基于身份的跨信任域签密方案

张 雪 冀会芳 李光松 韩文报
(信息工程大学数学工程与先进计算国家重点实验室 郑州 450002)

摘 要 实际网络环境尤其是未来异构网络融合环境中,各个信任域大多都是独立的自治域,使用不同的系统参数。为此提出了一种新的基于身份的跨信任域签密方案,该方案对PKG系统参数不作限制,各PKG可以使用完全不同的系统公开参数、不同的主密钥和公钥。并且在该签密协议的基础上给出了会话密钥的生成方法。在随机预言模型中给出了安全性证明,在BDH问题是困难的的假设下该协议是安全的,其满足机密性、不可伪造性、不可否认性和公开验证性。在与其他跨信任域签密方案计算开销相当的情况下,该方案不仅实现了跨信任域签密,而且对各PKG参数不作限制。

关键词 基于身份,签密,跨信任域,密钥协商
中图法分类号 TP309 **文献标识码** A **DOI** 10.11896/j.issn.1002-137X.2015.5.033

Identity-based Signcryption Cross Autonomous Domains

ZHANG Xue JI Hui-fang LI Guang-song HAN Wen-bao
(State Key Laboratory of Mathematical Engineering and Advanced Computing,
PLA Information Engineering University, Zhengzhou 450002, China)

Abstract Real networks especially heterogeneous networks consist of several cooperating sub-networks which belong to different trust domains which are independent and autonomous. The trust domains are maintained by different PKGs. A novel ID-based cross-domain signcryption scheme was proposed which is no restriction on PKG system parameters so that public system parameters, system master keys and system public keys can be totally different. Based upon this signcryption scheme, a cross-domain session key generation scheme was presented. Our cross-doamin signcryption protocol was proved to be secure in the random oracle model assuming the bilinear Diffle-Hellman problem is hard. It satisfies the basic security requirements confidentiality, unforgeability, non-repudiation and public verifiability. The scheme not only achieves cross-domain signcryption, but also makes no restriction on PKG system parameters on condition that computation overheads are little increased.

Keywords Identity-based, Signcryption, Cross-domain, Key agreement

1 引言

Shamir[1]于1984年提出了基于身份的公钥体制,给出了一种基于身份的签名(IBS)体制,但是直到2001年才由Boneh和Franklin[2]提出了第一个实用的基于身份的加密方案,该方案是基于双线性对构造的。基于身份的密码体制中,用户公钥即是用户的身份信息,而用户的私钥则由权威可信方私钥生成器(Private Key Generator,PKG)通过用户的身份信息直接计算得出。基于身份的密码体制避免了对称密码体制繁重的密钥管理问题,同时也避免了传统PKI公钥证书存储和管理维护开销大的问题。

签密的概念由Zheng[3]于1997年首次提出,可以在一个逻辑步骤内同时实现加密和签名,但该方案不具有公开验证性,其不可否认性也需要通过零知识证明协议来完成。基于身份的签密方案使得基于身份的密码系统的优势引入到签密方案中,2002年Malone-Lee[4]定义了基于身份的签密方案的安全模型,利用双线性对构造了第一个基于身份的签密方案,该方案具有机密性和不可伪造性。此方案可以看作是简化的Boneh-Franklin加密方案和Hess[5]基于身份签名方案的结合产物。路晓明等[6]给出的签密方案假设各PKG使用相同的参数,仅有主密钥和公钥不同。Li[7]、Lal[8]等人分别给出了不同PKG环境下基于身份的签密方案。张红旗[9]给出的方案虽然使用不同的椭圆曲线和生成元,但仍使用相同的Hash函数。

当前的多信任域[10]环境下的签密方案设计大多都是基于假设:各PKG使用相同的系统参数,仅有主密钥和私钥不同。但实际的网络环境中,尤其是未来异构网络融合应用中,各个信任域大多都是独立的自治域,使用不同的系统参数,因此以上方案大都难以满足实际的认证需要。为此,我们提出了一种应用范围更加广泛的跨信任域的签密方案,该方案对

