=g_1^x\wedge y_2=g_2^x\}$

设 ZPK$\{x_1,\cdots,x_t|R(x_1,\cdots,x_t)\}$表示ZPK证明者知道$(x_1,\cdots,x_t)$使得$R(x_1,\cdots,x_t)$为真。$H$: $\{0,1\}^*\to\{0,1\}^*$是一个可公开获取的密码学杂凑函数。

设$\langle g_1\rangle,\langle g_2\rangle$为在其中计算离散对数是困难的循环群，下面的协议[8]允许Alice向Bob证明她知道x满足$y_1=g_1^x$和$y_2=g_2^x$，其中y_1，y_2是公开的。Alice随机选取整数w，计算$W_1=g_1^{w_1}$，$W_2=g_1^{w_2}$，$c=H(W_1\|W_2)$，$D=w-cx$。Alice向Bob发送证据(c,D)。Bob验证$c=H(g_1^D y_1^c\|g_2^D y_2^c)$。记上述协议为 ZPK$\{x|y_1=g_1^x\wedge y_2=g_2^x\}$。

2.4　ZPK$\{x,r_1,r_2|y_1=g_1^x h_1^{r_1}\wedge y_2=g_2^x h_2^{r_2}\}$

设$\langle g_1\rangle\subseteq\langle h_1\rangle$ 和$\langle g_2\rangle\subseteq\langle h_2\rangle$在其中计算离散对数是困难的循环群，　Alice 不知道$\log_{g_i} h_i$ $(i=1,2)$。下面的协议[2]允许 Alice 向 Bob 证明她知道x,r_1,r_2满足$y_1=g_1^x h_1^{r_1}$和$y_2=g_2^x h_2^{r_2}$，其中 y_1，y_2 是公开的。Alice 随机选取整数 w,w_1,w_2，计算 $W_1=g_1^w h_1^{w_1}$，　$W_2=g_2^w h_2^{w_2}$，　$c=H(W_1\|W_2)$，　$D=w-cx$，　$D_1=w_1-cr_1$，　$D_2=w_2-cr_2$。Alice 向 Bob 发送证据(c,D,D_1,D_2)。Bob 验证 $c=H(g_1^D h_1^{D_1} y_1^c\|g_2^D h_2^{D_2} y_2^c)$。记上述协议为 ZPK$\{x,r_1,r_2|y_1=g_1^x h_1^{r_1}\wedge y_2=g_2^x h_2^{r_2}\}$。这是一个完全 ZPK，即使攻击者拥有无限的计算能力也不能提取 x 的任何信息。

3　可公开验证 ElGamal 加密

设p,q 是大素数，满足$q|p-1$，在Z_p^*计算离散对数是困难的。h 生成Z_q^*的一个阶为q的循环子群。设$G=\langle g\rangle=\langle f\rangle$ 是阶为 p的循环群。记 $x=y \bmod z$为 $x\equiv_z y$ 。

3.1　单个接受者的 ElGamal PVE

首先考虑只有一个接受者Bob时的ElGamal加密，证明密文隐藏的秘密消息与先前的承诺是一致的。接受者选取随机密钥$z\in Z_q$，公开其公钥$y\equiv_p h^z$。要用公钥y加密消息$m\in Z_p^*$，发送者Alice随机选取 $\alpha\in_R Z_q$ 并计算$A\equiv_p h^\alpha$，$B\equiv_p m^{-1}y^\alpha$，只有接受者可以从密文(A,B)中计算$m\equiv_p A^Z/B$。

假设Alice不知道$\log_g f$，下面的协议可以使验证者确信 (A,B) 中加密的消息m与承诺在$M=g^m f^r$ 中的消息m是相同的。

(1)　(承诺) Alice公开$M=g^m f^r$作为对秘密消息m的承诺。

(2)　(零知识证明) 对$i=0,\cdots,l-1$，其中l 是一个安全参数，Alice随机选取$w_i\in_R Z_q$，$\theta_i\in_R Z_p$，计算 $t_i\equiv_p h^{w_i}$，$s_i=g^{y^{w_i}} f^{\theta_i}$。Alice 计算 $c=H(M\|A\|B\|t_0\|s_0\|\cdots\|t_{l-1}\|s_{l-1}) \bmod 2^l$，$u_i\equiv_q w_i-c_i\alpha$，$\delta_i\equiv_p\theta_i-c_i B y^{u_i} r$，其中$c_i$ 是c的第$i$bit。Alice公开$(A,B,c,u_0,\delta_0,\cdots,u_{l-1},\delta_{l-1},)$。