到稿日期:2014-06-08 返修日期:2014-12-28 本文受国家自然科学基金资助项目(61201220)资助。
张 雪(1984—),女,博士生,主要研究方向为信息安全、无线网络安全,E-mail:whity_zhang@163.com;冀会芳(1982—),女,博士,讲师,主要研究方向为信息安全;李光松(1977—),男,博士,副教授,主要研究方向为信息安全、无线网络安全;韩文报(1963—),男,教授,博士生导师,主要研究方向为密码学、信息安全。

各个 PKG 系统参数不作限制，可以使用不同的系统公开参数、不同的主密钥和公钥。我们还在该签密协议的基础上给出了跨信任域的会话密钥的生成方法，该方案适用于扩展跨信任域的密钥协商方案。

2 基于身份的跨信任域签密方案

双线性映射

设 G_1，G_2 分别是阶为素数 q 的加法循环群和乘法循环群，P 为群 G_1 的生成元。称映射 $e:G_1\times G_1\to G_2$ 为一个双线性对，若下列性质成立：

双线性性：$e(aP,bQ)=e(P,Q)^{ab}$，对 $\forall P,Q\in G_1$，$a,b\in Z_q^*$ 均成立。

非退化性：存在 $\forall P,Q\in G_1$，使得 $e(P,Q)\neq 1_{G_2}$，其中 1_{G_2} 是 G_2 的单位元。

可计算性：对于 $\forall P,Q\in G_1$，存在有效算法来计算 $e(P,Q)$，即可在多项式时间内完成对 $e(P,Q)$ 的计算。

网络中存在多个独立、自治的信任域，每个信任域拥有自己信任的 PKG 提供密钥分发服务。假设所有信任域的各个 PKG 是可信的，每个 PKG 使用不同的公开参数 $\langle G_1,G_2,e,P,H_1,H_2,H_3\rangle$，主密钥 s 和公钥 $Pub=sP$ 均不同。

系统建立

在 PKG_A 管理域中，G_1^A，G_2^A 分别是阶为素数 q_A 的加法循环群和乘法循环群，P_A 为群 G_1^A 的生成元，G_1^A，G_2^A 满足双线性映射：$e_A:G_1^A\times G_1^A\to G_2^A$。$H_1^A:\{0,1\}^*\to G_1^A$，$H_2^A:G_2^A\to\{0,1\}^*$，$H_3^A:\{0,1\}^*\times G_1^A\to Z_{q_A}^*$。随机选取 $s_A\in Z_{q_A}^*$ 作为 PKG_A 的主密钥，相应的系统公钥为 $Pub_A=s_AP_A$。公开的系统参数为：$\langle G_1^A,G_2^A,q_A,P_A,Pub_A,e_A,H_1^A,H_2^A,H_3^A\rangle$。

在 PKG_B 管理域中，G_1^B，G_2^B 分别是阶为素数 q_B 的加法循环群和乘法循环群，P_B 为群 G_1^B 的生成元，G_1^B，G_2^B 满足双线性映射 $e_B:G_1^B\times G_1^B\to G_2^B$。$H_1^B:\{0,1\}^*\to G_1^B$，$H_2^B:G_2^B\to\{0,1\}^*$，$H_3^B:\{0,1\}^*\times G_1^B\to Z_{q_B}^*$。随机选取 $s_B\in Z_{q_B}^*$ 作为 PKG_B 的主密钥，相应的系统公钥为 $Pub_B=s_BP_B$。公开的系统参数为：$\langle G_1^B,G_2^B,q_B,P_B,Pub_B,e_B,H_1^B,H_2^B,H_3^B\rangle$。

用户密钥对生成

假设 Alice 属于 PKG_A，身份标识 $ID_{Alice}\in\{0,1\}^*$，对应的公私钥分别为 $Q_{Alice}=H_1^A(ID_{Alice})$ 和 $S_{Alice}=s_AQ_{Alice}$。

假设 Bob 属于 PKG_B，身份标识 $ID_{Bob}\in\{0,1\}^*$，对应的公私钥分别为 $Q_{Bob}=H_1^B(ID_{Bob})$ 和 $S_{Bob}=s_BQ_{Bob}$。

签密算法

Alice 用自己的私钥 S_{Alice} 和 Bob 的公钥 Q_{Bob} 对明文 $m_{Alice}\in\{0,1\}^*$ 签密，并将最后结果发送给 Bob。具体流程如下：

1)随机选取 $r_1^{Alice}\in Z_{q_A}^*$，$r_2^{Alice}\in Z_{q_B}^*$，计算 $R_1^{Alice}=r_1^{Alice}P_A$，$R_2^{Alice}=r_2^{Alice}P_B$。

2)计算

$w_{Alice}=e_B(r_2^{Alice}Pub_B,Q_{Bob})$

$c_{Alice}=m_{Alice}\oplus H_2^B(w_{Alice})$

3)计算 $h_{Alice}=H_3^A(c_{Alice},R_1^{Alice})$，

签名为 $\sigma_{Alice}=r_1^{Alice}Pub_A+h_{Alice}S_{Alice}$。

Alice 发送消息 $\{c_{Alice},R_1^{Alice},R_2^{Alice},\sigma_{Alice}\}$ 给 Bob。

Bob 收到 Alice 发来的消息 $\{c_{Alice},R_1^{Alice},R_2^{Alice},\sigma_{Alice}\}$ 后，执行以下步骤：

1)计算

$e_A(P_A,\sigma_{Alice})=e_A(R_1^{Alice},Pub_A)e_A(Pub_A,Q_{Alice})^{H_3^A(c_{Alice},R_1^{Alice})}$ 是否成立，即 Bob 确认该消息是否是 Alice 签名的，若确认是 Alice 的签名则接受该签密消息。

2)计算

$w_{Alice}^*=e_B(R_2^{Alice},S_{Bob})$

$m_{Alice}=H_2^B(w_{Alice}^*)\oplus c_{Alice}$

即用 Bob 的私钥 S_{Bob} 解密得到 m_{Alice}。

容易验证：

$$\begin{aligned}e_A(P_A,\sigma_{Alice})&=e_A(P_A,r_1^{Alice}Pub_A+h_{Alice}S_{Alice})\\&=e_A(P_A,r_1^{Alice}Pub_A)e_A(P_A,h_{Alice}S_{Alice})\\&=e_A(r_1^{Alice}P_A,Pub_A)e_A(P_A,S_{Alice})^{h_{Alice}}\\&=e_A(r_1^{Alice}P_A,Pub_A)e_A(P_A,s_AQ_{Alice})^{h_{Alice}}\\&=e_A(r_1^{Alice}P_A,Pub_A)e_A(s_AP_A,Q_{Alice})^{h_{Alice}}\\&=e_A(R_1^{Alice},Pub_A)e_A(Pub_A,\\&\quad Q_{Alice})^{H_3^A(c_{Alice},R_1^{Alice})}\end{aligned}$$

$$\begin{aligned}w_{Alice}^*&=e_B(R_2^{Alice},S_{Bob})=e_B(r_2^{Alice}P_B,s_BQ_{Bob})\\&=e_B(r_2^{Alice}s_BP_B,Q_{Bob})=e_B(r_2^{Alice}Pub_B,Q_{Bob})=w_{Alice}\end{aligned}$$

会话密钥生成

如果 Alice 和 Bob 相互完成一次签密，则双方完成认证的同时，也可以得到会话密钥。具体过程如下：

Alice 完成签密发送给 Bob 解签密后，Bob 使用同样的签密方式，用自己的私钥 S_{Bob} 和 Alice 的公钥 Q_{Alice} 对明文 $m_{Bob}\in\{0,1\}^*$ 签密，并将最后结果发送给 Alice。过程同上述 Alice 签密步骤：

1)随机选取 $r_1^{Bob}\in Z_{q_B}^*$，$r_2^{Bob}\in Z_{q_A}^*$，计算 $R_1^{Bob}=r_1^{Bob}P_B$，$R_2^{Bob}=r_2^{Bob}P_A$。