(3)　(验证)验证者接受该加密，如果

$$c=_{2^l}H(M\|A\|B\|h^{u_0}A^{c_0}\bmod p\|(g^{1-c_0}M^{c_0 B})^{y^{u_0}} f^{\delta_0}\|\cdots$$
$$\|h^{u_{l-1}}A^{c_{l-1}}\bmod p\|(g^{1-c_{l-1}}M^{c_{l-1}B})^{y^{u_{l-1}}} f^{\delta_{l-1}})$$

否则，验证者拒绝接受该加密。

3.2　分析单个接受者的 EleGamal PVE

下面根据2.1节的安全定义1分析上述协议。

定理1　上述PVE 协议是完备的。

证明　只需证明诚实的证明者和验证者总是能够成功地执行协议。注意到下述事实，对任意 $\alpha\in Z_q$，如果$(A,B)=(h^\alpha,m^{-1}y^\alpha)\bmod p$ 那么$M^B=g^{y^\alpha} f^{rB}$。因此只需证明$t_i\equiv_p h^{u_i}A^{c_i}$ 和 $s_i=(g^{1-c_i}M^{c_i B})^{y^{r_i}} f^{\delta_i}$ 成立。

(1)　$h^{u_i}A^{c_i}\equiv_p h^{u_i}(h^\alpha)^{c_i}\equiv_p h^{u_i+c_i\alpha}\equiv_p h^{w_i}\equiv_p t_i$

(2) $$(g^{1-c_i}M^{c_iB})^{y^{u_i}}f^{\delta_i}=(g^{1-c_i}(g^mf^r)^{c_iB})^{y^{u_i}}f^{\delta_i}$$

$$=g^{[(1-c_i)+c_imB]y^{u_i}}f^{c_iBy^{u_i}r+\delta_i}=g^{[(1-c_i)+c_iy^{\alpha}]y^{u_i}}f^{\theta_i}$$

$$=\begin{cases}g^{y^{u_i}}f^{\theta_i}, & c_i=0\\ g^{y^{u_i+\alpha}}f^{\theta_i}, & c_i=1\end{cases}=s_i$$

因此完备性成立。 证毕

定理2 上述PVE协议是有效的。

证明 这只需证明一个证明者欺骗诚实的验证者成功的概率是可以忽略的。在每一轮询问中，对于提问$c=0$ 和 $c=1$，当证明者声称的事实成立时，也就是A关于h的离散对数等于M^B关于g, y 和 f 的双重离散对数时，两种提问都可以回答。假定离散对数和双重离散对数是困难的，如果不等，则舞弊的证明者只能事先准备 t_i 和 u_i 应付其中的一个提问，因此每一轮作弊被发现的概率为1/2 。如果假定杂凑函数的输出服从均匀分布，那么重复 l 轮后，舞弊的证明者被发现的概率为$1-1/2^{-l}$。因此证明者欺骗成功的概率为$1/2^{-l}$，是可以忽略的。 证毕

定理3 上述PVE协议对多项式界的攻击者是语义安全的。

证明 只需证明在离散对数和双重离散对数困难性假设下，即使消息空间很有限，恶意的验证者也不能提取消息的任何信息。注意到公开的数据$(M,A,B,c,u_0,\delta_0,\cdots,u_{l-1},\delta_{l-1},)$中：

$$M=g^mf^r \tag{1}$$

$$A\equiv_p h^{\alpha} \tag{2}$$

$$B\equiv_p m^{-1}y^{\alpha} \tag{3}$$

$$u_i\equiv_q w_i-c_i\alpha \tag{4}$$

$$\delta_i\equiv_p \theta_i-c_iB\,y^{u_i}r \tag{5}$$

如果假定杂凑函数是理想的，则c可以视为与其它数据是相互独立的。又注意到δ_i 是已知的且θ_i 和r在Z_p中均匀分布，因此g^m在G中均匀分布。因此验证者不能在多项式时间确定g^m。类似地，$w_i\in_R Z_q$，那么$\alpha\in_R Z_q$ 和 $y^{\alpha}\bmod p$ 在一个q阶子群中均匀分布。联系(3)，则m在Z_p中均匀分布。因此验证者不能在多项式时间猜测m并予以验证。 证毕

定理3保证上述方案并不削弱ElGamal体制语义安全性，也就是说，攻击者不能区分两个ElGamal PVE加密的消息是否相同。在Stadler方案中由于泄漏了g^m，因此不可能是语义安全的。语义安全性在要加密的消息空间很有限时非常重要，可以防止攻击者穷举攻击。上述证明的消息复杂性为$3\lceil\log p\rceil+l(1+2\lceil\log q\rceil)$ bit，取l=100，p 为1024bit素数，q为160bit素数，那么上述证明的长度大约为4.3k字节，这在许多应用中是可以接受的。