2)计算

$w_{Bob}=e_A(r_2^{Bob}Pub_A,Q_{Alice})$

$c_{Bob}=m_{Bob}\oplus H_2^A(w_{Bob})$

3)计算 $h_{Bob}=H_3^B(c_{Bob},R_1^{Bob})$，

签名为 $\sigma_{Bob}=r_1^{Bob}Pub_B+h_{Bob}S_{Bob}$。

Bob 发送 $\{c_{Bob},R_1^{Bob},R_2^{Bob},\sigma_{Bob}\}$ 给 Alice。

Alice 收到 Bob 发来的消息 $\{c_{Bob},R_1^{Bob},R_2^{Bob},\sigma_{Bob}\}$ 后，执行以下步骤：

1)计算

$e_B(P_B,\sigma_{Bob})=e_B(R_1^{Bob},Pub_B)e_B(Pub_B,Q_{Bob})^{H_3^B(c_{Bob},R_1^{Bob})}$ 是否成立，即 Alice 确认该消息是否是 Bob 签名的，若确认是 Bob 的签名则接受该签密消息。

2)计算

$w_{Bob}^*=e_A(R_2^{Bob},S_{Alice})$

$m_{Bob}=H_2^A(w_{Bob}^*)\oplus c_{Bob}$

即用 Alice 的私钥 S_{Alice} 解密得到 m_{Bob}。

Alice 和 Bob 各进行一次签密完成了双方认证，同时也交换了认证密钥协商所需的双方临时公钥，即：R_1^{Alice}、R_2^{Alice}、R_1^{Bob}、R_2^{Bob}。那么 Alice 和 Bob 根据各自的临时私钥：r_1^{Alice}、r_2^{Alice}、r_1^{Bob}、r_2^{Bob}，可以计算得到协商的会话密钥。具体步骤如下：

1)Alice 和 Bob 分别计算 $K_{Alice,Bob}$，$K_{Bob,Alice}$。

$K_{Alice,Bob}=e_A(S_{Alice},R_2^{Bob})e_B(Q_{Bob},r_2^{Alice}Pub_B)$

$K_{Bob,Alice}=e_B(S_{Bob},R_2^{Alice})e_A(Q_{Alice},r_2^{Bob}Pub_A)$

$K_{Alice,Bob}=e_A(S_{Alice},R_2^{Bob})e_B(Q_{Bob},r_2^{Alice}Pub_B)$

$$=e_A(s_A Q_{Alice}, r_2^{Bob} P_A) e_B(Q_{Bob}, r_2^{Alice} s_B P_B)$$
$$=e_A(Q_{Alice}, P_A)^{s_A r_2^{Bob}} e_B(Q_{Bob}, P_B)^{r_2^{Alice} s_B}$$

$$K_{Bob,Alice}=e_B(S_{Bob}, R_2^{Alice}) e_A(Q_{Alice}, r_2^{Bob} Pub_A)$$
$$=e_B(s_B Q_{Bob}, r_2^{Alice} P_B) e_A(Q_{Alice}, r_2^{Bob} s_A P_A)$$
$$=e_B(Q_{Bob}, P_B)^{s_B r_2^{Alice}} e_A(Q_{Alice}, P_A)^{r_2^{Bob} s_A}$$

可知，$K_{Alice,Bob}=K_{Bob,Alice}$。令 $K_{AB}=K_{Alice,Bob}=K_{Bob,Alice}$。

2) Alice 计算 $K_1^{Alice}=r_1^{Alice} R_2^{Bob}$，$K_2^{Alice}=r_2^{Alice} R_1^{Bob}$，Bob 计算 $K_1^{Bob}=r_1^{Bob} R_2^{Alice}$，$K_2^{Bob}=r_2^{Bob} R_1^{Alice}$。显然 $K_1^{Alice}=K_1^{Bob}=r_1^{Alice} r_2^{Bob} P_A$，$K_2^{Alice}=K_2^{Bob}=r_2^{Alice} r_1^{Bob} P_B$，令 $K_1=K_1^{Alice}=K_1^{Bob}$，$K_2=K_2^{Alice}=K_2^{Bob}$。

3) Alice 和 Bob 分别计算得到会话密钥 $sk=H(K_{AB}, K_1, K_2, R_1^{Alice}, R_2^{Alice}, R_1^{Bob}, R_2^{Bob}, ID_{Alice}, ID_{Bob})$，$H:\{0,1\}^* \rightarrow \{0,1\}^k$，其中 k 表示会话密钥长度。

3 安全性及性能分析

安全性分析

这里以 Alice 签密为例进行分析。

(1)机密性

机密性是指除 Bob 本人以外，其他任何人都不能从 $\{c_{Alice}, R_1^{Alice}, R_2^{Alice}, \sigma_{Alice}\}$ 中得到消息 m_{Alice}。

定理 1 在随机预言模型中，若存在一个 IND-MPIBSC-CCA2 敌手 $\mathcal{A}$ 能在 t 时间内，经过至多 $q_{H_i^j}$ 次 $H_i^j(i=1,2,3,j=A,B)$ 询问、q_S 次签密询问、q_U 次解签密询问，以 ε 的优势赢得定义 1 中的游戏，则存在一个算法 $\mathcal{C}$，能够在时间 $t'=t+(q_S+4q_U)t_e$ 内，以 ε' 的优势解决 BDH 问题，其中 t_e 表示一次双线性对计算所需要的时间。

证明：首先以管理域 A 中用户给管理域 B 中用户发送签密文为例来证明。

$\mathcal{C}$ 接收一个随机的 BDH 问题实例：$(P_B, P_1, P_2, P_3)=(P_B, aP_B, bP_B, cP_B)$，其目标是计算出 $e_B(P_B, P_B)^{abc}$。$\mathcal{C}$ 把 $\mathcal{A}$ 作为子程序并扮演 IND-MPIBSC-CCA2 游戏中的 $\mathcal{A}$ 的挑战者。

游戏开始，$\mathcal{C}$ 把系统参数发送给 $\mathcal{A}$，其中 $Pub_B=cP_B$，$\mathcal{C}$ 亦不知道 c，c 模拟的是 PKG 的主私钥。$\mathcal{C}$ 维护 $L_i^j(i=1,2,3,j=A,B)$、L_S^A、L_U^A、L_S^B、L_U^B10 张列表，这些列表开始都为空，$L_i^j(i=1,2,3,j=A,B)$分别用于跟踪 $\mathcal{A}$ 对预言机 $H_i^j(i=1,2,3,j=A,B)$的询问，L_S^A，L_S^B 分别用于模拟域 A 和域 B 的签密预言机，L_U^A，L_U^B 分别用于模拟域 A 和域 B 的解签密预言机。

H_1^B 询问：$\mathcal{C}$ 首先从$(1,2,\cdots,q)$中选取一个随机数 i_b，假设 $\mathcal{A}$ 不会进行重复询问，对于 $\mathcal{A}$ 的第 i 次询问，若 $i=i_b$，则回答 $H_1^B(ID_u)=bP_B$ 并设置 $ID_u=ID_{i_b}$；否则从 $Z_{q_B}^*$ 中随机选取 x，计算 $Q_u=xP_B$ 和 $S_u=xPub_B$，并将$(ID_u, Q_{ID_u}, S_{ID_u}, x)$添加到 L_1^B 中，回答 $H_1^B(ID_u)=Q_u$。

H_1^A 询问：$\mathcal{C}$ 从 $Z_{q_A}^*$ 中随机选取 x，计算 $Q_u=xP_A$，$S_u=xPub_A$，并将(ID_u, Q_u, S_u, x)添加到 L_1^A 中，回答 $H_1^A(ID_u)=Q_u$。

H_2^A/H_2^B 询问：如果(w,h_2)在表 L_2^A/L_2^B 中，则返回 h_2；否则，从$(0,1)^*$中选取 h_2，将(w,h_2)添加到表 L_2^A/L_2^B 中，返回 h_2。

H_3^A/H_3^B 询问：如果$(c_{Alice}, R_1^{Alice}, h_3)/(c_{Bob}, R_1^{Bob}, h_3)$在表 L_3^A/L_3^B 中，返回 h_3；否则，从 $Z_{q_A}^*/Z_{q_B}^*$ 中选取 h_3，将$(c_{Alice}, R_1^{Alice}, h_3)/(c_{Bob}, R_1^{Bob}, h_3)$添加到表 L_3^A/L_3^B 中，返回 h_3。