3.3 多接收者的ElGamal PVE

现在考虑Alice发送ElGamal密文给多个接受者的情形，要求证明每一个密文中隐藏的消息与承诺的消息都是一致的。一个平凡的构造是重复执行3.1节的协议多次，显然这样的效率很低，下面给出效率更高的协议。记3.1节的协议为PVE$\{m,r,\alpha|M=g^mf^r\wedge A\equiv_p y^{\alpha}\wedge B\equiv_p m^{-1}y^{\alpha}\}$。设$n$ 个接受者的ElGamal公钥分别为$(p,h,y_j=h^{z_j}\bmod p)$，其中j=1 ,…, n。

Alice 公布$M=g^mf^r$作为对秘密消息m的承诺。对j=1 ,…, n, Alice 计算$A_j\equiv_p h^{\alpha_j}$ $B_j\equiv_p m^{-1}y_j^{\alpha_j}$，其中$\alpha_j\in_R Z_q$。Alice随机选取$\xi_j\in_R Z_q$ (j=1 ,…, n)并计算

$$c\equiv H(h^{\xi_1}\bmod p\,\|\,h^{\xi_2}\bmod p\,\|\,y_2^{\xi_2}y_1^{\xi_1}\bmod p\,\|\cdots$$

$$\|\,h^{\xi_n}\bmod p\,\|\,y_n^{\xi_n}y_1^{\xi_1}\bmod p)\bmod 2^l,$$

$$v_1\equiv_q\xi_1+c\alpha_1,\quad v_2\equiv_q\xi_2-c\alpha_2,\ \cdots,\ v_n\equiv_q\xi_n-c\alpha_n$$

然后Alice公布

$$\text{PVE}\{m,r,\alpha_1|M=g^mf\wedge A_1\equiv_p y_1^{\alpha_1}\wedge B_1$$

$$\equiv_p m^{-1}y_1^{\alpha_1}\},(c,A_1,B_1,v_1,\cdots,A_n,B_n,v_n)$$

如果PVE和

$$c\equiv H(h^{v_1}/A_1^c\bmod p\,\|\,h^{v_2}/A_2^c\bmod p\,\|\,y_2^{v_2}y_1^{v_1}(B_2/B_1)^c\bmod p\|\cdots$$

$$\|h^{vn}A_n^c\bmod p\|\,y_n^{v_n}y_1^{v_1}(B_n/B_1)^c\bmod p)\bmod 2^l$$

都成立，验证者接受该加密，否则拒绝接受。

注意到$(c,\ A_1,B_1,v_1,\cdots,A_n,B_n,v_n)$ 是2.3节ZPK的自然推广，它是ZPK $\{\alpha_1,\cdots,\alpha_n|A_1\equiv_p h^{\alpha_1}\wedge\cdots\wedge A_n\equiv_p h^{\alpha_n}\wedge B_2B_1^{-1}\equiv_p y_2^{\alpha_2}y_1^{-\alpha}\wedge\cdots\wedge B_nB_1^{-1}\equiv_p y_n^{\alpha_n}y_1^{-\alpha}\}$的证据。这一ZPK表明$n$个密文隐藏了同样的秘密消息，而单个接受者的PVE 表明第一个密文加密的消息与承诺的消息一致，因此所有的密文隐藏的消息与承诺的消息都是一致的。上述协议需要大约$(2n+1)\lceil\log_2 p\rceil+2l+(n+2l)\lceil\log_2 q\rceil$)bit。直接构造需要大约$(2n+1)\lceil\log_2 p\rceil+nl(1+2\lceil\log_2 q\rceil)$ bit，因此，上述协议在n很大时效率高得多。

4 可公开验证的RSA体制

这里只给出单个接受者的情形，对于多个接受者的情形可以用类似3.3节的方法得到。设 n 是RSA 模数，其分解只有消息接受者知道。$G=\langle g\rangle$ 是阶为 n 的循环群且其中离散对数是困难的。 RSA 公钥为 (e,n)，满足 $(e,\varphi(n))=1$，其中 $\varphi(\cdot)$ 是Euler Totient 函数。出于效率的考虑，许多国际标准建议$e=2^t+1$，如e=3 (RFC 1423), 65537 (X.509, PKCS#1)。因此这里考虑加密指数具有这种形式的情形。RSA 私钥为 $d\equiv_{\varphi(n)}e^{-1}$， 要用公钥加密一个消息$m\in Z_p^*$，发送者计算$A\equiv_n m^e$。只有接受者能够从密文中恢复明文$m\equiv_n A^d$。注意RSA体制不是语义安全的，因此不能构造语义安全的RSA PVE。下