$Extract_B$ 询问：假设 $\mathcal{A}$ 在进行该询问之前已经执行过了 H_1^B 询问，若 $ID_u=ID_b$，终止模拟；否则在表 L_1^B 中查找 ID_u 对应的条目(ID_u, Q_u, S_u, x)并返回 S_u。

$Extract_A$ 询问：假设 $\mathcal{A}$ 在进行该询问之前已经执行过了 H_1^A 询问，在表 L_1^A 中查找 ID_u 对应的条目(ID_u, Q_u, S_u, x)并返回 S_u。

Singcrypt 询问(ID_1, ID_2, m)：假设 $\mathcal{A}$ 在对 ID_1(管理域 A 中)和 ID_2(管理域 B 中)执行 *Singcrypt* 询问前已经执行过了 H_1^A/H_1^B 询问(分别在两个管理域中进行)：

在表 L_1^A 中查找条目(ID_1, Q_1, S_1, x)，在表 L_1^B 中查找条目(ID_2, Q_2, S_2, x)，从 $Z_{q_A}^*$ 中随机选择 r_1，从 $Z_{q_B}^*$ 中随机选择 r_2，计算 $R_1=r_1 P_A$，$R_2=r_2 P_B$；

计算 $w=e_B(r_2 Pub_B, Q_2)$，$c=m \oplus H_2^B(w)$，其中 $H_2^B(w)$ 可从上述 H_2^B 询问中获得；

计算 $h=H_3^A(c, R_1)$，$H_3^A(c, R_1)$可从上述 H_3^A 询问中获得；

计算 $\sigma=r_1 Pub_A+hS_1$；

返回$\{c, R_1, R_2, \sigma\}$。

UnSingcrypt 询问$(ID_1, ID_2, c, R_1, R_2, \sigma)$：假设 $\mathcal{A}$ 在对 ID_1(管理域 A 中)和 ID_2(管理域 B 中)执行 *UnSingcrypt* 询问前已经执行过了 H_1^A/H_1^B 询问(分别在两个管理域中进行)，此时对 ID_2 分两种情况讨论：

1) $ID_2 \neq ID_b$

在表 L_1^A 中查找条目(ID_1, Q_1, S_1, x)，在表 L_1^B 中查找条目(ID_2, Q_2, S_2, x)，如果 $ID_1 \notin L_1^A$ 或 $ID_2 \notin L_1^B$，返回 $\perp$，否则继续；

计算 $e_A(P_A, \sigma)=e_A(R_1, Pub_A) e_A(Pub_A, Q_1)^{H_3^A(c,R_1)}$ 是否成立，不成立则返回签密文无效，否则继续；

计算 $w=e_B(R_2, S_2)$，如果 $w \notin L_1^B$，返回 $\perp$；否则计算 $m=H_2^B(w) \oplus c$ 并返回 m。

2) $ID_2=ID_b$

按以下步骤遍历表 L_3^A 中的条目(c, R_1, h_3)：

如果 $ID_1 \in L_1^A$，找到表 L_1^A 中的 Q_1 和 S_1；否则移到表 L_2^B 中的下一个条目且重新开始；

如果$(c, R_1, h_3) \notin L_3^A$，返回符号 $\perp$；否则计算 $h_3=H_3^A(c, R_1)$；

计算 $e_A(P_A, \sigma)=e_A(R_1, Pub_A) e_A(Pub_A, Q_1)^{h_3}$ 是否成立，不成立则返回签密文无效；否则继续；

计算 $w=e_B(bPub_B, R_2)$，如果 $w \notin L_2^B$，返回 $\perp$；否则计算 $h_2=H_2^B(w)$；

计算 $m=h_2 \oplus c$ 并返回 m。

在经过多项式有界次上述询问后，$\mathcal{A}$ 输出两个希望挑战的身份$\{ID_1, ID_2\}$和两个消息$\{m_0, m_1\}$，如果 $ID_B \neq ID_b$，$\mathcal{C}$ 终止模拟；否则随机选取 $\sigma^* \in G_1^A$，$R_1^* \in G_1^A$，令 $R_2^*=aP_B$，$w=h$(h 就是 BDH 问题的候选答案)，计算 $c^*=H_2^B(w) \oplus m_u$，$u \in \{0,1\}$，然后提交挑战密文$(\sigma^*, R_1^*, R_2^*, c^*)$给 $\mathcal{A}$。

$\mathcal{A}$ 经过第二轮询问，这些询问与第一轮相同。在模拟结束时，$\mathcal{A}$ 输出一个 u' 作为对 u 的猜测。如果 $u'=u$，$\mathcal{C}$ 输出 $h=e_B(R_2^*, S_{ID_{ib}})=e_B(P_B, P_B)^{abc}$ 作为 BDH 问题的答案；否则 $\mathcal{C}$ 没有解决 BDH 问题。

下面计算 $\mathcal{C}$ 成功的概率。

如果 $\mathcal{A}$ 在第一阶段对 ID_b 进行 *Extract* 询问，$\mathcal{C}$ 将失败。

身份 ID_b 的选择有 $q_{H_1^B}$ 种可能，且至少有一个身份没执行 *Extract* 询问。因此 $\mathscr{A}$ 不对 ID_b 进行 *Extract* 询问的概率大于 $\frac{1}{q_{H_1^B}}$（进行 H_1^B 询问的次数）。此外，$\mathscr{A}$ 选择身份 ID_b 进行挑战的概率为 $\frac{1}{q_{H_1^B}}$。

在第二阶段，如果 $\mathscr{A}$ 对 $w=e_B(P_B,P_B)^{abc}$ 执行 H_2^B 询问，$\mathscr{C}$ 将失败。同理，$\mathscr{A}$ 不对 $w=e_B(P_B,P_B)^{abc}$ 执行 H_2^B 询问的概率大于 $\frac{1}{q_{H_2^B}}$（执行 H_2^B 询问的次数），因此，$\mathscr{C}$ 解决 BDH 问题的优势至少为 $\varepsilon\frac{1}{q_{H_1^B}q_{H_2^B}}$。在 $\mathscr{C}$ 的计算时间方面，每次 *Singcrypt* 询问需要 1 次双线性对运算，每次 *UnSingcrypt* 询问需要 4 次双线性对运算。

同理可证，管理域 B 中用户给管理域 A 中用户发送签密文仍然满足机密性。

证毕。

(2)不可伪造性

不可伪造性是指任何攻击者都不能伪造一个来自发送方的对消息的签密。本方案在适应性选择消息攻击下抗存在性伪造。如果存在一个敌手能够伪造一个我们的签名，则他也能够伪造下面的一个签名方案，该签名方案是 Hess 签名方案的一个变体。

签名：签名者随机选取 $r_1^{Alice}\in Z_{q_A}^*$，计算 $R_1^{Alice}=r_1^{Alice}P_A$ 和 $\sigma_{Alice}=r_1^{Alice}Pub_A+h_{Alice}S_{Alice}$，对消息 m_{Alice} 的签名为 $(R_1^{Alice},\sigma_{Alice})$。

验证：当收到签名 $(R_1^{Alice},\sigma_{Alice})$ 时，验证者计算 $h_{Alice}=H_3^A(c_{Alice},R_1^{Alice})$，并检验等式 $\sigma_{Alice}=r_1^{Alice}Pub_A+h_{Alice}S_{Alice}$ 是否成立。

由于 Hess 方案在适应性选择消息攻击下抗存在性伪造，因此我们的方案也同样抗存在性伪造。

(3)不可否认性

不可否认性是指任何人都不能够否认其发送过该签密消息。由于本方案满足签密的不可伪造性，只有本人 Alice 能够发送签名消息，因此只要 Bob 正确验证了 Alice 的签名，Alice 就不能否认曾经发过这个消息。

(4)公开验证性

只需要将 $\{c_{Alice},R_1^{Alice},R_2^{Alice},\sigma_{Alice}\}$ 给第三方验证者，验证 $e_A(P_A,\sigma_{Alice})=e_A(R_1^{Alice},Pub_A)e_A(Pub_A,Q_{Alice})^{H_3^A(c_{Alice},R_1^{Alice})}$ 是否成立，即可确认该消息是否是 Alice 签名的，该过程不需要 Bob 私钥的参与，也无需访问明文，即在保密性的基础上实现了公开验证性。