面计算安全的RSA PVE效率较高。

(1) (承诺) Alice公开$M=g^m$作为对秘密消息m的承诺。

(2) (零知识证明) Alice 计算

$M_1 = M^m$, $M_2 = M_1^{m^2}$, $M_3 = M_2^{m^4}$, $\cdots$, $M_t = M_{t-1}^{m^{2^{t-1}}}$; ZPK$\{m|$ $M=g^m \wedge M_1=M^m \wedge g^A=M_t^m\}$, ZPK$\{r_1|M_1=g^{r_1} \wedge M_2=M_1^{r_1}\}$, ZPK$\{r_2|$ $M_2=g^{r_2} \wedge M_3=M_2^{r_3}\}$, $\cdots$, ZPK$\{r_{t-1}|M_{t-1}=g^{r_{t-1}} \wedge M_t=M_{t-1}^{r_{t-1}}\}$。

(3) (验证)验证者验证上述所有零知识证明，如果所有的证明都是有效的，则接受Alice的加密证明。

显然任何诚实的证明者和验证者都可以成功执行上述协议，协议的有效性基于其应用的2.3节的基本ZPK是不可伪造的。协议需要$O(tl+(t+3)\lceil \log_2 n \rceil)$ bit，其中l是一个安全参数。实用中，t 通常很小，如1, 4, 16等，例如取$t=4$，$l=40$，n为1024 bit，此时需要大约800个字节。用选择分割方法需要$O(l\lceil \log_2 n \rceil)$ bit（$l \geq 40$），取同样的安全参数，选择分割方法需要5120个字节，因此上述方法比应用选择分割技术构造效率高得多。上述构造也可以推广到任意加密指数形式，此时在最坏的情况下需要 $O(\lceil \log_2 e \rceil^2 \times \lceil \log_2 n \rceil)$ bit。

5 结论

本文分别给出了 PVE 的 ElGamal 加密和 RSA 加密，并将 PVE 的 ElGamal 加密高效地推广到了多接收者环境。其中ElGamal情形是Stadler方案的改进，使其具有语义安全性，使得加密在消息空间很有限时也可以抗击穷举攻击。该方案有效地推广到了多接受者的情形。最后给出了 PVE 的 RSA 加密，效率远远高于使用选择分割一般技术的构造。上述协议可以应用于秘密数据托管、签名分享、公平交换、电子支付等。

参 考 文 献

[1] Stadler M. Publicly verifiable secret sharing. In EUROCRYPT'96, Brussels, Belgium, Springer Verlag, LNCS, 1996, vol. 1070: 191 – 199.

[2] Asokan N, Shoup V, Waidner M. Optimistic fair exchange of digital signatures. In EUROCRYPT'98, Paris, France, Springer Verlag, LNCS, 1998, vol. 1403: 591 – 606.

[3] Camenisch J, Maurer U, Stadler M. Digital payment systems with passive anonymity revoking trustees. In Computer Security—ESORICS'96, Berlin, German, Springer-Verlag, LNCS,1996, vol. 1146: 33 – 43.

[4] Frankel Y, Tsiounis Y, Yung M. Indirect discourse proofs: achieving efficient fair on-line e-cash. In ASIACRYPT'96, Tokyo, Japan, Springer-Verlag, LNCS, 1996, vol. 1163: 68 – 82.

[5] Poupard G, Stern J. Fair encryption of RSA keys. In EUROCRYPT'00, Springer-Verlag, LNCS, 2000, vol. 1807: 173 – 189.

[6] Young A, Yung M. Auto-recoverable auto-certifiable cryptosystems. In EUROCRYPT'98, Paris, France, Springer Verlag, LNCS, 1998, vol. 1403: 17 – 31.

[7] Fujisaki, E., Okamoto, T. Statistical zero knowledge protocols to prove modular polynomial relations. In CRYPTO'97, Francisco, America, Springer Verlag, LNCS, 1997, vol.1294: 16 – 30.

[8] Chaum D, Pedersen T R. Wallet databases with observers. In CRYPTO'92, Florida, America, Springer-Verlag. LNCS, 1993, vol.740: 89 – 105.

伍前红：男，1976年生，博士生，研究方向为密码学、可信计算与电子商务安全.

王继林：男，1966年生，副教授，研究方向为密码学、匿名理论与技术.

袁素春：女，1981年生，硕士生，研究方向为信号与系统、无线网络安全.

王育民：男，1936年生，教授，博士生导师，研究方向为密码与编码、信息安全.