性能分析

几种跨信任域签密方案的计算性能分析如表 1 所列。从比较中可以看到，本文提出的方案与其他方案相比最多只有 1 次点乘运算的差别，但其他几种跨信任域的签密方案都对 PKG 作了如下假设：各 PKG 使用相同的参数，仅有主密钥和私钥不同。而本方案在与其他跨信任域签密方案计算开销相当的情况下，不但实现了跨信任域的签密，并且对各 PKG 参数不作限制。

表 1　几种跨信任域签密方案的性能分析

方案	加密、签名			解密、验证			PKG 参数限制
	对运算	点乘运算	指数运算	对运算	点乘运算	指数运算	
文献[6]	1	4	0	4	0	1	有
文献[7]	1	3	1	4	0	1	有
文献[9]	1	5	0	4	0	1	有
本方案	1	5	0	4	0	1	无

结束语　本文提出了一种跨信任域的签密方案以及密钥生成方法，该方案不受 PKG 参数一致的假设制约，各个信任域可以具有完全不同的系统参数。下一步的研究重点是将该方案应用于异构无线网络安全切换，预期取得良好效果。

参 考 文 献

[1] Adi S. Identity-based cryptosystems and signature schemes [C] // Advances in Crypto'84. Springer-Verlag, 1984: 47-53

[2] Dan B, Matt F. Identity based encryption from the Weil paring [C] // Advances in Crypto'01. Springer-Verlag, 2001: 213-229

[3] Zheng Yu-liang. Digital Signcryption or How to Achieve Cost (Signature & Encryption)<<Cost(Signature)+Cost(Encryption) [C] // Advances in Crypto'97. Springer-Verlag, 1997, 1294: 165-179

[4] Malone-Lee John. Identity-based signcryption [R]. Cryptology ePrint Achive, Report 2002/098

[5] Hess Florian. Efficient identity based signature scheme based on Parings[C] // Proceeding of the 9th Workshop on Selective Areas on Cryptography (SAC 2002). Springer-Verlag, 2002, 2595

[6] 路晓明，冯登国. 一种基于身份的多信任域网格认证模型[J]. 电子学报，2006，34(4)：577-581

[7] Li Fa-gen, HuYu-pu, Zhang Chuan-rong. An identity based signcryption scheme for multi-domain Ad Hoc Networks[C] // Proceeding of ACNS 2007. 2007, 4521: 373-384

[8] Sunder L, Prashant K. Multi-PKG based signcryption [R]. Cryptology ePrint Archive, Report 2008/050

[9] 张红旗，张文波，等. 网格环境下基于身份的跨域认证研究[J]. 计算机工程，2009，35(17)：160-162

[10] 朱重，吴国新. 分布式多信域管理技术研究综述[J]. 计算机科学，2011，38(4)：38-92

(上接第 156 页)

[11] 鲍凤卿. 基于 Ns2 的 ZigBee 网络节点接入的研究[J]. 信息技术，2008(11)：95-98

[12] 徐沛成，胡国荣. 改进的 ZigBee 网络路由算法[J]. 计算机工程与设计，2013，34(9)：3019-3023

[13] Lj X, Hong S H, Fang K L. WSNHA-GAHR: a greedy and A* heuristic routing algorithm for wireless sensor networks in home automation[J]. IETCommunieations, 2011, 21(5): 1797-1805

[14] Lee J S, Su Y W, Shen C C. A comparative study of wireless protocols: bluetooth, UWB, ZigBee, and WiFi[C] // Proc of the International Conference on Information Networking (IECON'07). Taiwan: IEEE, 2007: 46-50

[15] Bhatia A, Kaushik P. A cluster based minimum battery cost AODV routing using multipath route for ZigBee[C] // Proceedings of the 2008 16th International Conference on Networks(ICON 2008). New Delhi, India, 2008: 1-7

[16] 刘兆孟. ZigBee 无线传感网路由协议研究与设计[D]. 无锡：江南大学，2013